Über Automorphismengruppen von Zyklischen Codes

Inaugural - Dissertation

zur
Erlangung des Doktorgrades der
Mathematisch-Naturwissenschaftlichen Fakultät
der Heinrich-Heine-Universität Düsseldorf

vorgelegt von
Dipl.-Math. Rolf Bienert
aus Reichenberg

Mai 2007

Aus dem Institut für Mathematik
der Heinrich-Heine-Universität Düsseldorf

Gedruckt mit Genehmigung der Mathematisch-Naturwissenschaftlichen Fakultät der Heinrich-Heine-Universität Düsseldorf

Referent: Prof. Dr. Fritz Grunewald
1. Korreferent: Prof. Dr. Otto Kerner
2. Korreferent: Priv.-Doz. Dr. Benjamin Klopsch
Tag der mündlichen Prüfung: 04.07.2007

Inhaltsverzeichnis

Tabellenverzeichnis

Kurzfassung

Es wurden bis zur Codelänge $N = 70$ lückenlos sämtliche binäre zyklische Codes und sämtliche zu diesen zyklischen Codes gehörenden Automorphismengruppen berechnet und identifiziert. Dabei wurden Gesetzmäßigkeiten gefunden und bewiesen, wie sich die Faktorenzerlegung(en) von N auf die Struktur der Automorphismengruppe (Kranzprodukt, Direktes Produkt, Semidirektes Produkt), sowie auf die Code-Attribute (Dimension, Minimaldistanz) auswirken.

$\mathfrak{Z}_N$ sei die zyklische Gruppe der Ordnung N. Sie operiert auf $\Omega = \{1, 2, \ldots, N\}$. Jeder zyklische Code C der Länge N kann als $\mathfrak{Z}_N$-Untermodul von $\mathbb{F}_2[\Omega]$ aufgefaßt werden. Der Code C ist dann auch ein $Aut(C)$-Untermodul dieses $\mathbb{F}_2$-Vektorraums. Diese Untermodul-Technik wurde bereits in der Arbeit selbst angewandt, um bestimmte zyklische Codes der Länge 217 zu ermitteln, die für die Aufstellung einer Vermutung über die Isomorphie-Faktoren von Automorphismengruppen benötigt wurden.

Besonderes Augenmerk bekam die Familie der Gruppen $PSL(r, 2), r \geq 3$:
Anhand des Untermodul-Verbands konnte gezeigt werden, wie mit zunehmendem r immer mehr Codes zur Automorphismengruppe $PSL(r, 2)$ (nämlich $2 \cdot (r - 2)$ Stück), zur Automorphismengruppe $PSL(r, 2) \wr \mathfrak{S}_2$ (nämlich $3 \cdot (r - 2)$ Stück), sowie zur Automorphismengruppe $\mathfrak{S}_2 \wr PSL(r, 2)$ (nämlich $4 \cdot (r - 2)$ Stück) gehören.
Insbesondere wurde noch eine Familie von Automorphismengruppen entdeckt:

$$Aut(C) \cong (\mathfrak{S}_2 \wr PSL(r, 2))/\mathfrak{S}_2^y,$$

mit einer zunehmenden Anzahl von y-Werten (nämlich $r - 2$ Stück), die sich nach einer Rekursionsformel angeben lassen. Die ebenfalls zunehmende Anzahl von zugehörigen Codes, nämlich $2, 5, 8, 12, 16, \ldots, 4 \cdot (r - 3)$ für die einzelnen y-Werte zu einem bestimmten r wurden der Übersicht halber in einem Dreiecksschema dargestellt – wie auch die y-Werte. Die Codes lassen sich als Plotkin-Summe zweier Untermoduln des $PSL(r, 2)$-Moduls $\mathbb{F}_2[\Omega]$ verstehen, so daß man auch ihre Attribute vorherbestimmen kann. Die Zuordnung der Codes zu ihren $r - 2$ Automorphismengruppen wurde über den hier eingeführten Verbandsraster-Abstand $\mathcal{VRA}_{ba}$ der beteiligten Untermoduln $\mathcal{U}_b \supseteq \mathcal{U}_a$ von $\mathbb{F}_2[\Omega]$ definiert.

Durch Beispiele und Grafiken im Text, sowie durch ein umfangreiches Tabellenwerk im Anhang – inklusive einer CD mit Codes, Automorphismengruppen und Auswertungsprogrammen (geschrieben in **Magma**) – wurde die Verständlichkeit dieser Arbeit verbessert,

wie auch die Möglichkeit für weitergehende Untersuchungen (z.B. Code-Isomorphien) geschaffen.

Abstract

Up to code length $N = 70$ all cyclic binary codes and all associated automorphism groups were calculated and identified completely. Hereby, certain laws and rules were found and proved. In particular, the impact of the factorization of N on the structure of the automorphism group (wreath product, direct product, semidirect product) as well as on the attributes of the code (dimension, minimum distance) was considered.

Let $\mathfrak{Z}_N$ be the cyclic group of order N. It acts on $\Omega = \{1, 2, \ldots, N\}$. Every cyclic code C of length N can be regarded as a $\mathfrak{Z}_N$-submodule of $\mathbb{F}_2[\Omega]$. The cyclic code C is also an $Aut(C)$-submodule of this $\mathbb{F}_2$-vectorspace. This submodule technique has already been applied within this thesis itself in order to construct specific cyclic codes of length 217 which were needed to support and formulate a conjecture about the isomorphic factors of automorphism groups.

The family $PSL(r, 2)$ of groups, $r \geq 3$ got a special focus within this thesis:
With the lattice of submodules it was shown that – with increasing r – more and more cyclic codes belong to the automorphism group $PSL(r, 2)$ (exactly $2 \cdot (r - 2)$ codes), as well as to the automorphism group $PSL(r, 2) \wr \mathfrak{S}_2$ (exactly $3 \cdot (r - 2)$ codes), and to the automorphism group $\mathfrak{S}_2 \wr PSL(r, 2)$ (exactly $4 \cdot (r - 2)$ codes).
In particular, one further family of automorphism groups was detected

$$Aut(C) \cong (\mathfrak{S}_2 \wr PSL(r, 2))/\mathfrak{S}_2^y$$

with an increasing number of y-values (exactly $r - 2$ values), which can be specified with a recursion formula. The also increasing number of related cyclic codes, these are $2, 5, 8, 12, 16, \ldots, 4 \cdot (r - 3)$ codes for each y-value of a given r had been laid out in a triangular scheme for reasons of clarity, as well as the related y-values.
Each cyclic code of this family can be understood as a Plotkin sum of two submodules of the $PSL(r, 2)$-Module $\mathbb{F}_2[\Omega]$. Therefore, the attributes of these codes can be predetermined. The relationship of these codes to their $r - 2$ automorphism groups was defined with a „lattice-grid-distance“ (German: „Verbandsraster-Abstand“), abbreviated $\mathcal{VRA}_{ba}$ of the submodules $\mathcal{U}_b \supseteq \mathcal{U}_a$ involved, which was introduced in the thesis.

Examples and graphics in the main text as well as an extensive set of tables in the appendix have been included to improve the understandability. This thesis is accompanied by a CD containing codes, automorphism groups, and listings as well as evaluation programs written in **Magma** for further analysis or research (e.g. isomorphics of codes).

Einleitung

Ziel dieser Arbeit ist es, die Automorphismengruppen von binären zyklischen Codes zu untersuchen.
Die zyklischen Codes sind die wichtigsten und am besten untersuchten linearen Codes, da die jeweiligen Codewörter der zu übertragenden Nutzinformation mit ihnen einfach zu erzeugen sind. Einige berühmte Codes, wie der *Golay-Code*, die Familie der *Hamming-Codes*, oder die *BCH-Codes* sind zyklische Codes. Darüberhinaus sind sie die Konstruktionsbasis für viele andere Codes – so z.B. die *Kerdock-, Preparata-* und *Justesen-Codes*.

Demgegenüber sind die Automorphismengruppen der binären zyklischen Codes bislang recht wenig untersucht worden; insbesondere fehlten konstruktive Aussagen über die Zusammensetzung dieser Gruppen.
Bevor weiter unten im Kapitel „Grundbegriffe“ eine Zusammefassung der in dieser Arbeit verwendeten Begriffe gegeben wird, seien hier bereits die beiden zentralen Begriffe aus dem Titel dieser Arbeit vorgestellt, nämlich „zyklischer Code“ und „Automorphismengruppe eines linearen Codes“. Darüberhinaus befindet sich am Ende dieser Arbeit ein Index.

Definition 0.1 (**Zyklischer Code**)
Ein binärer Code der Länge N ist eine Teilmenge $\mathcal{C}$ von $\mathbb{F}_2^N$.
Er heißt linear*, wenn er ein Untervektorraum von $\mathbb{F}_2^N$ ist. Er heißt* zyklisch*, wenn jede zyklische Verschiebung eines Codevektors ebenfalls ein Codevektor ist, d.h.,*

$$(c_1, c_2, \ldots, c_N) \in \mathcal{C} \Longrightarrow (c_N, c_1, c_2, \ldots, c_{N-1}) \in \mathcal{C}. \tag{1}$$

Dabei ist $\mathbb{F}_2$ der Körper mit den zwei Elementen 0 und 1.

Da die Automorphismengruppen für diese Arbeit von großer Bedeutung sind, sei deren Definition hier als nächstes aufgeführt (die symmetrische Permutationsgruppe von n Elementen wird in dieser Arbeit durchgängig mit $\mathfrak{S}_n$ bezeichnet):

Definition 0.2 (**Automorphismengruppe eines linearen Codes**)
Sei $x_1, \ldots, x_N$ die Standardbasis von $\mathbb{F}_2^N$.
Dann operiert die symmetrische Gruppe $\mathfrak{S}_N$ auf $\mathbb{F}_2^N$ wie folgt:

$$\sigma(\sum_{i=1}^{N} \lambda_i \cdot x_i) = \sum_{i=1}^{N} \lambda_i \cdot x_{\sigma(i)},\ (\sigma \in \mathfrak{S}_N,\ \lambda_i \in \mathbb{F}_2). \tag{2}$$

Sei $\mathcal{C} \subseteq \mathbb{F}_2^N$ *ein linearer Code. Dann ist die* Automorphismengruppe *von* $\mathcal{C}$ *definiert durch*

$$Aut(\mathcal{C}) := \{\sigma \in \mathfrak{S}_N \mid \forall c \in \mathcal{C} : \sigma(c) \in \mathcal{C}\}. \tag{3}$$

Bemerkung 0.3
Die Gruppe $Aut(\mathcal{C})$ kann man sich auch als Matrizengruppe, d.h. als Untergruppe von $GL(N, \mathbb{F}_2)$ vorstellen. Man bildet dabei $\sigma \in \mathfrak{S}_N$ auf die zu σ gehörige Permutationsmatrix ab.

Für die übrigen Begriffe sei auf das anschließende Kapitel „Grundbegriffe“ verwiesen.

Bei den Untersuchungen zu dieser Arbeit wurde die Möglichkeit genutzt, mit dem Computer-Algebra-Programmsystem **Magma** zyklische Codes kleiner Länge über dem Körper $\mathbb{F}_2$ und deren Automorphismengruppen zu berechnen.
Dies habe ich für sämtliche zyklischen Codes und sämtliche Automorphismengruppen der Codelängen $N \leq 70$ ausgeführt. Die relevanten Informationen habe ich in einem Listenwerk dokumentiert[1]. Dadurch wurden Regelmäßigkeiten sichtbar bei der Anzahl und Struktur der Codes und ihrer Automorphismengruppen. Um diese Regelmäßigkeiten zu verifizieren, wurden sporadisch auch Codelängen $N \geq 70$ gerechnet. Die identifizierten Automorphismengruppen wurden dann mit ihrer Bezeichnung, bzw. mit ihrer – bisweilen komplizierten – Produktdarstellung in einem Tabellenwerk zusammengefaßt. Dadurch wurden weitere Regelmäßigkeiten sichtbar.
Dabei ist die Identifikation einer Automorphismengruppe wegen der Erkennung der Einzelfaktoren und deren Verknüpfungen mitunter sehr schwierig; auch ihre vorherige Berechnung wird mit zunehmender Codelänge immer zeitaufwendiger bis unmöglich, bzw. stößt an die Computergrenzen.

Nach der Verifikation wurden einige gefundene Regelmäßigkeiten formuliert und bewiesen. Damit ist jetzt die Möglichkeit vorhanden, für eine gegebene Codelänge x die Existenz von zyklischen Codes mit ihren Attributen und den zugehörigen Automorphismengruppen mit ihrer Gruppenstruktur anzugeben (s. dazu auch Kap. 4 „Test“).

Warum beschäftigen wir uns überhaupt mit Automorphismengruppen von Codes?
Wir können damit konkret große endliche Permutationsgruppen konstruieren, die auf einer Menge von x Elementen transitiv operieren. Wir können die Struktur dieser Gruppen angeben, d.h., ihre Kompositionsfaktoren mit den z.T. unterschiedlichen Kompositionen. Schließlich lassen sich daraufhin auch die Ordnungen dieser Gruppen bestimmen.

Der Inhalt dieser Arbeit besteht aus dem bereits erwähnten Listenwerk mit seiner Vollständigkeit bis zur Codelänge $N = 70$, dem Tabellenwerk im Anhang, sowie dem Textteil, in dem die gefundenen Regelmäßigkeiten formuliert und bewiesen werden.

[1] Wegen des Umfangs ist das Listenwerk – zusammen mit den Dateien der Codes und Automorphismengruppen – auf der beiliegenden CD verfügbar.

Wegen des Umfangs dieser Informationen ist eine CD, auf der sich das Listenwerk – zusammen mit den Dateien der Codes und Automorphismengruppen, sowie einigen Auswertungsprogrammen befindet, als Bestandteil dieser Arbeit auf der dritten Umschlagseite zu finden.
Um die Navigation in dieser Arbeit zu erleichtern, ist neben dem Inhaltsverzeichnis nicht nur das Tabellenverzeichnis und der Index zu erwähnen, sondern ganz besonders die Tatsache, daß sich die vorliegende Dissertation auch als pdf-Datei auf der beiliegenden CD befindet, so daß man noch gezielter nach Begriffen, aber auch nach Zahlen, wie z.B. Gruppen-Ordnungen suchen kann.
Bevor wir die weiteren wichtigen Ergebnisse dieser Arbeit vorstellen, sei eine der Regelmäßigkeiten hier beispielhaft herausgegriffen. Dabei bezeichnen wir üblicherweise die linearen Codes mit ihren drei wesentlichen Attributen *Codelänge* N, *Dimension* k und *Minimaldistanz* d als $[N,k,d]$-Codes.

Satz 0.4 (**Zentraler Satz für zyklische Codes**)
Sei $N = a \cdot b$ eine Faktorenzerlegung mit $N, a, b \in \mathbb{N}$.
Dann existiert ein zyklischer $[N,a,b]$-Code mit der Automorphismengruppe

$$\mathfrak{S}_b \wr \mathfrak{S}_a,$$

sowie ein zyklischer $[N,b,a]$-Code mit der Automorphismengruppe

$$\mathfrak{S}_a \wr \mathfrak{S}_b.$$

Dabei wird das sogenannte Kranzprodukt (mit dem Verknüpfungszeichen „$\wr$“) eine entscheidende Rolle spielen. In der Literatur [15], [4], [11], sowie [5] werden verschiedene Arten von Kranzprodukten definiert und leider nicht immer einheitlich bezeichnet.
Wir benutzen hier ausschließlich das sog. **Permutations-Kranzprodukt** $\mathfrak{G} \wr \mathfrak{H}$, so wie es auch in **Magma** implementiert ist: Hierbei wird die Gruppe $\mathfrak{G}$ so oft in einem Kranz um die Gruppe $\mathfrak{H}$ herum angeordnet, wie die Kardinalität $|\Omega|$ der Menge Ω angibt, auf der $\mathfrak{H}$ transitiv operiert.

Die genaue Definition ist im anschließenden Kapitel „Grundbegriffe“ unter 0.31 gegeben.
Im Folgenden werde ich die weiteren Ergebnisse aufführen:

Satz 0.5 (**Erster Hauptsatz für zyklische Codes**)
Zu jedem technischen Übertragungsproblem, nämlich k Bits so zu übertragen, daß e Fehler korrigiert werden können, existiert ein zyklischer $[N,k,d]$-Code C_k, mit

$$d = 2e + 1 \quad \textit{und} \quad N = k \cdot d.$$

Die Automorphismengruppe von C_k ist

$$\mathfrak{S}_d \wr \mathfrak{S}_k,$$

das Erzeugerpolynom von C_k ist

$$g(x) = \sum_{i=0}^{d-1} x^{ik}$$

und das Kontrollpolynom von C_k ist

$$h(x) = 1 + x^k.$$

Der Satz und sein Beweis finden sich im Kapitel 2 unter der Nummer 2.13.

Satz 0.6 (**Zweiter Hauptsatz für zyklische Codes**)
Zu jedem technischen Übertragungsproblem, nämlich $k-1$ Bits so zu übertragen, daß e Fehler korrigiert und bis zu $2e+1$ Fehler erkannt werden können, existiert ein zyklischer $[N, k-1, 2d]$-Code C, mit $\dim(C) = k-1$ und $md(C) = 2d$, sowie

$$d = e + 1 \text{ und } N = k \cdot d.$$

Die Automorphismengruppe von C ist

$$\mathfrak{S}_d \wr \mathfrak{S}_k,$$

das Erzeugerpolynom von C ist

$$g(x) = \sum_{i=0}^{e} x^{ik} + x^{ik+1}$$

und das Kontrollpolynom von C ist

$$h(x) = \sum_{i=0}^{k-1} x^i.$$

Der Satz und sein Beweis finden sich im Kapitel 2 unter der Nummer 2.14.

Satz 0.7 (**Dritter Hauptsatz für zyklische Codes**)
Sei $N = a \cdot b$ eine Faktorenzerlegung mit $N, a, b \in \mathbb{N}$, wobei a und b nicht beide gleichzeitig kleiner als 5 sein dürfen.
Dann existieren ein zyklischer $[N, a, b]$-Code mit der Automorphismengruppe

$$\mathfrak{S}_b \wr \mathfrak{S}_a,$$

sowie ein zyklischer $[N, b, a]$-Code mit der Automorphismengruppe

$$\mathfrak{S}_a \wr \mathfrak{S}_b.$$

Es sei ferner $2 \neq a < b$ und a, b seien teilerfremd.
Dann gilt folgende Aussage:
Es gibt einen zyklischen $[N, a+b-1, a]$-Code mit der Automorphismengruppe

$$\mathfrak{S}_a \times \mathfrak{S}_b.$$

Die ersten beiden Aussagen bilden den **Zentralen Satz für zyklische Codes**, Teile 1 und 2; zum Beweis siehe Satz 2.19 und 2.2.
Die letzte Aussage beweisen wir allgemein im Satz 3.6 als ein Bestandteil des **Zentralen**

r	l	N	y
3	7	14	**3**
4	15	30	4 10
5	31	62	5 **15** 25
6	63	126	6 21 41 56
7	127	254	7 28 **63** 98 119
8	255	510	8 36 92 162 218 246
9	511	1022	9 45 129 **255** 381 465 501
10	1023	2046	10 55 175 385 637 847 967 1012
11	2047	4094	11 66 231 561 **1023** 1485 1815 1980 2035

Tabelle 1: Exponenten y der Automorphismengruppen $Aut(\mathcal{C}) \cong (\mathfrak{S}_2 \wr PSL(r,2))/\mathfrak{S}_2^y$, $l = 2^r - 1$, $N = 2 \cdot l$

Satzes für zyklische Codes, Teil 3 (Satz 3.3). Weitere Details hierzu findet man im Abschnitt 3 „Zusammenfassung zyklische Codes“.

Es wurde zusätzlich eine interessante Familie von zyklischen Codes und Automorphismengruppen im Zusammenhang mit den $PSL(r,2)-$Gruppen gefunden:

Satz 0.8
Sei $N = 2 \cdot (2^r - 1)$ mit $r \geq 3$. Dann existieren zyklische Codes der Länge N mit folgenden Automorphismengruppen:

$$\mathfrak{S}_2 \wr PSL(r,2) \quad \textit{und} \quad PSL(r,2) \wr \mathfrak{S}_2,$$

sowie $r-2$ Automorphismengruppen der Form eines „verminderten“[2] Kranzprodukts

$$(\mathfrak{S}_2 \wr PSL(r,2))/\mathfrak{S}_2^y,$$

wobei die Exponenten y rekursiv in einem Dreiecksschema ermittelt werden (s. Tabelle 1). Diese ausdividierten Normalteiler $\mathfrak{S}_2^y$ sind gleichzeitig Untermoduln der $PSL(r,2)$-Moduln $\mathbb{F}_2[\Omega]$ und repräsentieren selbst zyklische Codes der Länge $2^r - 1$ mit $PSL(r,2)$ als Automorphismengruppe. Dabei sind dann die y-Werte die Dimensionen dieser Codes.

Der Beweis stützt sich auf einen grundlegenden Aufsatz von Abdukhalikov [1].

Mit dem folgenden Fakt haben wir nun eine dritte Möglichkeit, um zyklische Codes zu erzeugen:

[2] Zur Konstruktion eines *verminderten Kranzprodukts* s.a. Def. 0.32.

Fakt 0.9
Sei $\mathfrak{Z}_N$ die zyklische Gruppe der Ordnung N.
Die Untermoduln des $\mathfrak{Z}_N$-Moduls $\mathbb{F}_2[\{1,2,\ldots,N\}]$ sind genau die zyklischen Codes der Länge N.

Der folgende fundamentale Satz stellt einen wichtigen und offensichtlichen Zusammenhang zwischen der Gruppe $\mathfrak{G} \leq \mathfrak{S}_N$ und der Automorphismengruppe $\mathrm{Aut}(C)$ eines von einem Untermodul des $\mathfrak{G}$-Moduls $\mathbb{F}_2[\{1,2,\ldots,N\}]$ erzeugten linearen Codes C dar:

Satz 0.10
Sei $\mathfrak{G} \leq \mathfrak{S}_N$ und $\Omega = \{1,2,\ldots,N\}$. Dann gilt:
Die Automorphismengruppen $Aut(C)$ der von den Untermoduln des $\mathfrak{G}$-Moduls $\mathbb{F}_2[\Omega]$ erzeugten linearen Codes C der Länge N genügen der Relation

$$\mathfrak{G} \leq Aut(C) \leq \mathfrak{S}_N. \tag{4}$$

Auch dieser Satz wird im Kapitel 9 bewiesen.

Im Zusammenhang mit den Code-Isomorphien (s. Kapitel 0.1) haben wir eine interessante Vermutung aufstellen können. Dazu müssen wir zwei Definitionen voranstellen. Dabei ist es sinnvoll, zunächst den „Anzahl“-Begriff zu präzisieren:
Ein zyklischer Code der Länge N ist ein Untervektorraum des $\mathbb{F}_2^N$, der invariant ist unter zyklischer Koordinatenpermutation.

Definition 0.11 (**Code-Isomorphie)**
Zwei lineare Codes $\mathcal{C}_1$, $\mathcal{C}_2 \subseteq \mathbb{F}_2^N$ heißen zueinander isomorph genau dann, wenn es eine Permutationsmatrix $\sigma \in \mathfrak{S}_N \leq GL(N,\mathbb{F}_2)$ gibt, mit $\sigma(\mathcal{C}_1) = \mathcal{C}_2$.

Dabei ist das Bild eines zyklischen Codes nicht notwendig wieder ein zyklischer Code.

Definition 0.12 (**Isomorphie-Faktor)**
Sei nun $\mathcal{C}_1$ ein zyklischer Code der Länge N. Die Menge aller zyklischen Codes, die zu $\mathcal{C}_1$ ismomorph sind, sei definiert als

$$Iso(\mathcal{C}_1) := \{C \in \mathbb{F}_2^N \mid C \cong \mathcal{C}_1\}. \tag{5}$$

Dann nennen wir $z := |Iso(\mathcal{C}_1)|$ den Isomorphie-Faktor *von $\mathcal{C}_1$.*

Dabei ist dieser Faktor anscheinend eine Eigenschaft der Automorphismengruppe $\mathrm{Aut}(\mathcal{C}_1)$: Auch alle weiteren Codes $C_x \ncong \mathcal{C}_1$ mit dieser Automorphismengruppe $Aut(\mathcal{C}_1) = Aut(C_x)$ treten in Paketen zu z isomorphen Codes auf (es wurden Werte bis $z = 60$ nachgewiesen).

Vermutung 0.13
Wir vermuten:

1. *Seien $\mathcal{C}_1 \ncong \mathcal{C}_2 \subseteq \mathbb{F}_2^N$ zwei zyklische Codes.*
   Die Anzahl der jeweils zu $\mathcal{C}_i$, $(i = 1,2)$ isomorphen zyklischen Codes ist eine invari-

ante Eigenschaft der zugehörigen Automorphismengruppe $Aut(\mathcal{C}_i)$, d.h., es gilt:

$$|Iso(\mathcal{C}_1)| = |Iso(\mathcal{C}_2)|, \text{ falls } Aut(\mathcal{C}_1) = Aut(\mathcal{C}_2) \tag{6}$$

2. *Sei $\mathcal{C} \in \mathbb{F}_2^N$ ein zyklischer Code. Falls*

$$Aut(\mathcal{C}) = \prod \mathfrak{G}_i, \text{ mit } \prod_i grad(\mathfrak{G}_i) = N, \tag{7}$$

wobei neben dem Kranzprodukt auch das direkte Produkt zur Bildung des Gruppenprodukts der $\mathfrak{G}_i$ zugelassen ist und $grad(\mathfrak{G}_i)$ den Permutationsgrad von $\mathfrak{G}_i$ bezeichnet, dann gilt:

$$z = |Iso(\mathcal{C})| = \prod_i |Iso(C_i)|, \text{ mit } Aut(C_i) = \mathfrak{G}_i. \tag{8}$$

oder mit anderen Worten:
Der Isomorphie-Faktor z einer Automorphismengruppe $Aut(\mathcal{C})$, die durch ein Gruppenprodukt der $\mathfrak{G}_i$ gebildet wird, ist das Produkt der Isomorphie-Faktoren z_i der einzelnen Produktgruppen $\mathfrak{G}_i$ und zwar egal, ob sie als direkte Produkte, Kranzprodukte, oder gemischte Produkte miteinander verknüpft sind.

Welche endlichen Gruppen tauchen nun allgemein als Automorphismengruppen der zyklischen Codes der Länge N auf?
Dabei bezeichnen wir in Anlehnung an die Syntax von **Magma** die Menge aller Permutationsgruppen, die transitiv auf der Menge $\Omega = \{1, 2, \ldots, N\}$ operieren,
mit $TransitiveGroups(N)$. Es gilt folgender

Fakt 0.14
Die Automorphismengruppen der zyklischen Codes der Länge N sind isomorph zu Permutationsgruppen $\mathfrak{G}_N \leq \mathfrak{S}_N$, die transitiv auf N Elementen operieren. Dabei gilt:

$$\{\mathfrak{G}_N\} \subsetneqq TransitiveGroups(N).$$

Man kann am Beispiel $N = 7$ leicht sehen, daß $\{\mathfrak{G}_N\}$ eine **echte** Teilmenge von $TransitiveGroups(N)$ ist[3]:
Es existieren für $N = 7$ genau 8 zyklische Codes – das sind 4 Codes und ihre jeweiligen dualen Codes. Da ein Code stets dieselbe Automorphismengruppe hat, wie sein dualer Code, kann es keinesfalls mehr als 4 verschiedene Automorphismengruppen geben (tatsächlich sind es nur zwei: $\mathfrak{S}_7$ und $PSL(3, 2)$).
Nun gibt es aber insgesamt 7 Permutationsgruppen, die auf der Menge $\Omega = \{1, 2, \ldots, 7\}$ transitiv operieren, d.h., mindestens 3 dieser Gruppen sind keine Automorphismengruppen von nichttrivialen zyklischen Codes der Länge $N = 7$ (dazu gehören u.a. die Gruppen $\mathfrak{Z}_7$, $\mathfrak{A}_7$, sowie die metazyklische Gruppe $\mathfrak{MZ}(7, 3)$).

[3] noch überzeugender mag das Beispiel $N = 24$ sein, mit 81 zyklischen Codes und 25000 transitiven Gruppen

Da außerdem folgende Inklusionskette gilt[4] (für eine bestimmte Codelänge N und alle Codes sind binär):

$$\{Zyklische\ Codes\} \subsetneqq \{Gruppencodes\} \subsetneqq \{Lineare\ Codes\} \subsetneqq \{Codes\}$$

ist einsehbar, daß transitive Gruppen existieren, die nicht als Automorphismengruppe eines zyklischen Codes auftreten, sondern (nach PHELPS [13]) als Automorphismengruppe eines nicht-zyklischen (ggfs. sogar nicht-linearen) Codes.
Um bei obigem Beispiel zu bleiben, existieren zur Codelänge $N = 7$ insgesamt 598 Gruppencodes (auf der Basis aller 96 Untergruppen der $\mathfrak{S}_7$ als jeweilige Startgruppe), davon sind also 590 nicht-zyklisch !
Von den insgesamt 15 zugehörigen Automorphismengruppen aller 598 Gruppencodes sind nur dieselben zwei Automorphismengruppen transitiv, wie bei den zyklischen Codes.
Während der Orientierungsphase zu dieser Arbeit wurden auch nicht-zyklische Gruppencodes bis zur Länge $N = 30$ (mit transitiven Gruppen als Startgruppen) untersucht. Dabei wurden aber durchaus Fälle beobachtet, bei denen auch solche transitive Gruppen als Automorphismengruppen von nicht-zyklischen Gruppencodes auftreten, die keine Automorphismengruppen von zyklischen Codes dieser Codelänge sind (Beispiel: $N = 22$, Startgruppe = $M22$, Automorphismengruppe = $M22$).
In diesem Zusammenhang sei abschließend aus Satz 0.10 noch eine Folgerung abgeleitet:

Folgerung 0.15
Sei $\mathfrak{G} \leq \mathfrak{S}_N$ die Startgruppe und $\mathbb{F}_2[\Omega]$ deren $\mathfrak{G}$-Modul mit $\Omega = \{1, \ldots, N\}$. Dann gilt:

$$|\mathfrak{G}| \leq |Aut(C)|,\ \forall C \subseteq \mathbb{F}_2[\Omega]. \tag{9}$$

d.h., die Ordnung der Automorphismengruppe eines Codes ist stets größer oder gleich der Ordnung der Startgruppe, mit der dieser Code erzeugt wird. Darüberhinaus gilt:

$$|\mathfrak{G}|\ \textit{teilt}\ |Aut(C)|,\ \forall C \subseteq \mathbb{F}_2[\Omega]. \tag{10}$$

Weitere Ergebnisse:

- Codelängen mit „gleichartiger“ Faktorenzerlegung haben dieselbe Anzahl nichttrivialer Codes, sowie dieselbe Anzahl und Typen von Automorphismengruppen (Beispiele: $N = 66$, 78, 110, aber nicht 102; $N = 35$, 77, 91, aber nicht 49, 63 oder 119; $N = 28$, 92, aber nicht 60 bzw. $N = 33$, 39, 55, 65, aber nicht 125).

- Tauchen bei einer Codelänge Gruppen $\mathfrak{G} \lneqq \mathfrak{S}_N$ (z.B. $PSL(r, s)$, $M23$, Metazyklische Gruppen) als Komponenten der Automorphismengruppen von zyklischen Codes auf, so existiert (falls N gerade) für diese Codelänge eine gerade Zahl zusätzlicher selbstdualer Codes (Details siehe Abschnitt 3.4 „Selbstduale Codes“).
  Wir bezeichnen diese Gruppen $\mathfrak{G}$ im Folgenden als „*Spezialgruppen*“. Darüberhinaus treten alle von diesen Spezialgruppen betroffenen zyklischen Codes in Paketen von 2, 4, 6, 18, 16, etc. isomorphen Codes auf (Details siehe Kapitel 0.1 „Isomorphien von Codes“, sowie Kapitel 9 „G-Moduln und lineare Codes“).

[4] zum Begriff der „Gruppencodes“ und der „Startgruppe“ siehe 0.20.

- Weitere Ergebnisse wurden erarbeitet im Zusammenhang mit der Zerlegung der Codelänge N in 3 (oder mehr) Faktoren. Wegen des Umfangs sei an dieser Stelle auf die Abschnitte
  3.2 „Zerlegung der Codelänge in 3 Faktoren“, sowie
  3.3 „Zerlegung der Codelänge in 4 Faktoren“ verwiesen.

- Das gleiche gilt für die Ergebnisse zur Vererbung (oder Fortpflanzung) von Eigenschaften der zyklischen Codes, sowie der Automorphismengruppen bei Vervielfachung der Codelänge (Details siehe Kapitel 2 „Vererbung von zyklischen Codes und ihren Automorphismengruppen“).

Diese Arbeit entstand im Anschluß an die Vorlesung „Kodierungstheorie“ von
Prof. Dr. Fritz Grunewald im Sommersemester 2004 [3].

Danksagungen

An dieser Stelle möchte ich mich bei folgenden Personen für ihre Unterstützung während der Anfertigung meiner Dissertation bedanken:

- meinem Doktorvater, Herrn Prof. Dr. Fritz Grunewald, HHU Düsseldorf – für das interessante Thema, die vielfältigen Anregungen und die fruchtbare Betreuung, sowie für die intensive Unterstützung bei der Beschaffung leistungsfähiger Rechner, ohne die uns viele interessante Ergebnisse verborgen geblieben wären.
  Er hat es verstanden, durch seine Art ein Klima zu schaffen, in dem die Balance in einem Magischen Dreieck aus Freiheit der Forschung, Ergebnisorientierung, sowie Motivation stets vorhanden war.

- Herrn Prof. Dr. Otto Kerner, HHU Düsseldorf – für die Bereitschaft, das erste Koreferat zu übernehmen.
  Seine klar gegliederte Vorlesung „Einführung in die Algebra“ ist ein willkommener Baustein in der Vorbereitung auf die mündliche Prüfung.

- Herrn PD Dr. Benjamin Klopsch, Royal Holloway University of London (HHU Düsseldorf bis Dez. 2006) – für die intensive Unterstützung bei Fragen der Gruppentheorie und **Magma**-Details, sowie für die Bereitschaft, das zweite Koreferat zu übernehmen. Darüberhinaus habe ich ihm viele nützliche Hinweise zu verdanken: Besonders in der Schlußphase ist auf seinen Rat hin noch manche Formulierung umgestellt worden – auch hat er mich auf eine Beweislücke aufmerksam gemacht.

- Frau Dr. Evija Ribnere, HHU Düsseldorf – für Antworten zu Fragen der Gruppentheorie und **Magma**-Details. Besonders in der Orientierungsphase war ihre Hilfe sehr aufbauend.

- Herrn Daniel Appel, M.Sc., HHU Düsseldorf – für das sorgfältige Korrekturlesen. Die Umsetzung seiner Änderungsvorschläge haben wesentlich zur Verbesserung der Lesbarkeit und Verständlichkeit dieser Arbeit beigetragen.

- Herrn Alfred E. Feuersänger, M.Sc. math. et phys., Framingham MA, USA – für intensive Literatur-Recherchen, sowie technische Informationen über Hamming-Codes und den Fehler-Korrektur-Prozeß. Auf seine langjährige Erfahrung habe ich gerne zurückgegriffen.

- Herrn Dipl.-Math. Bertold Nöckel, HHU Düsseldorf – für die Betreuung der **Magma**-LINUX-Systeme. Er hat nicht nur auf meinen Wunsch die jeweils neuesten **Magma**-Versionen besorgt und installiert, sondern auch die älteren Versionen verfügbar gehalten, was von großem Nutzen war (s. Anhang: „**Magma**-Besonderheiten“).

- meinen beiden Töchtern Anja und Sonja wegen ihres Verständnisses während der ganzen Zeit für die MAGNA CUM AETATE-Promotion ihres Vaters.
  Durch ihre Selbständigkeit habe ich mich voller Stolz ganz auf die Forschung für diese Arbeit konzentrieren können.

- meinen Eltern, die mich zeitlebens gefördert und gefordert haben. Leider hat meine Mutter das Ende meiner Arbeit nicht mehr erlebt; dafür hat mein Vater diese Art der Doppel-Unterstützung liebevoll und konsequent fortgesetzt.

- meiner lieben Frau Haike – post mortem, die vor fast 30 Jahren an der HHU ihr Mathematik-Diplom erwarb. Ich habe ihr sehr viel zu verdanken, besonders zu Beginn unseres gemeinsamen Mathematik-Studiums in Hannover 1965. Daher habe ich ihr diese Arbeit zu ihrem zehnten Todestag gewidmet.

Grundbegriffe

Es wird davon ausgegangen, daß der Leser mit den Grundzügen der Codierungstheorie vertraut ist, wie sie z.B. im Buch vom F. J. MacWilliams und N. J. A. Sloane [16] beschieben sind.
Dennoch halte ich es für sinnvoll, einige für diese Arbeit wesentliche Definitionen und Sätze zusammenzustellen.

Begriffe und Definitionen

Begriffe der Codierungstheorie

Als Standardliteratur habe ich das Buch von F. J. MacWilliams und N. J. A. Sloane [16] verwendet.
Grundsätzlich werden alle Codes in dieser Arbeit als binäre Codes, d.h., als Codes über dem Körper $\mathbb{F}_2$ betrachtet.

Definition 0.16 (**linearer Code)**
Sei K ein Körper und $N \in \mathbb{N}$.
Eine Teilmenge $\mathcal{C} \subseteq K^N$ heißt Code *der Länge N.*
Ein Untervektorraum $\mathcal{C} \subseteq K^N$ heißt linearer Code*. Seine Dimension $0 \leq k \leq N$ heißt* Dimension *des linearen Codes $\mathcal{C}$.*

Definition 0.17 (**Hamming-Abstand)**
Sei K ein Körper und $N \in \mathbb{N}$. Sei ferner $u, v \in K^N$. Dann heißt

$$d(u,v) := \left|\{i \mid u_i \neq v_i, (i = 1, \ldots, N)\}\right| \tag{11}$$

der Hamming-Abstand *von u und v.*

Definition 0.18 (**Minimaldistanz)**
Sei $\mathcal{C} \subseteq K^N$ ein Code. Dann heißt

$$md(\mathcal{C}) := min\{d(u,v) \mid u \neq v \in \mathcal{C}\} \tag{12}$$

die Minimaldistanz *von $\mathcal{C}$.*

Wir verwenden die folgende Schreibweise: $\mathcal{C}$ ist ein $[N, k, d]$-Code.
Dabei gilt: N ist die Länge, k die Dimension und d die Minimaldistanz des Codes $\mathcal{C}$.

Definition 0.19 (**Zyklischer Code**)
Ein Code $\mathcal{C}$ der Länge N heißt zyklisch*, wenn er linear ist und jede zyklische Verschiebung eines Codevektors ebenfalls ein Codevektor ist, d.h.,*

$$(c_1, c_2, \ldots, c_N) \in \mathcal{C} \Longrightarrow (c_N, c_1, c_2, \ldots, c_{N-1}) \in \mathcal{C}. \tag{13}$$

Bemerkung 0.20
Man kann zyklische Codes der Länge N als einen Spezialfall der *Gruppencodes* betrachten: Hierbei wird die zyklische Gruppe $\mathfrak{Z}_N$ als sog. *Startgruppe* genommen. Dabei bildet der *Erzeugungsvektor* $v \in \mathbb{F}_2^N$ zusammen mit allen $\sigma \cdot v, \sigma \in \mathfrak{Z}_N$ eine Basis des Untervektorraums $C \subseteq \mathbb{F}_2^N$. Gruppencodes sind ebenfalls lineare Codes, bei denen aber auch nicht-zyklische Gruppen als Startgruppe zur Konstruktion der Codes verwendet werden. Zur genauen Definition der Gruppencodes und *Gruppenalgebren* sei auf die Literatur verwiesen, z.B. MacWilliams [16] Ch5, §3.

Definition 0.21 (**Erzeugungsvektor**)
Unter allen mögliche Vektoren $v \in \mathbb{F}_2^N$, die zusammen mit allen $\sigma \cdot v, \sigma \in \mathfrak{Z}_N$ eine Basis des Untervektorraums $C \subseteq \mathbb{F}_2^N$ bilden, zeichnen wir genau einen Vektor Ev als
den Erzeugungvektor *aus, für den gilt:*

$$Ev < v, \forall v \in C. \tag{14}$$

Bemerkung 0.22
Dies begeutet, daß der Erzeugungsvektor Ev stets mit einer „1“ an niedrigster Stelle beginnt – genauso, wie das mit Ev verwandte Erzeugerpolynom $g(x)$ stets den Term „+1“ besitzt und daher den kleinsten Polynomgrad unter allen möglichen Polynomen zur Erzeugung eines Codevektors $c \in C$ hat.

Definition 0.23 (**Automorphismengruppe eines linearen Codes**)
Sei $x_1, \ldots, x_N$ die Standardbasis von $\mathbb{F}_2^N$.
Dann operiert die symmetrische Gruppe $\mathfrak{S}_N$ auf $\mathbb{F}_2^N$ wie folgt:

$$\sigma(\sum_{i=1}^{N} \lambda_i \cdot x_i) = \sum_{i=1}^{N} \lambda_i \cdot x_{\sigma(i)}, \ (\sigma \in \mathfrak{S}_N, \ \lambda_i \in \mathbb{F}_2) \tag{15}$$

Sei $\mathcal{C} \subseteq \mathbb{F}_2^N$ ein Untervektorraum, d.h. ein linearer Code. Dann ist die Automorphismengruppe *von $\mathcal{C}$ definiert durch*

$$Aut(\mathcal{C}) := \{\sigma \in \mathfrak{S}_N \mid \forall c \in \mathcal{C} : \sigma(c) \in \mathcal{C}\}. \tag{16}$$

Bemerkung 0.24
Die Gruppe $Aut(\mathcal{C})$ kann man sich auch als Matrizengruppe, d.h. als Untergruppe von $GL(N, \mathbb{F}_2)$ vorstellen. Man bildet dabei $\sigma \in \mathfrak{S}_N$ auf die zu σ gehörige Permutationsmatrix ab.

Definition 0.25 (**trivialer Code im Sinne dieser Arbeit**)
Als trivialen Code im Sinne dieser Arbeit wollen wir einen Code $\mathcal{C}$ der Länge N bezeichnen, für dessen Automorphismengruppe $Aut(\mathcal{C})$ gilt:

$$Aut(\mathcal{C}) = \mathfrak{S}_N, \quad oder \quad Aut(\mathcal{C}) = \mathfrak{A}_N, \quad oder \quad Aut(\mathcal{C}) \quad ist\ auflösbar \tag{17}$$

An dieser Stelle möchte ich erwähnen, daß die alternierende Gruppe $\mathfrak{A}_N$ im gesamten Untersuchungsbereich nie als Automorphismengruppe in Erscheinung trat.

Definition 0.26 (**Rohcodes**)
Als zyklische Rohcodes *bezeichnen wir alle*[5] *zyklischen Codes einer Länge N. Das heißt, die Rohcodes sind die Vereinigung aus trivialen und nichttrivialen Codes im Sinne dieser Arbeit (abgekürzt: „iSdA“).*

Dabei ist es sinnvoll, den „Anzahl“-Begriff zu präzisieren:
Ein zyklischer Code der Länge N ist ein Untervektorraum des $\mathbb{F}_2^N$, der unter zyklischer Koordinatenpermutation invariant bleibt.

Im Gegensatz zu vielen anderen Familien von fehlerkorrigierenden Codes existieren zyklische Codes für jede beliebige Codelänge. Das ist für die technische Realisierung sicherlich von Nutzen.
Einige berühmte Codes, wie die *Hamming-Codes*, oder der *Golay-Code* sind zyklisch.
Man kann die zyklischen Codes auf drei Arten betrachten und auch so erzeugen:

1. als Gruppencodes zu der zyklischen Gruppe $\mathfrak{Z}_N$ mit je einem Erzeugungsvektor v aus dem Umgebungsraum $\mathbb{F}_2^N$. Zu jedem Code C gehört eine Generatormatrix G_C (zur Transformation eines Informationsvektors in einen Codevektor) und eine Kontrollmatrix H_C (zur Fehlerkorrektur).

2. als algebraische Codes aus Produktkombinationen der Wurzeln des Kreisteilungspolynoms $X^N - 1$ in dem Quotientenring $\mathbb{F}_2[X]/(X^N - 1)$. Zu jedem Code C gehört ein Generatorpolynom (oder „Erzeugerpolynom“) $g(x) \in \mathbb{F}_2[X]/(X^N - 1)$ (die Koeffizienten des Generatorpolynoms sind genau die Elemente des obigen Erzeugungsvektors), sowie ein Kontrollpolynom $h(x) \in \mathbb{F}_2[X]/(X^N - 1)$. Auch hier wird durch Multiplikation eines „Informationspolynoms“ mit dem Generatorpolynom das „Codepolynom“ gebildet, welches später (nach der Übertragung) durch Multiplikation mit dem Kontrollpolynom einer Prüfung und ggfs. Korrektur unterzogen wird.

3. als Untermoduln des $\mathfrak{Z}_N$-Moduls $\mathbb{F}_2[\Omega]$, mit $\Omega = \{1, 2, \ldots, N\}$ (s. dazu Fakt 9.2).

Alle 3 Arten der Erzeugung sind für diese Arbeit verwendet worden.

Definition 0.27 (**dualer Code**)
Sei $C \in \mathbb{F}_2^N$ ein zyklischer Code. Dann heißt

$$C^\perp := \{u \in \mathbb{F}_2^N \mid \forall c \in C : u \cdot c = 0\} \tag{18}$$

der duale Code *zu C.*

[5] inklusive evtl. vorhandener isomorphen Codes

Für spätere Aussagen und Beweise benötigen wir noch das folgende allgemeine Lemma:

Lemma 0.28
Sei $C \in \mathbb{F}_2^N$ ein zyklischer Code. Dann gilt:
Der zu C zugehörige duale Code $C^\perp$ ist zyklisch und es gilt:

$$Aut(C) = Aut(C^\perp). \tag{19}$$

Zusatz: Wenn C ein $[N,k]$ - Code ist, so ist $C^\perp$ ein $[N, N-k]$ - Code.

Beweis. Nach MacWilliams [16] Ch7, §5, Theorem 4 ist der zu C zugehörige Code $C^\perp$ zyklisch.
Den Zusatz findet man in van Lint [8] §3.2.
Es ist noch zu zeigen: $Aut(C) = Aut(C^\perp)$.
Sei H eine Kontrollmatrix von C. Für jede Permutation $\varphi \in Aut(C)$ und für jeden Codevektor $c \in C$ gilt:

$$H * c = 0 = H * \varphi(c) = \varphi(H) * c. \tag{20}$$

Also ist $\varphi(H)$ ebenfalls eine Kontrollmatrix für C. Da mit H auch $\varphi(H)$ gleichzeitig eine Generatormatrix für $C^\perp$ ist, folgt daraus die Behauptung. □

Diese Erkenntnis hat sich positiv auf die Durchlaufzeit der **Magma**-Programme zur Ermittlung der zyklischen Gruppencodes ausgewirkt, so daß doppelt so große Codelängen behandelt werden konnten, wie wenn man sämtliche Vektoren eines Vektorraums als Startvektor für einen Gruppencode untersuchen muß.

Zum besseren Verständnis sei an dieser Stelle an folgende Zusammenhänge erinnert:

Fakt 0.29
Das Generatorpolynom g_C eines zyklischen Codes C ist das Kontrollpolynom $h_{C^\perp}$ des dualen Codes $C^\perp$.
Das Kontrollpolynom h_C eines zyklischen Codes C ist das Generatorpolynom $g_{C^\perp}$ des dualen Codes $C^\perp$.
Diese Aussagen gelten sinngemäß auch für die Generatormatrizen und die Kontrollmatrizen von C bzw. $C^\perp$.
Sei $k = \dim(C)$ = Zeilenzahl der Generatormatrix von C. Dann gilt:

$$grad(g_C) = N - k = \dim(C^\perp) = grad(h_{C^\perp})$$

$$grad(h_C) = k = \dim(C) = grad(g_{C^\perp})$$

Beweis. Diese Aussagen werden in der Standardliteratur bewiesen, siehe z.B. [16] □

Begriffe der Gruppentheorie

Als Standardliteratur habe ich das Buch von B. Huppert [4] verwendet.
Neben den Bezeichnungen für die symmetrischen, alternierenden und zyklischen Gruppen $\mathfrak{S}_n, \mathfrak{A}_n, \mathfrak{Z}_n$, die auf der Menge Ω operieren, mit $|\Omega| = n$, werden wir auch einigen Spezialgruppen begegnen, deren Bezeichnung nicht immer eindeutig ist. Dabei bedeutet:

- $\mathfrak{K}_4$: Klein'sche Vierergruppe
- $M23$: Mathieu-Gruppe für $|\Omega| = 23$; analog: $M22$
- $\mathfrak{Z}_N$: zyklische Gruppe der Ordnung N
- $\mathfrak{MZ}(p,q)$: metazyklische pq-Gruppe (q teilt $p-1$, p prim) $\mathfrak{MZ}(p,q) \cong \mathfrak{Z}_p \rtimes \mathfrak{Z}_q$
- $PSL(r,s) = L(r,s) = A(r-1,s) \cong SL(r,s)$: Projektive Spezielle Lineare Gruppe (dabei gilt „$\cong SL(r,s)$“ nur für $s = 2$, was aber hier wegen $\mathbb{F}_2$ erfüllt ist.)

Definition 0.30 (**transitive Permutationsgruppe)**
Eine Permutationsgruppe $\mathfrak{G}$ heißt transitiv*, wenn ihre Permutationen jedes Element der Menge, auf der $\mathfrak{G}$ operiert, in jedes (andere) Element der Menge überführt.*

Wie bereits in der Einleitung erwähnt, wird das sogenannte Kranzprodukt in dieser Arbeit eine entscheidende Rolle spielen. In der Literatur [15], [4], [11], sowie [5] werden verschiedene Arten von Kranzprodukten definiert und leider nicht immer einheitlich bezeichnet. Wir benutzen hier ausschließlich das sog. **Permutations-Kranzprodukt**, so wie es auch in **Magma** implementiert ist und nennen es der Einfachheit halber „Kranzprodukt“.
Wir wollen daher dessen Definition hier voranstellen [4]:

Definition 0.31 (**Kranzprodukt)**
Sei $\mathfrak{G}$ eine Gruppe und $\mathfrak{H}$ eine (nicht notwendig transitive) Permutationsgruppe auf der endlichen Ziffernmenge Ω. Unter dem Kranzprodukt $\mathfrak{G} \wr \mathfrak{H}$ *von $\mathfrak{G}$ mit $\mathfrak{H}$ (wreath-product im Englischen) verstehen wir die Menge*

$$\{(f,H) | H \in \mathfrak{H},\ f \text{ Abbildung von } \Omega \text{ in } \mathfrak{G}\},$$

versehen mit der Multiplikation

$$(f_1, H_1)(f_2, H_2) = (g, H_1 H_2)$$

mit $g(i) = f_1(i) f_2(i^{H_1})$ für $i \in \Omega$.

Eine gute Erklärung mit Beispiel findet man in [15] Chapter 7, Wreath Products:
Hier wird zur Veranschaulichung[6] an den Endpunkten einer (zentralen) regelmäßigen geometrischen Figur (z.B. ein Stern) jeweils die Kopie eines weiteren (äußeren) geometrischen Gebildes angehängt (dadurch entsteht der Kranz). Die innere Figur entspricht der Menge Ω, auf der die Permutationsgruppe $\mathfrak{H}$ operiert, das äußere Gebilde entspricht der Menge, auf der die Gruppe $\mathfrak{G}$ operiert (in unserem Fall ist $\mathfrak{G}$ ebenfalls eine Permutationsgruppe).

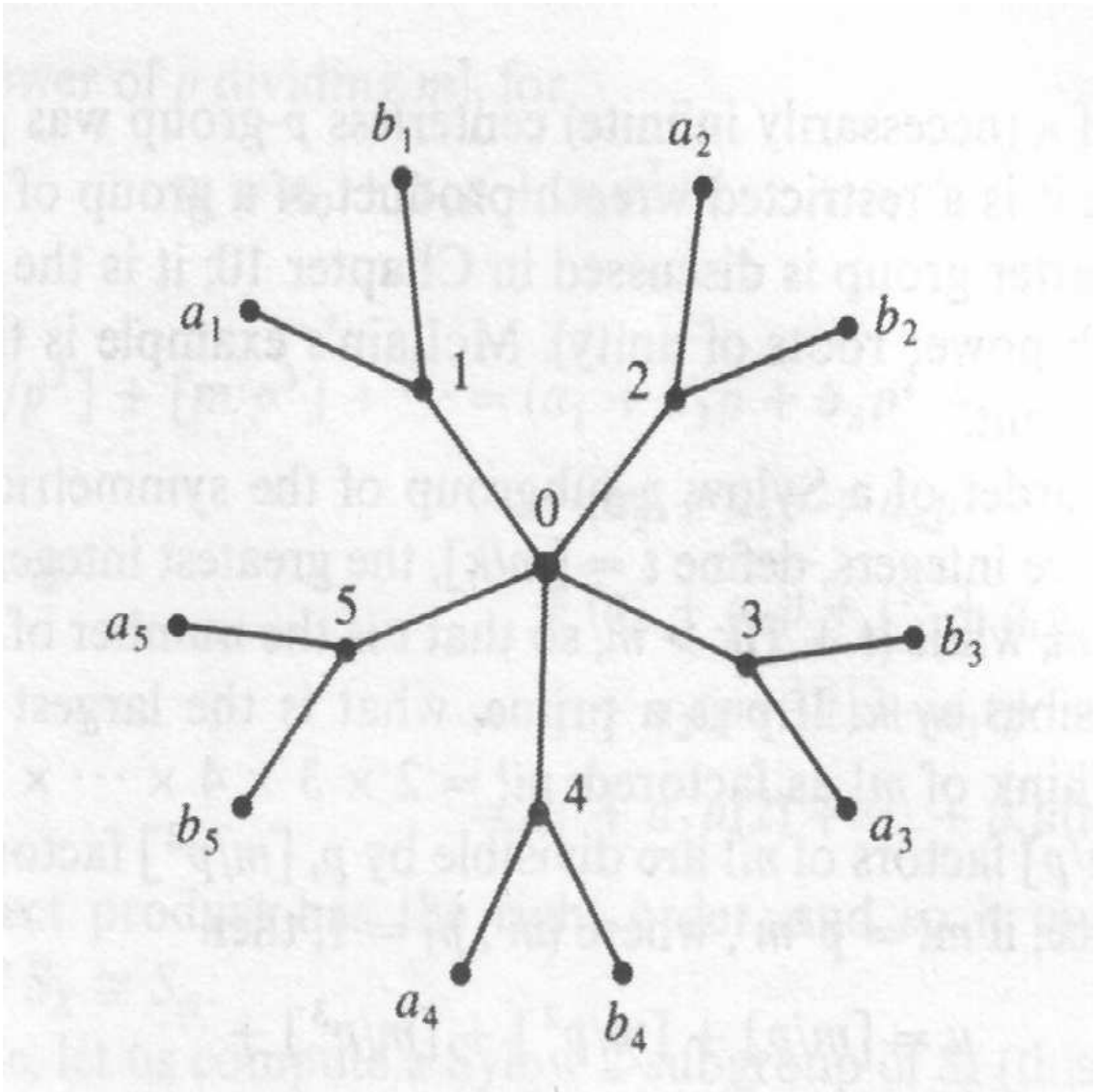
[6] s. Bild auf der nächsten Seite, Momentaufnahme des permutierenden Gruppenkranzes $\mathfrak{S}_2 \wr \mathfrak{S}_5$

Bei der Kranzproduktbildung durchlaufen die $|\Omega|$ äußeren Gebilde auf dem Kranz jeweils für sich alle durch $\mathfrak{G}$ definierten Gruppenoperationen (bei uns: Permutationen), das sind $|\mathfrak{G}|^{|\Omega|}$ Möglichkeiten. Darüberhinaus durchläuft die innere zentrale Figur zusätzlich noch alle Permutationen der Permutationsgruppe $\mathfrak{H}$.
Die formale Produktbildung bei diesem (auch Gruppenkranz genannten) Kranzprodukt erfolgt – um bei diesem Bild zu bleiben – von außen nach innen[7], also:

$$\mathfrak{G} \wr \mathfrak{H}.$$

Dabei ist die Operation $\wr$ assoziativ, aber nicht kommutativ, denn

$$|\mathfrak{G} \wr \mathfrak{H}| = |\mathfrak{G}|^{|\Omega|} \cdot |\mathfrak{H}|.$$



Momentaufnahme des permutierenden Gruppenkranzes $\mathfrak{S}_2 \wr \mathfrak{S}_5$

[7] d.h., in der Schreibweise $\mathfrak{G} \wr \mathfrak{H}$ von links nach rechts, bzw. in den **Magma**-Kompositionslisten von unten nach oben

Definition 0.32 (**vermindertes Kranzprodukt**)
(dies wird im Abschnitt 5.3 näher beschrieben)
Sei G eine Gruppe, die auf einer Menge $\Omega := \{1, \ldots, n\}$ operiert ($n \in \mathbb{N}$). Sei $\mathbb{F}_2[\Omega]$ der zugehörige Permutationsmodul. Ist $\mathfrak{S}_2 \wr G$ das zugehörige Kranzprodukt, so gibt es einen offensichtlichen Gruppenisomorphismus:

$$\mathfrak{S}_2 \wr G \cong \mathbb{F}_2[\Omega] \rtimes G \tag{21}$$

Ist $U \subseteq \mathbb{F}_2[\Omega]$ ein G-Untermodul, so ist U ein Normalteiler in $(2) \wr G$. Den Quotienten

$$\mathfrak{S}_2 \wr G \ /U \tag{22}$$

nenne ich vermindertes Kranzprodukt.

Dabei operiert G auf $U \subseteq \mathbb{F}_2[\Omega]$ durch die Aktion auf der Index-Menge $\{1, 2, \ldots, n\}$.
In einigen Fällen (s. z.B. Kap. 10, Abschnitt 10.2) existieren Codes $\mathcal{C}$ der Länge $N = 2 \cdot n$, deren Automorphismengruppe ein semidirektes Produkt[8] des Untermoduls $\overline{U}$ mit der Gruppe G ist:

$$Aut(\mathcal{C}) = \overline{U} \rtimes G. \tag{23}$$

Wegen der Konstruktion des G-Moduls $\mathbb{F}_2[\Omega]$ und des obigen Gruppenisomorphismus gilt nun folgende Isomorphie:

$$Aut(\mathcal{C}) = \overline{U} \rtimes G \cong \mathfrak{S}_2 \wr G \ /U \cong (\mathfrak{S}_2 \wr G)/\mathfrak{S}_2^y, \quad y = \dim(U). \tag{24}$$

Diese verminderten Kranzprodukte sind für uns besonders wichtig, weil eine große Anzahl von Automorphismengruppen von zyklischen Codes gerader Länge (z.B. $N = 42$, s. Tabellenwerk) so dargestellt werden kann.

Definition 0.33 (**Kardinalität**)
Operiert eine Gruppe $\mathfrak{G}$ auf einer Menge Ω, so heißt $|\Omega|$ die Kardinalität *von Ω.*

Die Kardinalität von Ω ist von großer Bedeutung bei der Konstruktion (z.B. mit **Magma**) eines Kranzprodukts, wie auch eines direkten Produktes, da eine bestimmte Gruppe durchaus auf Mengen unterschiedlicher Kardinalität operieren kann.

Beispiel 0.34
So operiert die Gruppe $\mathfrak{Z}_2$ als Untergruppe von $\mathfrak{S}_4$ (intransitiv) auf einer Menge Ω der Kardinalität 4.
Operiert die Gruppe $\mathfrak{Z}_2$ hingegen auf einer Menge Θ von 2 Elementen (transitiv), so hat Θ die Kardinalität 2.

Auch bei gemischten Produkten muß man sehr vorsichtig sein:
So identifizieren wir für die 5. Automorphismengruppe zur Codelänge $N = 15$:

[8] s. Kap. 5: „Das semidirekte Gruppenprodukt“

$G5 = \mathfrak{S}_3 \times \mathfrak{S}_5$ und laut **Magma** operiert diese Gruppe auf einer Menge der Kardinalität 15. Konstruieren wir diese Gruppe selbst (z.B. zur Isomorphieüberprüfung), stellen wir fest, daß diese Gruppe offenbar natürlicherweise auf einer Menge der Kardinalität 8 operiert:

```
> T5:=DirectProduct(Sym(3),Sym(5));
> T5;
Permutation group T5 acting on a set of cardinality 8
```

Man sagt in diesem Zusammenhang auch: „T5 hat den **Permutationsgrad** 8“.
Nun gilt zwar noch $G5 \cong T5$, aber spätestens bei der Konstruktion von $\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_5)$ mit **Magma** gelangen wir zu völlig unterschiedlichen Gruppen.

Definition 0.35 (**modularer Verband)**
Eine nichtleere Menge V von Elementen $a, b, \ldots$ heißt ein Verband*, wenn je zwei Elementen $a, b \in V$ die Elemente $a \cap b$ und $a \cup b$ aus V eindeutig zugeordnet sind, so daß die folgenden Gesetze (Kommutativ-Gesetz, Assoziativ-Ges., Verschmelzungs-Ges.) gelten:*

$$\begin{aligned} a \cap b &= b \cap a, \\ a \cup b &= b \cup a, \\ a \cap (b \cap c) &= (a \cap b) \cap c, \\ a \cup (b \cup c) &= (a \cup b) \cup c, \\ a \cap (a \cup b) &= a, \\ a \cup (a \cap b) &= a. \end{aligned}$$

Man kann eine Beziehung $a \subseteq b$ einführen durch $a \cap b = a$. Damit wird V zu einer halbgeordneten Menge, d.h., zu $a, b \in V$ existiert stets mit $a \cap b$ ein Infimum *und mit $a \cup b$ ein* Supremum.
Ein Verband V heißt modular*, falls für beliebige Elemente $a, b, c \in V$ gilt:*
Wenn $a \subseteq c$, so gilt $a \cup (b \cap c) = (a \cup b) \cap c$ (modulares Gesetz).

Beispiele für Verbände:

1. Die Untergruppen einer Gruppe bilden einen Verband; insbesondere bilden die Automorhismengruppen der zyklischen Codes der Länge N einen Teilverband des Untergruppenverbands der symmetrischen Gruppe $\mathfrak{S}_N$.

2. Die Unterräume eines Vektorraums bilden einen modularen Verband bezüglich der Inklusion als Halbordnung. Das gilt insbesondere für lineare Codes.

0.1 Isomorphien von Codes

Während der Untersuchungen zu dieser Arbeit fiel mir auf, daß bei einigen Codelängen – und dort auch nur bei einigen Automorphismengruppen – zyklische Codes mit denselben Attributen (N, k, d) auftraten. Eine Überprüfung mit **Magma** ergab, daß sie isomorph sind (s. Abschnitt 3.4).
Wir wollen daher zunächst die Code-Isomorphie definieren:

Definition 0.36 (**Code-Isomorphie)**
Zwei lineare Codes $\mathcal{C}_1$, $\mathcal{C}_2 \subseteq \mathbb{F}_2^N$ heißen zueinander isomorph genau dann, wenn es eine Permutationsmatrix $\sigma \in \mathfrak{S}_N \leq GL(N, \mathbb{F}_2)$ gibt, mit $\sigma(\mathcal{C}_1) = \mathcal{C}_2$, oder in Zeichen:

$$\mathcal{C}_1 \cong \mathcal{C}_2 :\Longleftrightarrow \exists \sigma \in \mathfrak{S}_N \leq GL(N, \mathbb{F}_2) : \sigma(\mathcal{C}_1) = \mathcal{C}_2. \tag{25}$$

Man überzeugt sich leicht, daß neben der Code-Isometrie[9] der beiden Codes insbesondere gilt $Aut(\mathcal{C}_1) = Aut(\mathcal{C}_2)$.

Bei der Untersuchung der Codes im Kapitel 8 und 10 haben wir ebenfalls Code-Isomorphien beobachtet und daraufhin auch die übrigen bereits gerechneten Codes überprüft. Wir kommen dabei zu folgendem Ergebnis:

- Zyklische Codes mit Spezialgruppen $G \lneqq \mathfrak{S}_n$ als Automorphismengruppe oder als Faktor(en) in den hier (in dieser Arbeit) beschriebenen Gruppenprodukten der Automorphismengruppe haben isomorphe Codes.
  Das ist nach obiger Definition und dem unten bewiesenen Satz 0.38 einleuchtend, denn es existieren Permutationen $\sigma \in \mathfrak{S}_N$, die keine Permutationen von G sind; d.h., diese Abbildungen sind keine Automorphismen, sondern (nur) Isomorphismen.

- Je nach Typ der Spezialgruppe $Aut(\mathcal{C})$ existieren 2, 4, 6, 8, oder auch mehr (bis 60 nachgewiesen) isomorphe Codes. Wir nennen diesen Faktor den *Isomorphie-Faktor*, oder kurz: den *Iso-Faktor*.

- Dabei wurde festgestellt, daß alle Codes, die zu einer solchen Gruppe als Automorphismengruppe gehören, jeweils dieselbe Anzahl von isomorphen Doubletten haben. Das heißt, daß der Iso-Faktor offenbar eine invariante Eigenschaft der Automorphismengruppe ist.

- Eine Technik wurde dabei beobachtet: isomorphe Codes haben jeweils stets einen Zwilling, dessen signifikanter Teil des Erzeugungsvektors genau das Spiegelbild des anderen Codes darstellt.

Wir formulieren aus den Beobachtungen die ersten Aussagen:

Fakt 0.37
Für Codes $\mathcal{C}_1$, $\mathcal{C}_2$ gilt: $\mathcal{C}_1 \cong \mathcal{C}_2 \Leftrightarrow \mathcal{C}_1^\perp \cong \mathcal{C}_2^\perp$.

[9] d.h., $N_1 = N_2, k_1 = k_2$ und $d_1 = d_2$

Satz 0.38
Sei $\mathcal{C} \in \mathbb{F}_2^N$ ein zyklischer Code. Falls
$Aut(\mathcal{C}) = \wr_i \mathfrak{S}_i$, mit $\prod_i i = N$, $i \in I$,
d.h., falls wir nur symmetrische Gruppen als Kranzfaktoren der Automorphismengruppe von $\mathcal{C}$ haben, so existiert zu $\mathcal{C}$ kein isomorpher Code.

Beweis. Widerspruchsannahme: Es existiert ein Code $\mathcal{C}_x \neq \mathcal{C}$ mit $\mathcal{C}_x \cong \mathcal{C}$. Dann muß es nach unseren Untersuchungen (s. Kap. 2) ein Paar von elementaren Teilcodes $\mathcal{B}_x \neq \mathcal{B}$ von $\mathcal{C}_x$ bzw, $\mathcal{C}$ geben, mit $\mathcal{B}_x \cong \mathcal{B}$ und mit $Aut(\mathcal{B}_x) = Aut(\mathcal{B}) = \mathfrak{S}_n$, $n \in I$. Nach obiger Definition der Code-Isomorphie existiert ein $\sigma \in \mathfrak{S}_n \leq GL(n, \mathbb{F}_2)$ mit $\sigma(\mathcal{B}_x) = \mathcal{B}$. Da $\mathfrak{S}_n$ gleichzeitig als Automorphismengruppe von $\mathcal{B}$ und $\mathcal{B}_x$ vorausgesetzt war und $\sigma \in \mathfrak{S}_n$, muß σ also ein Automorphismus sein und somit gilt $\mathcal{B}_x = \mathcal{B}$ im Widerspruch zur Annahme.
$\mathcal{B}$ (und damit dann auch $\mathcal{C}$) ist also nur zu sich selbst isomorph. □

Als Folge davon wurde beobachtet, daß der signifikante Teil des jeweiligen Erzeugungsvektors für derartige Codes spiegelsymmetrisch ist, d.h., ein Spiegelbild zu sich selbst.

Nach den Unteruchungen zu dieser Arbeit besteht Anlaß zu der folgenden

Vermutung 0.39
Sei $\mathcal{C} \in \mathbb{F}_2^N$ ein zyklischer Code. Falls
$Aut(\mathcal{C}) = \prod \mathfrak{S}_i$, mit $\prod_i i = N$, $i \in I$,
d.h., falls wir nur symmetrische Gruppen als Faktoren der Automorphismengruppe von $\mathcal{C}$ haben, so existiert zu $\mathcal{C}$ kein isomorpher Code.
Dabei ist neben dem Kranzprodukt auch das direkte Produkt zur Produktbildung von Gruppenprodukten möglich.

Für das semidirekte Produkt haben wir bereits ein Gegenbeispiel:
Die vierte Automorphismengruppe zur Codelänge $N = 15$, nämlich $\mathfrak{Z}_3 \rtimes \mathfrak{S}_5$, hat den Iso-Faktor 2.

Weiterhin wurde beobachtet, daß sich bei zyklischen Codes mit mehreren Spezialgruppen $G_i \lneqq \mathfrak{S}_n$ als Faktoren in den hier weiter oben beschriebenen Gruppenprodukten der Automorphismengruppe die Iso-Faktoren offenbar multiplizieren: Anstoß gab die Automorphismengruppe $PSL(3,2) \wr PSL(3,2)$ für $N = 49$ mit dem Iso-Faktor 4.
Da $PSL(3,2)$ für sich allein den Iso-Faktor 2 hat, war noch nicht klar, ob sich die Faktoren addieren, multiplizieren, oder gar potenzieren. Die kleinste Codelänge zu einer Spezialgruppe mit einem Iso-Faktor $\neq 2$ ist 31 mit der Gruppe $PSL(5,2)$ und dem Iso-Faktor 6. So wurden die ersten 1500 Codes (von $2097152 = 2^{21}$) der Länge 217 ($= 7 \cdot 31$) gerechnet und die Automorphismengruppe $PSL(3,2) \times PSL(5,2)$ gefunden – mit einem Iso-Faktor von $12 = 2 \cdot 6$. Ein Kranzprodukt dieser beiden Spezialgruppen war noch nicht dabei.
Die Ordnung von $PSL(3,2) \wr PSL(5,2)$ ist
$9650724940120547497073791938378043225118689073940554304725457149198094827520$.

Die Ordnung von $PSL(5,2) \wr PSL(3,2)$ ist
167924750449146691926241999658293769722134528000000 0.

Durch die von mir entwickelte Technik, Codes als Untermoduln von $\mathbb{F}_2[\Omega]$ zu erzeugen, konnte danach der $PSL(5,2) \wr PSL(3,2)$-Modul erzeugt und unter den 30 seiner Untermoduln ein $[217, 38, 16]$-Code (und der duale $[217, 179, 4]$-Code) gefunden werden, die beide die Automorphismengruppe $PSL(5,2) \wr PSL(3,2)$ haben. Daraufhin habe ich in einem zweiten Schritt auf algebraischen Weg alle zyklischen Codes mit vorgegebener Dimension und Minimaldistanz abgespeichert. Hier nun das interessante Ergebnis:
Von 2097152 Codes der Länge 217 gibt es genau zwölf $[217, 38, 16]$**-Codes und alle zwölf haben die Automorphismengruppe** $PSL(5,2) \wr PSL(3,2)$**!**
Leider war **Magma** nicht mehr in der Lage, die Isomorphie dieser 12 Codes zu überprüfen, aber es sind alle notwendigen Kriterien erfüllt.
Damit scheidet die oben in Erwägung gezogene Potenzierung der Iso-Faktoren bei Kranzprodukten aus und wir können jetzt die folgende fundierte Vermutung (s. auch 0.13) formulieren.
Zunächst wollen wir noch den oben eingeführten Isomorphie-Faktor präziser definieren:

Definition 0.40 (**Isomorphie-Faktor)**
Sei $\mathcal{C}_1$ ein zyklischer Code der Länge N.
Die Menge aller zyklischen Codes, die zu $\mathcal{C}_1$ ismomorph sind, sei definiert als

$$Iso(\mathcal{C}_1) := \{C \subseteq \mathbb{F}_2^N \mid C \cong \mathcal{C}_1,\ C \text{ zyklisch}\}. \tag{26}$$

Dann nennen wir $z := |Iso(\mathcal{C}_1)|$ den Isomorphie-Faktor *von $\mathcal{C}_1$.*

Vermutung 0.41
Wir vermuten:

1. *Seien $\mathcal{C}_1 \ncong \mathcal{C}_2 \subseteq \mathbb{F}_2^N$ zwei zyklische Codes.*
   Die Anzahl der jeweils zu $\mathcal{C}_i$, $(i = 1, 2)$ isomorphen zyklischen Codes ist eine invariante Eigenschaft der zugehörigen Automorphismengruppe $Aut(\mathcal{C}_i)$, d.h., es gilt:

$$|Iso(\mathcal{C}_1)| = |Iso(\mathcal{C}_2)|,\ \text{falls } Aut(\mathcal{C}_1) = Aut(\mathcal{C}_2) \tag{27}$$

2. *Sei $\mathcal{C} \in \mathbb{F}_2^N$ ein zyklischer Code. Falls*

$$Aut(\mathcal{C}) = \prod \mathfrak{G}_i,\ \text{mit } \prod_i grad(\mathfrak{G}_i) = N, \tag{28}$$

   wobei neben dem Kranzprodukt auch das direkte Produkt zur Bildung des Gruppenprodukts der $\mathfrak{G}_i$ zugelassen ist und $grad(\mathfrak{G}_i)$ den Permutationsgrad von $\mathfrak{G}_i$ bezeichnet, dann gilt:

$$z = |Iso(\mathcal{C})| = \prod_i |Iso(C_i)|,\ \text{mit } Aut(C_i) = \mathfrak{G}_i. \tag{29}$$

oder mit anderen Worten:
Der Isomorphie-Faktor z einer Automorphismengruppe $Aut(\mathcal{C})$, die durch ein Gruppenprodukt der $\mathfrak{G}_i$ gebildet wird, ist das Produkt der Isomorphie-Faktoren z_i der einzelnen Produktgruppen $\mathfrak{G}_i$ und zwar egal, ob sie als direkte Produkte, Kranzprodukte, oder gemischte Produkte miteinander verknüpft sind.

Bei der Untersuchung der $PSL(r, 2)$-Gruppen bezüglich der Code-Isomorphien zeigten sich (außer der Zunahme der Codeanzahl) ein weiteres interessantes Phänomen:

- Die sprunghafte Erhöhung (Quantensprung) des „Isomorphie-Faktors“ setzt sich weiter fort und erfolgt (unregelmäßig) anfangs um den Faktor 3:
  So finden wir zunächst für $PSL(r, 2)$ jeweils bei ungeradem r ($3 \leq r \leq 7$) die Erhöhung der Iso-Faktoren von 2 auf 6 und 18 ($PSL(7, 2)$), während wir bei $PSL(8, 2)$ auf einen Iso-Faktor von 16 zurückfallen, um dann bei $PSL(9, 2)$ wieder den dreifachen Wert von 48 als Iso-Faktor zu finden.
  Für $PSL(10, 2)$ finden wir einen Iso-Faktor von 60, während wir bei $PSL(11, 2)$ einen Iso-Faktor haben (≤ 176)[10], der auf jeden Fall kleiner ist als das Dreifache von 60 (180).

Anschließend möchte ich die bislang gefundenen Spezialgruppen in einer Tabelle zusammenfassen – aufsteigend nach Iso-Faktor und der Codelänge des ersten Auftretens sortiert. Dabei sind die Angaben bis zur Codelänge $N = 73$ vollständig.

Abschließend sei noch bemerkt, daß im Zuge der Untersuchung der PLOTKIN-Summe (s. Abschnitt 2.2) beobachtet wurde, daß auch Code-Isomorphien zwischen zyklischen und nicht-zyklischen Codes existieren: So gibt es zum $[7, 4, 3]$-Hamming-Code noch einen weiteren isomorphen zyklischen Code, aber darüberhinaus noch weitere 22 nicht-zyklische isomorphe lineare Codes.

Eine weitergehende Untersuchung der offenen Fragen an dieser Stelle würde sicher den Rahmen dieser Arbeit sprengen. Ich könnte mir aber durchaus eine eigenständige wissenschaftliche Arbeit zu diesem Thema auf der Basis meiner Ergebnisse und gesammelten Daten vorstellen.

[10] Für die zugehörige Codelänge $N = 2047$ konnte **Magma** die Isomorphien nicht mehr bestimmen. Notwendig für eine Code-Isomorphie ist die Übereinstimmung von $[N, k, d]$. Ich habe dort in einem Fall 176 Codes mit einer derartigen Übereinstimmung $[2047, 2036, 3]$ (Hamming-Code $\mathcal{CH}_{11}$) gefunden und somit eine Abschätzung nach oben erhalten.

Faktor	Code-Länge	Automorphismengruppe
2	7	$PSL(3,2)$
2	15	$PSL(4,2)$
2	21	$PSL(3,4) \rtimes \mathfrak{S}_3$
2	23	$M23$
2	35	$\mathfrak{MZ}(7,3) \times \mathfrak{S}_5$
2	85	$\mathfrak{MZ}(17,8) \times \mathfrak{S}_5$
4	49	$PSL(3,2) \wr PSL(3,2)$
4	51	$PSL(2,16) \rtimes \mathfrak{Q}_3$
6	31	$PSL(5,2)$
6	63	$PSL(6,2)$
6	63	$PSL(2,8) \rtimes \mathfrak{MZ}(7,3)$
6	63	$\mathfrak{S}_3 \rtimes (PSL(3,4) \rtimes \mathfrak{S}_3)$
8	73	$PSL(3,8) \rtimes \mathfrak{Z}_3$
8	85	$PSL(4,4) \rtimes \mathfrak{Z}_2$
8	85	$(PSL(2,16) \rtimes \mathfrak{Z}_5) \rtimes \mathfrak{Z}_4$
8	89	$\mathfrak{MZ}(89,11)$ auflösbar
12	217	$PSL(5,2) \times PSL(3,2)$
12	217	$PSL(5,2) \wr PSL(3,2)$
16	255	$PSL(8,2)$
16	511	$PSL(3,2) \times \mathfrak{MZ}(73,9)$
18	127	$PSL(7,2)$
48	511	$PSL(9,2)$
60	1023	$PSL(10,2)$
≤ 176	2047	$PSL(11,2)$

Tabelle 2: Tabelle der Isomorphie-Faktoren

Kapitel 1

Der zentrale Satz für zyklische Codes

Dieses Kapitel ist sehr umfangreich. Daher soll hier die Kapitelstruktur vorgestellt werden. Ziel dieser Arbeit ist es, die Automorphismengruppen von zyklischen Codes zu untersuchen und eine Übersicht darüber zu gewinnen. Dazu benötigen wir das Permutations.-Kranzprodukt (s. „Grundbegriffe“), um diese Gruppen zu beschreiben. Die Codes (und ihre zugehörigen Automorphismengruppen) werden in dieser Reihenfolge untersucht:

- Codelängen ohne zyklische Codes
- Zykl. Codes der Länge $N = 2 \cdot l$
- Zykl. Codes der Länge $N = 4 \cdot m$
- Zykl. Codes der Länge $N = 8 \cdot j$
- Zykl. Codes der Länge $N = 2^r \cdot i$
- Zykl. Codes der Länge $N = 3 \cdot l$
- Zykl. Codes der Länge $N = 9 \cdot l$
- Zykl. Codes der Länge $N = 5 \cdot l$
- Zykl. Codes der Länge $N = 7 \cdot l$

In diesem Kapitel wollen wir uns mit den zyklischen Codes und ihren Automorphismengruppen befassen. Um diese näher zu untersuchen, habe ich mit dem Computeralgebrasystem **Magma** die zyklischen Codes als Gruppencodes der jeweiligen zyklischen Gruppe berechnet und die zugehörigen Automorphismengruppen ermittelt. Bei der Betrachtung der Kompositionsfaktoren dieser Automorphismengruppen fielen mir interessante Gesetzmäßigkeiten über deren Struktur auf, die wir im Folgenden formulieren und beweisen werden.

1.1 Codelängen ohne zyklische Codes

Zuerst wollen wir die Frage untersuchen, warum es für einige N keine nichttrivialen (im Sinne dieser Arbeit) zyklischen Codes gibt. Dabei wurde folgendes bislang beobachtet:

Satz 1.1
Es gibt keine nichttrivialen (i.S.d.A.) zyklischen Codes für folgende kleine N: $N = 1$, 2, 3, 4, 5, 6, 8, 9.

Beweis. exemplarisch billig berechenbar. □

Die Untersuchung der weiteren Codelängen N, mit N prim, kommt zu folgendem Ergebnis:

Beobachtung 1.2
Sei $N \leq 127$ eine Primzahl. Es folgen 2 Aussagen:

1. *Es gibt keine nichttrivialen (i.S.d.A.) zyklischen Codes für N prim, es sei denn, es existiert eine spezielle nichtauflösbare Permutationsgruppe $\mathfrak{G} \lneqq \mathfrak{S}_N$ als Automorphismengruppe, die auf einer Menge Ω der Kardinalität N transitiv operiert.*
   Dies sind die Gruppen
   - $PSL(3,2)$ *für* $N = 7$,
   - $M23$ *für* $N = 23$,
   - $PSL(5,2)$ *für* $N = 31$,
   - $PSL(3,8) \rtimes \mathfrak{Z}_3$ *für* $N = 73$,
   - $PSL(7,2)$ *für* $N = 127$.
2. *Diese jeweilige spezielle Gruppe ist dann auch die einzige Automorphismengruppe für alle zyklischen Codes der Länge N.*

Interessant ist in diesem Zusammenhang der Fall $N = 17$:
Hier gibt es zwar eine spezielle nichtauflösbare Permutationsgruppe, die auf einer Menge Ω der Kardinalität 17 transitiv operiert, nämlich die Gruppe $PSL(2,16)$. Allerdings tritt sie nicht als Automorphismengruppe bei $N = 17$, oder $N = 34$ auf, sondern erst bei $N = 51$ – und zwar in einem Konstrukt mit 2 semidirekten Produkten. Diese Automorphismengruppe wird von 64 Codes angenommen (mit einem Iso-Faktor 4).
Es gibt jedoch die auflösbare Automorphismengruppe $\mathfrak{MZ}(17,8)$ mit 4 zugehörigen Codes der Länge $N = 17$, davon je 2 isomorph. Wegen der Auflösbarkeit von $\mathfrak{MZ}(17,8)$ sind diese Codes trivial im Sinne dieser Arbeit und daher im Tabellenwerk nicht berücksichtigt

Bemerkung 1.3
zur Aussage 1.) der obigen Beobachtung:
Es sind alle Codelängen mit N prim im Untersuchungsbereich ($N \leq 127$) daraufhin überprüft worden.

[0] zur Definition von *trivial* siehe 0.25

zur Aussage 2.):
Für $N \leq 127$ konnte keine Primzahl $p = N$ gefunden werden, zu der es zwei verschiedene nichtauflösbare Permutationsgruppen gibt, die auf einer Menge Ω mit der Kardinalität $|\Omega| = p$ operieren.
Für $N = 127$ gibt es insgesamt $524288 = 2^{19}$ Rohcodes (s. Kap. 6). Insgesamt sind aber **nur** 180 Codes nichttrivial, mit $PSL(7, 2)$ als Automorphismengruppe.
Davon bleiben – wegen des Iso-Faktors von 18 für $PSL(7, 2)$, (s. Tabelle 2) – **nur** 10 Codes (bis auf Isomorphie) übrig (s. Tabelle 10.1).

Dies definiert auf der Menge der Primzahlen eine Klasseneinteilung in zwei disjunkte Klassen:

1. Primzahlen mit nichttrivialen zyklischen Codes
2. Primzahlen ohne nichttriviale zyklische Codes
   Dabei unterscheiden wir diesen zweiten Fall noch nach Primzahlen mit trivialen zyklischen Codes
   (a) mit auflösbaren Automorphismengruppen $Aut(C)$ – zusätzlich zu $\mathfrak{S}_p$, bzw.
   (b) nur mit der symmetrischen Gruppe $\mathfrak{S}_p$ als Automorphismengruppe.

Zu dieser Einteilung gehört die folgende Aussage:

Fakt 1.4
Im Fall 2b) ergibt die Bahnzerlegung[1] *von* Ω *stets nur* 2 *Bahnen. Wir werden im Kapitel 6 sehen, daß es dann für* $N = p$ *deswegen nur* $2^2 = 4$ *zyklische Codes gibt. Das sind die* 4 *primitiven Codes (s. Abschnitt 2.1* Elementarcodes*).*
Treten bei der Bahnzerlegung von Ω *mehr als* 2 *Bahnen auf, so liegt Fall 1) oder 2a) vor: Sowohl für* $p = 7$ *(Fall 1), wie für* $p = 17$ *(Fall 2a) bekommen wir* 3 *Bahnen.*

Bemerkung 1.5
Die Zahl 89 gehört ebenfalls zu den Codelängen ohne nichttriviale zyklische Codes:
Während bei den übrigen untersuchten Primzahlen ohne nichttriviale zyklischen Codes die Anzahl der trivialen Codes meist bei 4, bisweilen auch bei 8 oder 16 lag, sind es hier immerhin 512 triviale Codes.
Ursache ist hier die auflösbare metazyklische Gruppe $\mathfrak{MZ}(89, 11) = \mathfrak{Z}_{89} \rtimes \mathfrak{Z}_{11}$. Damit gehört $p = 89$ zum obigen Fall 2a) – die Bahnzerlegung von Ω ergibt 9 Bahnen.
Ich habe deshalb ausnahmsweise für diese Codelänge einen Eintrag in der Liste der zyklischen Codes (s. Anhang A) vorgenommen.

Diese Thematik der zyklischen Codes für Primzahl-Codelängen könnte man durchaus weiterverfolgen. Wir wollen uns aber in dieser Arbeit den Codelängen zuwenden, die eine Faktorenzerlegung haben und dabei untersuchen, inwieweit sich diese Faktorenzerlegung auf die Attribute der zyklischen Codes, bzw. auf die Struktur der Automorphismengruppen dieser Codes auswirkt.

[1] s. Definition 6.1

1.2 Zyklische Codes gerader Länge

Um die ganze Thematik schrittweise zu erarbeiten, wollen wir uns zuerst den zyklischen Codes gerader Länge widmen.
Es sei an dieser Stelle daran erinnert, daß wir unter dem **Kranzprodukt**

$$\mathfrak{G} \wr \mathfrak{H}$$

stets das sog. **Permutations-Kranzprodukt** verstehen, so wie es auch in **Magma** implementiert ist.

1.2.1 Zyklische Codes der Länge $N = 2 \cdot l$

Die folgende Schreibweise gilt mit ihrer Nomenklatur in allen folgenden Aussagen.

Bezeichnung 1.6
Sei $N \in \mathbb{N}$ gerade ($N = 2 \cdot l$ mit $l \geq 5$)[2] und sei
$u = (1, 0, 1, 0, \ldots) \in \mathbb{F}_2^N$,
$v = (0, 1, 0, 1, \ldots) \in \mathbb{F}_2^N$.
Dann sei $C_2 := \langle u, v \rangle$ der aus u und v erzeugte Code.

Wir beweisen nun einen ersten einfachen Satz:

Hilfssatz 1.7
C_2 ist zyklisch. Es ist $\dim(C_2) = 2$.

Beweis. Da die Vektoren u und v linear unabhängig sind, erzeugen sie einen 2-dimensionalen Unterraum C_2, zu dem außer u und v nur noch der Nullvektor und der Einsvektor gehören. Man überzeugt sich leicht, daß jede zyklische Verschiebung eines jeden Vektors aus C_2 wieder einen Vektor aus C_2 ergibt. Damit erfüllt C_2 die Kriterien eines zyklischen Codes. □

Wir beweisen nun einen weiteren einfachen Satz:

Hilfssatz 1.8
Sei C_2 der in 1.6 definierte Code. Dann gilt:
C_2 hat die Minimaldistanz $d = l = \frac{N}{2}$, d.h., C_2 ist ein linearer $[N, 2, \frac{N}{2}]$ - Code.

Beweis. Es ist leicht zu sehen, daß sowohl u, als auch v in genau l Positionen vom Nullvektor, wie auch vom Einsvektor verschieden sind. Nach der Definition der Minimaldistanz in MacWilliams [16] Ch1, §3 gilt also: $d = l = \frac{N}{2}$. □

Nun wollen wir drei wichtige Sätze über die Automorphismengruppe $Aut(C_2)$ formulieren und beweisen:

[2] Die Einschränkung $l \geq 5$ hängt mit der Forderung zusammen, daß die Automorphismengruppe nicht auflösbar sein soll. Geht man von dieser Forderung ab, so kann man auch diese Voraussetzung fallen lassen.

Lemma 1.9
Sei C_2 der in 1.6 definierte Code. Dann gilt:

$$\mathfrak{S}_2 \leq Aut(C_2). \tag{1.1}$$

Beweis. Sei $\mathfrak{S}_2 = \{1, \sigma\}$. Wir definieren eine Operation von $\mathfrak{S}_2$ auf $\mathbb{F}_2^N, N \in \mathbb{N}$ und $N = 2 \cdot l$: Sei $c = (a_1, b_1, a_2, b_2, \ldots, a_l, b_l)$ ein Codevektor. Dann gilt:

$$1 \cdot c = c \tag{1.2}$$

$$\sigma \cdot c = (b_1, a_1, b_2, a_2, \ldots, b_l, a_l). \tag{1.3}$$

Dann ist $\sigma \cdot c = ((b_1, a_1), (b_2, a_2), \ldots, (b_l, a_l))$ ebenfalls ein Codevektor. Dies definiert eine Operation der symmetrischen Gruppe $\mathfrak{S}_2$ auf $\mathbb{F}_2^N$, die den Code C_2 invariant läßt. □

Lemma 1.10
Sei C_2 der in 1.6 definierte Code. Dann gilt:

$$\mathfrak{S}_l \leq Aut(C). \tag{1.4}$$

Beweis. Sei $c = ((a_1, b_1), (a_2, b_2), \ldots)$ ein Codevektor. Dann ist $((a_2, b_2), (a_1, b_1), \ldots)$ ebenfalls ein Codevektor. Dies definiert eine Operation der symmetrischen Gruppe $\mathfrak{S}_l$ auf $\mathbb{F}_2^N$, die den Code C_2 invariant läßt. □

Lemma 1.11
Sei C_2 der in 1.6 definierte Code. Dann gilt:

$$\mathfrak{S}_l \times \mathfrak{S}_l \leq Aut(C_2). \tag{1.5}$$

Beweis. Sei $c = (a_1, b_1, a_2, b_2, \ldots, a_l, b_l)$ ein Codevektor. Dann können zum einen die a_i permutiert werden und zum anderen die b_i. Dies definiert eine Operation der Gruppe $\mathfrak{S}_l \times \mathfrak{S}_l$ auf $\mathbb{F}_2^N$, die den Code C_2 invariant läßt. □

Nun folgt unser erster Hauptsatz über die Struktur der Automorphismengruppe des Codes C_2.

Satz 1.12 (Zentraler Satz für zyklische Codes gerader Länge, Teil 1)
Sei C_2 der in 1.6 definierte Code. Dann gilt:

$$\mathfrak{S}_l \wr \mathfrak{S}_2 \cong Aut(C_2). \tag{1.6}$$

Beweis. Die Gruppe von linearen Abbildungen, die von $\mathfrak{S}_2$ und $\mathfrak{S}_l \times \mathfrak{S}_l$ (nach Satz 1.9 und Satz 1.11) erzeugt wird, ist isomorph zum Kranzprodukt $\mathfrak{S}_l \wr \mathfrak{S}_2$.
Damit ist gezeigt, daß $Aut(C_2)$ eine Untergruppe U besitzt, die isomorph zu $\mathfrak{S}_l \wr \mathfrak{S}_2$ ist, d.h. es gilt also:

$$\mathfrak{S}_l \wr \mathfrak{S}_2 \cong U \leq Aut(C_2). \tag{1.7}$$

Es bleibt zu zeigen, daß $Aut(C_2) = U$ gilt[3]:
Sei $\varphi \in Aut(C_2)$ beliebig. Wegen $Aut(C_2) \leq \mathfrak{S}_N$ gilt $\varphi \in \mathfrak{S}_N$. Wir zeigen, daß $\varphi \in U$ gilt. Sei

$$\Lambda_1 := \quad \{1, 3, 5, \ldots, N-1\} \tag{1.8}$$

$$\Lambda_2 := \quad \{2, 4, 6, \ldots, N\}. \tag{1.9}$$

Da φ den linearen Code C_2 in sich überführen muß, folgt

- $\alpha)$ $\quad \varphi(\Lambda_1) = \Lambda_1 \quad \wedge \quad \varphi(\Lambda_2) = \Lambda_2 \quad$ oder
- $\beta)$ $\quad \varphi(\Lambda_1) = \Lambda_2 \quad \wedge \quad \varphi(\Lambda_2) = \Lambda_1.$

Wir führen jetzt eine Fallunterscheidung durch:

- α : In diesem Fall ist φ das Produkt zweier Permutationen aus $\mathfrak{S}_l$ und damit gilt nach Lemma 1.11 $\varphi \in U$.
- β : In diesem Fall ist $\sigma * \varphi$ ein Element aus $Aut(C_2)$, das die Bedingung $\alpha)$ erfüllt. Das Element σ ist in Lemma 1.9 definiert. Nach dem ersten Fall folgt $\sigma * \varphi \in U$

□

Wenn wir uns noch einmal den Code C_2 genauer ansehen, stellen wir fest, daß die beiden erzeugenden Vektoren u und v zusammen eine Aneinanderreihung von l Einheitsmatrizen der Dimension 2 darstellen. Dieses Gebilde ist die Generatormatix des Codes C_2. Dieses Konstruktionsprinzip werden wir auch im Folgenden verwenden (jetzt bauen wir ein Gebilde aus 2 Einheitsmatrizen der Dimension l, das ist dann die Generatormatrix des neuen Codes C_l):

Bezeichnung 1.13
Sei $N \in \mathbb{N}$ *gerade* $(N = 2 \cdot l$ *mit* $l \geq 5)$ *und sei*
$x_1 = (1, 0, 0, \ldots, 0, 1, 0, 0, \ldots, 0) \in \mathbb{F}_2^N$,
$x_2 = (0, 1, 0, \ldots, 0, 0, 1, 0, \ldots, 0) \in \mathbb{F}_2^N$,
. . . . . .
. . . . . .
$x_l = (0, 0, 0, \ldots, 1, 0, 0, 0, \ldots, 1) \in \mathbb{F}_2^N$.
Dann sei $C_l := \langle x_1, x_2, \ldots, x_l \rangle$ *der aus den* x_i *erzeugte Code.*

Wir beweisen nun einen weiteren einfachen Satz:

Hilfssatz 1.14
C_l *ist zyklisch. Es ist* $\dim(C_l) = l = \dfrac{N}{2}$.

[3] wir werden im Kapitel 9, nach Folgerung 9.5 aus den dortigen Erkenntnissen einen knappen Beweis ableiten können.

Beweis. Da die Vektoren x_1 bis x_l alle linear unabhängig sind, erzeugen sie einen l-dimensionalen Unterraum C_l. Man überzeugt sich leicht, daß jede zyklische Verschiebung eines jeden Vektors aus C_l wieder einen Vektor aus C_l ergibt. Damit erfüllt C_l die Kriterien eines zyklischen Codes. □

Wir beweisen nun einen weiteren einfachen Satz:

Hilfssatz 1.15
Sei C_l der in 1.13 definierte Code. Dann gilt:
C_l hat die Minimaldistanz $d = 2$, d.h., C_l ist ein linearer $[N, \frac{N}{2}, 2]$ - Code.

Beweis. Nach der Definition der Minimaldistanz in MacWilliams [16] Ch1, §3 ist leicht zu sehen, daß die x_i in genau 2 Positionen vom Nullvektor verschieden sind. Auch durch Summenbildung einzelner x_i ist eine von Null verschiedene Hammingdistanz nicht unter den Wert von 2 zu bringen. □

Satz 1.16
Sei C_l der in 1.13 definierte Code. Dann gilt:
C_l ist ein selbstdualer Code ($C_l = C_l^\perp$) mit der Dimension $k = l = \frac{N}{2}$.

Beweis. Das oben dargestellte Erzeugendensystem der $\langle x_1, x_2, \ldots, x_l \rangle$ stellt nach Konstruktion die Generatormatrix G_{C_l} für den dadurch definierten Code C_l dar. Es gilt:

$$G_{C_l} = (E_l | E_l) = (E_l | E_{N-l}) = (-E_l^t | E_{N-l}) = H_{C_l}.$$

Damit ist die Generatormatrix gleich der Kontrollmatrix des Codes C_l (nach Lütkebohmert [10], Lemma 1.15). Somit ist der $[N, \frac{N}{2}, 2]$-Code C_l selbstdual. □

Aus dem obigen Satz und den Beobachtungen bei der Untersuchung der zyklischen Codes gewinnen wir die

Folgerung 1.17
Sei $N \leq 70$. Für gerades N ist die Anzahl der zyklischen Codes ungerade.

Beweis. Sei A die Menge der zyklischen $[N, k, d]$-Codes, mit $k \leq \frac{N}{2}$, die nicht selbstdual sind und sei B die Menge der dazu dualen Codes.
Dann gilt $|A| = |B|$ und $|A| + |B|$ ist somit eine gerade Zahl.
Ist nun N gerade, so existiert stets der selbstduale Code C_l, wie oben gezeigt. Wir haben im Satz 0.38 bewiesen, daß es zu diesem Code keine isomorphen Codes gibt. Wir werden weiter sehen, daß eventuelle weitere selbstduale Codes stets in einer geraden Anzahl von isomorphen Codes auftreten. Damit ist die Gesamtzahl der zyklischen Codes für gerades N eine ungerade Zahl. □

Im Abschnitt 3.4 werden wir noch Ergebnisse über eventuelle weitere selbstduale Codes diskutieren.
Nun folgt unser Hauptsatz über die Struktur der Automorphismengruppe des selbstdualen Codes ($C_l = C_l^\perp$):

Satz 1.18 (**Zentraler Satz für zyklische Codes gerader Länge, Teil 2**)
Sei C_l der in 1.13 definierte Code. Dann gilt:
Die Automorphismengruppe des selbstdualen Codes C_l ist isomorph zum folgenden Kranzprodukt:

$$Aut(C_l) \cong \mathfrak{S}_2 \wr \mathfrak{S}_l. \tag{1.10}$$

Den Beweis zum Satz 1.18 führen wir analog, wie für $Aut(C_2)$ (s. oben, Satz 1.12), d.h., wir werden jetzt auch drei wichtige Sätze über die Automorphismengruppe $Aut(C_l)$ formulieren und beweisen:

Lemma 1.19
Sei C_l der in 1.13 definierte Code. Dann gilt:

$$\mathfrak{S}_2 \leq Aut(C_l). \tag{1.11}$$

Beweis. Sei $\mathfrak{S}_2 = \{1, \sigma\}$. Wir definieren eine Operation von $\mathfrak{S}_2$ auf $\mathbb{F}_2^N, N \in \mathbb{N}$ und $N = 2 \cdot l$: Sei $c = (a_1, b_1, \ldots, l_1, a_2, b_2, \ldots, l_2)$ ein Codevektor. Dann gilt:

$$1 \cdot c = c \tag{1.12}$$

$$\sigma \cdot c = (a_2, b_2, \ldots, l_2, a_1, b_1, \ldots, l_1). \tag{1.13}$$

Dann ist $\sigma \cdot c = ((a_2, b_2, \ldots, l_2), (a_1, b_1, \ldots, l_1))$ ebenfalls ein Codevektor. Dies definiert eine Operation der symmetrischen Gruppe $\mathfrak{S}_2$ auf $\mathbb{F}_2^N$, die den Code C_l invariant läßt. □

Lemma 1.20
Sei C_l der in 1.13 definierte Code. Dann gilt:

$$\mathfrak{S}_l \leq Aut(C_l). \tag{1.14}$$

Beweis. Sei $c = (a_1, b_1, \ldots, l_1, a_2, b_2, \ldots, l_2)$ ein Codevektor.
Dann ist $((b_1, a_1, \ldots, l_1), (b_2, a_2, \ldots, l_2))$ ebenfalls ein Codevektor. Dies definiert eine Operation der symmetrischen Gruppe $\mathfrak{S}_l$ auf $\mathbb{F}_2^N$, die den Code C_l invariant läßt. □

Wir benötigen noch den folgenden

Satz 1.21
Sei C_l der in 1.13 definierte Code. Dann gilt:

$$\underbrace{\mathfrak{S}_2 \times \mathfrak{S}_2 \times \ldots \times \mathfrak{S}_2}_{l-mal} \leq Aut(C_l). \tag{1.15}$$

Beweis. Sei $c = (a_1, b_1, \ldots, l_1, a_2, b_2, \ldots, l_2)$ ein Codevektor.
Dann können die $a_i, b_i, \ldots, l_i$ jeweils für sich (d.h. unabhängig voneinander) permutiert werden.
Dies definiert eine Operation der Gruppe $\underbrace{\mathfrak{S}_2 \times \mathfrak{S}_2 \times \ldots \times \mathfrak{S}_2}_{l-mal}$ auf $\mathbb{F}_2^N$,
die den Code C_l invariant läßt. □

Nun können wir den obigen Hauptsatz 1.18 über die Struktur der Automorphismengruppe des selbstdualen Codes beweisen:

Beweis. Die Gruppe von linearen Abbildungen, die von $\mathfrak{S}_l$ und $\underbrace{\mathfrak{S}_2 \times \ldots \times \mathfrak{S}_2}_{l-mal}$ (nach Satz 1.10 und Satz 1.21) erzeugt wird, ist isomorph zum Kranzprodukt $\mathfrak{S}_2 \wr \mathfrak{S}_l$. Die Argumentation ist analog zum Beweis vom Satz 1.12. □

Korollar 1.22
Es gibt genau 2 *weitere zyklische Codes mit derselben Automorphismengruppe, nämlich den* $[N, l-1]$ *- Code und den dazu dualen* $[N, l+1]$ *- Code.*
Wir nennen diese Codes benachbart *zum Code* C_l.
Der $[N, l-1]$ *- Code wird von dem Vektor* $x = (1, 1, 0, 0 \ldots, 0, 1, 1, 0, \ldots, 0)$ *zyklisch erzeugt, wobei sich die dritte* 1 *an der Stelle* $l+1$ *befindet. Dieser Code hat die Minimaldistanz* $4 = 2 \cdot 2$.
Der $[N, l+1]$ *- Code wird von dem Vektor* $x = (1, 1, 1, \ldots, 1, 0, 0, 0, \ldots, 0)$ *zyklisch erzeugt, wobei sich die erste* 0 *an der Stelle* $l+1$ *befindet. Dieser Code hat die Minimaldistanz* 2.

Beweis. Wir werden das Korollar im Kapitel 2 „Vererbung“ allgemein beweisen (Sätze 2.3 bis 2.2, angewandt auf den **„zweiten Elementarcode“**, s. Abschnitt 2.1). □

Es folgt nun ein erstes einfaches Beispiel für die Codelänge $N = 10$. Die Erläuterungen sind nach dem Beispiel aufgeführt.

Beispiel 1.23 ($N = 10$)

```
Zyklische Codes der Laenge N = 10

Lfd.Nr.  k   d     #PermGrp          #AutoGrp

   1     8   2         10              28800
   2     2   5         10              28800
   3     6   2         10               3840
   4     4   4         10               3840
   5     5   2         10               3840

Es wurden 5 verschiedene Codes gefunden
abzueglich der Codes, bei denen die Automorphismengruppe aufloesbar ist,
oder gleich der alternierenden oder der symmetrischen Gruppe vom Grad 10 ist

Es wurden 2 verschiedene Automorphismengruppen
ueber alle Codes gefunden:

1 . Automorphismen-Gruppe mit 28800 Elementen
Permutation group PG acting on a set of cardinality 10
Order = 28800 = 2^7 * 3^2 * 5^2

    G
    |  Cyclic(2)          =Sym(2)
    * ==================
    |  Cyclic(2)        \
    *                    >=Sym(5)
    |  Alternating(5)   /
    * ------------------
    |  Cyclic(2)        \
    *                    >=Sym(5)
    |  Alternating(5)   /
    1

2 . Automorphismen-Gruppe mit 3840 Elementen
Permutation group PG acting on a set of cardinality 10
Order = 3840 = 2^8 * 3 * 5

    G
    |  Cyclic(2)       \
    *                   >=Sym(5)
    |  Alternating(5)  /
    * =================
    |  Cyclic(2)         =Sym(2)
    * -----------------
    |  Cyclic(2)         =Sym(2)
    * -----------------
    |  Cyclic(2)         =Sym(2)
    * -----------------
    |  Cyclic(2)         =Sym(2)
    * -----------------
    |  Cyclic(2)         =Sym(2)
    1
```

Die Kompositionsfaktoren der Automorphismengruppen werden im Computeralgebrasystem **Magma** von oben ($\mathrm{G} = Aut(C)$) nach unten (1) gelistet. Dies entspricht beim Bild des Kranzes der Richtung von innen nach außen. Zur Verdeutlichung habe ich in den Beispielen die innere Permutationsgruppe $\mathfrak{H}$ von dem äußeren Kranz durch eine doppelte Trennlinie

```
================
```

abgesetzt, sowie die einzelnen Kopien der Gruppe $\mathfrak{G}$ auf dem Kranz durch eine einfache Trennlinie

```
----------------
```

von einander separiert.

Bemerkung 1.24
Die im obigen Beispiel mit den laufenden Nummern 2 und 5 bezeichneten Codes entsprechen unseren Definitionen. Daher wollen wir hier die Generatormatrizen beider Codes mit aufführen:

```
Lfd.Nr.  k   d     #PermGrp          #AutoGrp

   2     2   5         10              28800

[10, 2, 5] Linear Code over GF(2)
Generator matrix:
[1 0 1 0 1 0 1 0 1 0]
[0 1 0 1 0 1 0 1 0 1]

Lfd.Nr.  k   d     #PermGrp          #AutoGrp

   5     5   2         10               3840

[10, 5, 2] Cyclic Linear Code over GF(2)
Generator matrix:
[1 0 0 0 0 1 0 0 0 0]
[0 1 0 0 0 0 1 0 0 0]
[0 0 1 0 0 0 0 1 0 0]
[0 0 0 1 0 0 0 0 1 0]
[0 0 0 0 1 0 0 0 0 1]
```

Wir können nun aus den oben bewiesenen zwei Hauptsätzen folgende Schlußfolgerungen ableiten:

Korollar 1.25
Sei N gerade ($N = 2 \cdot l$ mit $l \geq 5$). Für alle zyklischen Codes der Länge N existieren mindestens zwei Automorphismengruppen, nämlich:

$$Aut(C_2) \cong \mathfrak{S}_l \wr \mathfrak{S}_2, \tag{1.16}$$

$$Aut(C_l) \cong \mathfrak{S}_2 \wr \mathfrak{S}_l. \tag{1.17}$$

Korollar 1.26
Sei N gerade ($N = 2 \cdot l$ mit $l \geq 5$). Für alle zyklischen Codes der Länge N existieren mindestens 5 nichttriviale (im Sinne dieser Arbeit) Codes, nämlich:
1. Der Code C_2, wie in der Bezeichnung 1.6 dargelegt,
2. Der zu C_2 duale Code $C_2^{\perp}$, siehe 0.28,
3. Der sebstduale Code C_l, siehe 1.16,
4. und 5. Die beiden „Nachbarcodes“ zum selbstdualen Code, siehe Korollar 1.22.

Beweis. Die beiden Korollare ergeben sich aus den weiter oben bewiesenen Aussagen. □

Die in den Korollaren 1.25 und 1.26 ausgesprochenen Schranken werden für einige N scharf, so z.B. für $N = 10$ (siehe obiges Beispiel), $N = 12$, 16, 22, 26, 34, 38, 58, 74 (bis hierher untersucht), 82, 86, 94, 106, 118, 122, 134, etc.

Bis auf $N = 12$, 16 sind diese Codelängen von der Gestalt $N = 2 \cdot l$, mit l prim und es existieren zur Codelänge l nur triviale Codes.
Wir werden dazu im Kapitel 2 den Satz 2.21 formulieren und beweisen.

Bemerkung 1.27
Bei zyklischen Codes gerader Länge $N = 2 \cdot l$ existieren für bestimmte l noch zusätzliche spezielle Automorphismengruppen, nämlich dann, wenn l prim ist, aber dennoch nichttriviale zyklische Codes für $N = l$ existieren (z.B.: $l = 7, 23, 31, 73, 127, \ldots\ldots$), wie im Abschnitt 1.1 diskutiert.
Diese Thematik wird in einem separaten Abschnitt 3.5 behandelt.

1.2.2 Zyklische Codes der Länge $N = 4 \cdot m$

Für gerade Codelängen N mit $N = 4 \cdot m$ habe ich noch weitere Gesetzmäßigkeiten entdeckt, die wir im Folgenden formulieren wollen.
Wie im vorigen Abschnitt gezeigt, existieren für gerade Codelängen $N = 2 \cdot l$ stets die

beiden Automorphismengruppen:

$$\mathfrak{S}_l \wr \mathfrak{S}_2 \tag{1.18}$$

$$\mathfrak{S}_2 \wr \mathfrak{S}_l \tag{1.19}$$

und die zugehörigen 5 zyklischen Codes.
Die hier im Folgenden gemachten Aussagen stellen eine Zusammenfassung der Erkenntnisse aus dem umfangreichen Listen- und Tabellenwerk dar und sind für die Codelängen $20 \leq N \leq 100$, $N = 4 \cdot m$ **anhand der identifizierten Automorphismengruppen und deren zugehörige Codes exemplarisch überprüft worden.**

Beobachtung 1.28
Sei N *weiterhin gerade* ($N = 2 \cdot l$ *mit* $l = 2 \cdot m$ *und* $m \geq 5$).
Es gilt nun: Es gibt mindestens 4 *weitere Automorphismengruppen:*

$$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_m \tag{1.20}$$

$$\mathfrak{S}_2 \wr \mathfrak{S}_m \wr \mathfrak{S}_2 \tag{1.21}$$

$$\mathfrak{S}_m \wr \mathfrak{S}_4 \tag{1.22}$$

$$\mathfrak{S}_4 \wr \mathfrak{S}_m \tag{1.23}$$

und – falls m *ungerade, so existieren auch noch*

$$\mathfrak{S}_4 \times \mathfrak{S}_m \quad \textit{und} \tag{1.24}$$

$$\underbrace{(\mathfrak{S}_2 \times \cdots \times \mathfrak{S}_2)}_{(2m)-mal} \rtimes (\mathfrak{S}_m \times \mathfrak{S}_3). \tag{1.25}$$

sowie – falls es eine Spezialgruppe gibt (z.B. PSL(r,2), oder M23), die auf einer Menge Ω *der Kardinalität* m *transitiv operiert – auch*

$$\mathfrak{S}_4 \times \mathit{Spezialgruppe}_m \quad \textit{und} \tag{1.26}$$

$$\underbrace{(\mathfrak{S}_2 \times \cdots \times \mathfrak{S}_2)}_{(2m)-mal} \rtimes (\mathit{Spezialgruppe}_m \times \mathfrak{S}_3). \tag{1.27}$$

Die Automorphismengruppe (1.25) läßt sich noch auf zwei andere Arten darstellen (wir werden das später in der Zusammenfassung noch genauer erläutern):

1. als „vermindertes“ Kranzprodukt:

$$(\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_m))/\mathfrak{S}_2^m, \tag{1.28}$$

2. als „gemischtes Gruppenprodukt“:

$$(\mathfrak{K}_4 \wr \mathfrak{S}_m) \rtimes \mathfrak{S}_3. \tag{1.29}$$

In der letzten Darstellung wird am meisten deutlich, daß diese Automorphismengruppe eine Untergruppe von $\mathfrak{S}_4 \wr \mathfrak{S}_m$ ist.

Die Automorphismengruppe (1.27) läßt sich noch auf zwei andere Arten darstellen (wir werden das später in der Zusammenfassung noch genauer erläutern):

1. als „vermindertes“ Kranzprodukt:

$$(\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times Spezialgruppe_m))/\mathfrak{S}_2^m, \tag{1.30}$$

2. als „gemischtes Gruppenprodukt“:

$$(\mathfrak{K}_4 \wr Spezialgruppe_m) \rtimes \mathfrak{S}_3. \tag{1.31}$$

In der letzten Darstellung wird am meisten deutlich, daß diese Automorphismengruppe eine Untergruppe von $\mathfrak{S}_4 \wr Spezialgruppe_m$ ist.
Die Isomorphie der oben angegebenen gemischten Produkte ergibt sich aus der Verwandtschaft der Kompositionsreihen von $\mathfrak{S}_3$ und $\mathfrak{S}_4$. Es gilt:

$$\mathfrak{S}_4 \cong \mathfrak{K}_4 \rtimes \mathfrak{S}_3 \cong (\mathfrak{S}_2 \times \mathfrak{S}_2) \rtimes \mathfrak{S}_3 \cong \mathfrak{S}_2^2 \rtimes \mathfrak{S}_3. \tag{1.32}$$

Bemerkung 1.29
Der Fall 'm gerade' wird im nächsten Teilabschnitt behandelt ($N = 8 \cdot j$).
Bei den obengenannten vier weiteren Kranzprodukten fällt folgendes auf (wir werden das im nächsten Teilabschnitt weiterverfolgen, um allgemeine Aussagen ableiten zu können):
Haben wir nur 2 Kranzfaktoren, so existieren auch beide Vertauschungen als Kranzprodukte. Zu jedem dieser beiden Kranzprodukte gehören 4 Codes, nämlich 2 bezüglich der Dimension k benachbarte Codes und deren zugehörige duale Codes.

Haben wir jedoch 3 Kranzfaktoren, so permutieren nur die letzten beiden Faktoren; als ersten Faktor haben wir stets die $\mathfrak{S}_2$.
Zu jedem dieser beiden Kranzprodukte gehören 2 Codes.
Siehe dazu auch den Abschnitt „Zusammenfassung zyklische Codes“, insbesondere hinsichtlich der Aussagen über Dimension und Minimaldistanz dieser Codes.
Die beiden Automorphismengruppen (im Fall m ungerade) 1.24, sowie 1.28 werden je zweimal angenommen.

Wie bereits oben erwähnt, wollen wir im Abschnitt „Zusammenfassung zyklische Codes“ die Zerlegung der Codelänge N in 2, 3 (und teilweise 4) Faktoren mit den uns interessierenden Fragen allgemein behandeln.
Wegen der Komplexität des semidirekten Produkts werden wir die letzte im Satz erwähnte Automorphismengruppe in einem gesonderten Kapitel behandeln.

Korollar 1.30
Unter der Voraussetzung der vorigen Beobachtung ($N = 4 \cdot m,\ m \geq 5$) gilt:
Die Anzahl der zyklischen Codes ist ≥ 17.
Die Anzahl der zugehörigen Automorphismengruppen ist ≥ 6.

Für 'm ungerade' erhöhen sich die Grenzen der oben gemachten Abschätzungen auf ≥ 21 *zyklische Codes, bzw.* ≥ 8 *zugehörige Automorphismengruppen.*[4]

Bemerkung 1.31
Die im obigen Korollar angegebenen Schranken werden z.B. bei $N = 32$ scharf für m gerade, sowie bei $N = 20$, 44, 52, 68 und 76 für m ungerade. In diesen Fällen ist $7, 23 \neq m$ prim und es existieren zur Codelänge m keine nichttrivialen Codes. Auf $m = 7, 23$ wird gleich noch eingegangen.
Den Fall 'm ungerade' habe ich für folgende Codelängen untersucht: $N = 20$, 28, 36, 44, 52, 60, 68, 76 und 92.
Ende der Bemerkung

Ohne auf die Ausführungen von Abschnitt 3.5 vorgreifen zu wollen, möchte ich doch der Vollständigkeit halber für $N = 28$ ($m = 7$) noch die weiteren zusätzlichen Automorphismengruppen angeben, die anstelle der $\mathfrak{S}_7$ die Spezialgruppe $PSL(3, 2)$ in den obigen Produktformeln haben:

$$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr PSL(3, 2) \tag{1.33}$$

$$\mathfrak{S}_2 \wr PSL(3, 2) \wr \mathfrak{S}_2 \tag{1.34}$$

$$PSL(3, 2) \wr \mathfrak{S}_4 \tag{1.35}$$

$$\mathfrak{S}_4 \wr PSL(3, 2) \tag{1.36}$$

$$\mathfrak{S}_4 \times PSL(3, 2). \tag{1.37}$$

[4] Es sei hier auf das Tabellenwerk im Anhang verwiesen.

Soweit die Analogien zu den obigen Formeln. Ohne Analogien existieren weiter noch:

$$PSL(3,2) \wr \mathfrak{S}_2 \wr \mathfrak{S}_2 \tag{1.38}$$

$$PSL(3,2) \times (\mathfrak{S}_2 \wr \mathfrak{S}_2) \tag{1.39}$$

$$\mathfrak{S}_2 \wr (\mathfrak{S}_2 \times PSL(3,2)) \tag{1.40}$$

$$(\mathfrak{S}_2 \wr (\mathfrak{S}_2 \times PSL(3,2)))/\mathfrak{S}_2^6, \tag{1.41}$$

sowie zwei Kranzprodukte aus der dritten Automorphismengruppe von $N = 14$ mit der Gruppe $\mathfrak{S}_2$:

$$\mathfrak{S}_2 \wr ((\mathfrak{S}_2 \wr PSL(3,2))/\mathfrak{S}_2^3) \tag{1.42}$$

$$((\mathfrak{S}_2 \wr PSL(3,2))/\mathfrak{S}_2^3) \wr \mathfrak{S}_2 \tag{1.43}$$

$$\tag{1.44}$$

sowie ein weiteres komplexeres Gruppenprodukt (s. Tabelle im Anhang):

$$\mathfrak{S}_2^8 \rtimes (\mathfrak{S}_3 \times PSL(3,2)), \tag{1.45}$$

oder als vermindertes Kranzprodukt ausgedrückt[5]:

$$\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times PSL(3,2))/\mathfrak{S}_2^{13} \tag{1.46}$$

$$\cong ((\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times PSL(3,2)))/\mathfrak{S}_2^7)/\mathfrak{S}_2^6. \tag{1.47}$$

Am sinnvollsten scheint mir hier die folgenden Darstellung zu sein:

$$((\mathfrak{K}_4 \wr PSL(3,2))/\mathfrak{K}_4^3) \rtimes \mathfrak{S}_3 \cong ((\mathfrak{K}_4 \wr PSL(3,2))/\mathfrak{S}_2^6) \rtimes \mathfrak{S}_3. \tag{1.48}$$

Die obigen Formeln gelten sinngemäß auch für $N = 60$ mit $PSL(4,2)$ anstelle von $PSL(3,2)$, sowie auch für $N = 92$ mit $M23$ anstelle von $PSL(3,2)$ (s. Tabellenwerk).

Bei den nun folgenden Beispielen habe ich zunächst die Codeliste der zyklischen Codes der Länge $N = 20$ abgedruckt, sowie anschließend die Automorphismengruppen Nr. 3 und 4 (von 8) mit ihren Kompositionsfaktoren im Magma-Originalformat.
Man sieht, daß die Struktur der Automorphismengruppen nicht auf Anhieb erkennbar ist. Daran anschließend habe ich beide Beispiele zur Verdeutlichung der Kranzproduktstruktur mit Trennlinien und Kommentaren versehen.
Weitere Beispiele kann kann man jederzeit von der beiliegenden CD ausdrucken.

[5] siehe dazu auch Formel (1.30)

Beispiel 1.32 ($N = 20$ **Liste der zyklischen Codes)**

```
Lineare Permutations-Gruppencodes der Laenge N = 20
der zyklischen Permutationsgruppe

Lfd.Nr.  k   d     #PermGrp          #AutoGrp

   1    18   2         20     26336378880000
   2     2  10         20     26336378880000
   3    17   2         20         4976640000
   4     3  10         20         4976640000
   5    16   2         20         4976640000
   6     4   5         20         4976640000
   7    16   2         20          955514880
   8     4   8         20          955514880
   9    15   2         20          955514880
  10     5   4         20          955514880
  11    14   2         20            3932160
  12     6   4         20            3932160
  13    13   4         20             737280
  14     7   4         20             737280
  15    12   2         20           29491200
  16     8   4         20           29491200
  17    12   4         20               2880
  18     8   4         20               2880
  19    11   2         20         3715891200
  20     9   4         20         3715891200
  21    10   2         20         3715891200

Es wurden 21 verschiedene Codes gefunden
abzueglich der Codes, bei denen die Automorphismengruppe aufloesbar ist,
oder gleich der alternierenden oder der symmetrischen Gruppe vom Grad 20 ist

CPU Zeit = 0.76 Sekunden
```

Beispiel 1.33 ($N = 20$, **Originaldruck der Kompositionsfaktoren) (von der 3. Automorphismen-Gruppe)**

```
3 . Automorphismen-Gruppe mit 955514880 Elementen
Permutation group PG acting on a set of cardinality 20
Order = 955514880 = 2^18 * 3^6 * 5

    G
    |  Cyclic(2)
    *
    |  Alternating(5)
    *
    |  Cyclic(2)
    *
    |  Cyclic(3)
    *
    |  Cyclic(2)
    *
    |  Cyclic(2)
    *
    |  Cyclic(2)
    *
    |  Cyclic(3)
    *
    |  Cyclic(2)
    *
    |  Cyclic(2)
    *
    |  Cyclic(2)
    *
    |  Cyclic(3)
    *
    |  Cyclic(2)
    *
    |  Cyclic(2)
    *
    |  Cyclic(2)
    *
    |  Cyclic(3)
    *
    |  Cyclic(2)
    *
    |  Cyclic(2)
    *
    |  Cyclic(2)
    *
    |  Cyclic(3)
    *
    |  Cyclic(2)
    *
    |  Cyclic(2)
    1
```

Beispiel 1.34 ($N = 20$, **Originaldruck der Kompositionsfaktoren) (von der 4. Automorphismen-Gruppe)**

```
4 . Automorphismen-Gruppe mit 3932160 Elementen
Permutation group PG acting on a set of cardinality 20
Order = 3932160 = 2^18 * 3 * 5

    G
    |  Cyclic(2)
    *
    |  Alternating(5)
    *
    |  Cyclic(2)
    *
    |  Cyclic(2)
    *
    |  Cyclic(2)
    *
    |  Cyclic(2)
    *
    |  Cyclic(2)
    *
    |  Cyclic(2)
    *
    |  Cyclic(2)
    *
    |  Cyclic(2)
    *
    |  Cyclic(2)
    *
    |  Cyclic(2)
    *
    |  Cyclic(2)
    *
    |  Cyclic(2)
    *
    |  Cyclic(2)
    *
    |  Cyclic(2)
    *
    |  Cyclic(2)
    *
    |  Cyclic(2)
    1
```

Beispiel 1.35 ($N = 20$**, mit Grenzlinien der Kranzproduktstruktur** $\mathfrak{S}_4 \wr \mathfrak{S}_5$**)**

```
3 . Automorphismen-Gruppe mit 955514880 Elementen
Permutation group PG acting on a set of cardinality 20
Order = 955514880 = 2^18 * 3^6 * 5

    G
    |  Cyclic(2)      \
    *                   >=Sym(5) innere Permutationsgruppe des Kranzes
    |  Alternating(5) /
    * ================
    |  Cyclic(2)      \
    *                   \
    |  Cyclic(3)        \
    *                     >=Sym(4) Gruppe 1 des Aussenkranzes
    |  Cyclic(2)        /
    *                   /
    |  Cyclic(2)      /
    * ----------------
    |  Cyclic(2)
    *
    |  Cyclic(3)
    *
    |  Cyclic(2)
    *
    |  Cyclic(2)
    * ----------------
    |  Cyclic(2)
    *
    |  Cyclic(3)
    *
    |  Cyclic(2)
    *
    |  Cyclic(2)
    * ----------------
    |  Cyclic(2)
    *
    |  Cyclic(3)
    *
    |  Cyclic(2)
    *
    |  Cyclic(2)
    * ----------------
    |  Cyclic(2)      \
    *                   \
    |  Cyclic(3)        \
    *                     >=Sym(4) Gruppe 5 des Aussenkranzes
    |  Cyclic(2)        /
    *                   /
    |  Cyclic(2)      /
    1 ----------------
```

Beispiel 1.36 ($N = 20$**, mit Grenzlinien der Kranzproduktstruktur** $\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_5$**)**

```
4 . Automorphismen-Gruppe mit 3932160 Elementen
Permutation group PG acting on a set of cardinality 20
Order = 3932160 = 2^18 * 3 * 5

      1-2-3------------Kranzebene (von innen nach aussen)
   G
   |  Cyclic(2)      \
   *                  >=Sym(5) innerste Permutationsgruppe des Kranzes
   |  Alternating(5) /
    * ###############
     |  Cyclic(2)      =Sym(2) Permutationsgruppe 1 von 5 des Zwischenkranzes
      * ==============
       |  Cyclic(2)       =Sym(2) Gruppe 1 des 1. Aussenkranzes zum Zw.-kranz
        * ---------------
       |  Cyclic(2)       =Sym(2) Gruppe 2 des 1. Aussenkranzes zum Zw.-kranz
    * ###############
     |  Cyclic(2)      =Sym(2) Permutationsgruppe 2 von 5 des Zwischenkranzes
      * ==============
       |  Cyclic(2)       =Sym(2) Gruppe 1 des 2. Aussenkranzes zum Zw.-kranz
        * ---------------
       |  Cyclic(2)       .....u.s.w.
    * ###############
     |  Cyclic(2)
      * ==============
       |  Cyclic(2)
        * ---------------
       |  Cyclic(2)
    * ###############
     |  Cyclic(2)
      * ==============
       |  Cyclic(2)
        * ---------------
       |  Cyclic(2)       .......
    * ###############
     |  Cyclic(2)      =Sym(2) Permutationsgruppe 5 von 5 des Zwischenkranzes
      * ==============
       |  Cyclic(2)
        * ---------------
       |  Cyclic(2)
   1
```

1.2.3 Zyklische Codes der Länge $N = 8 \cdot j$

Für gerade Codelängen N mit $N = 8 \cdot j$ habe ich noch weitere Gesetzmäßigkeiten entdeckt, die wir im Folgenden formulieren wollen.
Wie in den beiden vorigen Abschnitten gezeigt, existieren für gerade Codelängen $N = 4 \cdot m$ stets die 6 beschriebenen Automorphismengruppen mit den zugehörigen 17 zyklischen Codes.

Die hier im Folgenden gemachten Aussagen stellen eine Zusammenfassung der Erkenntnisse aus dem umfangreichen Listen- und Tabellenwerk dar und sind für die Codelängen N = 40, 48, 56, 64, 72, 80, 88, 96 anhand der identifizierten Automorphismengruppen und deren zugehörige Codes exemplarisch überprüft worden.

Beobachtung 1.37 (Teil 1)
Sei N durch 8 teilbar ($N = 8 \cdot j$ und $j \geq 5$).
Dann gilt: Es gibt mindestens 10 weitere Automorphismengruppen:

$$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_j \wr \mathfrak{S}_2 \tag{1.49}$$

$$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_j \tag{1.50}$$

$$\mathfrak{S}_j \wr \mathfrak{S}_8 \tag{1.51}$$

$$\mathfrak{S}_8 \wr \mathfrak{S}_j \tag{1.52}$$

$$\mathfrak{S}_j \wr \mathfrak{S}_2 \wr \mathfrak{S}_4 \tag{1.53}$$

$$\mathfrak{S}_j \wr \mathfrak{S}_4 \wr \mathfrak{S}_2 \tag{1.54}$$

$$\mathfrak{S}_4 \wr \mathfrak{S}_2 \wr \mathfrak{S}_j \tag{1.55}$$

$$\mathfrak{S}_4 \wr \mathfrak{S}_j \wr \mathfrak{S}_2 \tag{1.56}$$

$$\mathfrak{S}_2 \wr \mathfrak{S}_4 \wr \mathfrak{S}_j \tag{1.57}$$

$$\mathfrak{S}_2 \wr \mathfrak{S}_j \wr \mathfrak{S}_4 \tag{1.58}$$

Bemerkung 1.38
Bei den obengenannten 10 weiteren Kranzprodukten fällt folgendes auf (wir werden das im nächsten Teilabschnitt zusammenfassen):
Haben wir nur 2 Kranzfaktoren, so existieren auch beide Vertauschungen als Kranzprodukte. Zu jedem dieser beiden Kranzprodukte gehören 4 Codes, nämlich 2 bezüglich der Dimension k benachbarte Codes und deren zuhörige duale Codes.
Dabei gibt es noch den Sonderfall $j = 8$; also für $N = 64$ fallen diese beiden Kranzprodukte zusammen. Die Anzahl der zugehörigen Codes bleibt bei 4.

Haben wir 3 Kranzfaktoren, so existieren ebenfalls alle Vertauschungen (also 6) als Kranzprodukte.
Von diesen 6 Kranzprodukten mit je 3 Faktoren sind noch einmal 2 ausgezeichnet, die nämlich die $\mathfrak{S}_2$ als ersten Faktor haben: Zu jedem dieser beiden Kranzprodukte gehören ebenfalls 4 Codes, nämlich 2 bezüglich der Dimension k benachbarte Codes und deren zuhörige duale Codes.
Haben wir jedoch 4 Kranzfaktoren, so permutieren nur die letzten beiden Faktoren; als erste beide Faktoren haben wir konstant $\mathfrak{S}_2 \wr \mathfrak{S}_2$.

Beobachtung 1.39 (Teil 2)
Falls j ungerade, so existieren auch noch

$$\mathfrak{S}_8 \times \mathfrak{S}_j \tag{1.59}$$

$$(\mathfrak{S}_2 \wr \mathfrak{S}_4) \times \mathfrak{S}_j \tag{1.60}$$

$$(\mathfrak{S}_4 \wr \mathfrak{S}_2) \times \mathfrak{S}_j \tag{1.61}$$

$$\mathfrak{S}_j \times (\mathfrak{S}_4 \wr \mathfrak{S}_2) \tag{1.62}$$

$$\mathfrak{S}_j \times (\mathfrak{S}_2 \wr \mathfrak{S}_4) \tag{1.63}$$

$$(\mathfrak{S}_j \times \mathfrak{S}_4) \wr \mathfrak{S}_2 \tag{1.64}$$

$$\mathfrak{S}_2 \wr (\mathfrak{S}_j \times \mathfrak{S}_4) \tag{1.65}$$

$$\mathfrak{S}_2 \wr (\mathfrak{S}_j \times (\mathfrak{S}_2 \wr \mathfrak{S}_2)) \tag{1.66}$$

$$\mathfrak{S}_2 \wr (\mathfrak{S}_2 \times \mathfrak{S}_j) \wr \mathfrak{S}_2)) \tag{1.67}$$

Bemerkung 1.40
Der Beweis der obigen Existenzaussagen ergibt sich durch Anwendung der im Kapitel 2 „Vererbung von zyklischen Codes und ihren Automorphismengruppen“ bewiesenen Sätze 2.2, 2.19, sowie Satz 3.3.

Korollar 1.41
Unter der Voraussetzung der vorigen Aussagen ($N = 8 \cdot j,\ j \geq 5$) und der Einschränkung $j \neq 8$ gilt:
Die Anzahl der zyklischen Codes ≥ 45. Falls j ungerade ist, so ist die Anzahl der zyklischen Codes ≥ 53.
Die Anzahl der zugehörigen Automorphismengruppen ist ≥ 16 , bzw. ≥ 20.

Bemerkung 1.42
Da die Beispiele mit größeren N sehr raumgreifend sein können, habe ich hier darauf ver-

zichtet. Man kann sie aber jederzeit von der beiliegenden CD ausdrucken.
Bei einigen Codelängen (z.B. $N = 48$, 80, siehe Tabellen im Anhang) treten zusätzlich noch Automorphismengruppen mit verminderten Kranzprodukten auf. Wegen der Komplexität werden sie allgemein im Abschnitt 3.2.2 „Gemischte Produkte“ behandelt.
Für $N = 64$ existieren nach den obigen Ausführungen 41 zyklische Codes mit 15 Automorphismengruppen. Es sind ausschließlich Kranzprodukte, so wie auch bei $N = 16$ und $N = 32$. Daher haben wir diese Beobachtung unter 2.20 formuliert.

1.2.4 Zyklische Codes der Länge $N = 2^r \cdot i, (i$ ungerade$)$

Sei i ungerade, denn – falls i gerade, gäbe es die Darstellung $N = 2^{r+1} \cdot (i/2)$.
Nun wollen wir die bisher beobachteten und beschriebenen Gesetzmäßigkeiten zusammenfassen und allgemein formulieren und beweisen. Wir wollen das in Form einer Rekursionsformel beschreiben.
Dabei hängt Anzahl und Gestalt der Gruppenprodukte von r ab.

Satz 1.43
Sei N weiterhin gerade $(N = 2^r \cdot i, r \geq 3)$*, i ungerade und* $i \geq 5$*).*
Dann gilt: Zusätzlich zu den Automorphismengruppen aus Kranzprodukten, die bereits durch Faktorzerlegungen von $(N = 2^t \cdot h, t < r)$ *existieren (siehe hierzu auch die früheren Abschnitte für* $t = 1, 2, 3$*), gibt es weitere Automorphismengruppen mit Kranzprodukten – zunächst mit* 2 *Faktoren:*

$$\mathfrak{S}_i \wr \mathfrak{S}_2^r$$

$$\mathfrak{S}_2^r \wr \mathfrak{S}_i.$$

Dazu gehören jeweils 4 *Codes.*
Darüberhinaus gibt es weitere Automorphismengruppen mit Kranzprodukten in allen Permutationen der folgenden 3 *Faktoren (solange* $s < r - s$*):*

$$\mathfrak{S}_i, \mathfrak{S}_2, \mathfrak{S}_{2^{r-1}}$$

$$\mathfrak{S}_i, \mathfrak{S}_{2^2}, \mathfrak{S}_{2^{r-2}}$$

$$\vdots$$

$$\mathfrak{S}_i, \mathfrak{S}_{2^s}, \mathfrak{S}_{2^{r-s}}.$$

Falls r gerade ist, so existiert in der letzten Zeile ein s mit $s = r - s$ *und es gibt* 3 *Kranzprodukte mit den Faktoren*

$$\mathfrak{S}_i, \mathfrak{S}_{2^s}, \mathfrak{S}_{2^s}.$$

Die Anzahl dieser Kranzprodukte mit 3 *Faktoren ist* $((r-1)/2) \cdot 3!$.

Falls $r \geq 4$*, so gibt es weitere Automorphismengruppen mit Kranzprodukten in allen Permutationen der folgenden* 4 *Faktoren (solange* $s < r - (s+1)$*):*

$$\mathfrak{S}_i, \mathfrak{S}_2, \mathfrak{S}_2, \mathfrak{S}_{2^{r-2}}$$

$$\mathfrak{S}_i, \mathfrak{S}_2, \mathfrak{S}_{2^2}, \mathfrak{S}_{2^{r-3}}$$

$$\vdots$$

$$\mathfrak{S}_i, \mathfrak{S}_2, \mathfrak{S}_{2^s}, \mathfrak{S}_{2^{r-(s+1)}}.$$

Falls r *ungerade ist, so existiert in der letzten Zeile ein* s *mit* $s = r - (s+1)$ *und es gibt* 12 *Kranzprodukte mit den Faktoren*

$$\mathfrak{S}_i, \mathfrak{S}_2, \mathfrak{S}_{2^s}, \mathfrak{S}_{2^s}.$$

Die Anzahl dieser Kranzprodukte mit 4 *Faktoren ist* $((r-3)/2) \cdot 4!$*.*
Usw., wobei mit größerem r *die möglichen Wiederholungen von Faktoren, wie* $\mathfrak{S}_2$ *oder* $\mathfrak{S}_4$*, etc. zunehmen. Die Anzahl der Kranzprodukte aus allen Permutationen dieser Faktoren kann mithilfe der Kombinatorik ermittelt werden.*
Das geht so weiter, bis schließlich $r!/(r-2)!$ *Kranzprodukte mit* r *Faktoren durch Permutation gebildet werden können:*

$$\underbrace{\mathfrak{S}_i \wr \mathfrak{S}_2 \wr \ldots \wr \mathfrak{S}_2 \wr \mathfrak{S}_4}_{r \ \textit{Faktoren}}$$

Darüberhinaus existieren stets 2 *Automorphismengruppen mit folgenden beiden Kranzprodukten:*

$$\mathfrak{S}_2 \wr \ldots \wr \mathfrak{S}_2 \wr \mathfrak{S}_i \wr \mathfrak{S}_2$$

$$\underbrace{\mathfrak{S}_2 \wr \ldots \wr \mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_i}_{(r+1) \ \textit{Faktoren}}$$

Beweis. Der Beweis ergibt sich durch Anwendung der im Kapitel 2 „Vererbung von zyklischen Codes und ihren Automorphismengruppen“ bewiesenen Sätze. □

1.3 Zyklische Codes, deren Länge durch eine ungerade Primzahl teilbar ist

Nun wollen wir uns den zyklischen Codes zuwenden, deren Länge $N = q \cdot l$ ist, mit $2 \neq q$ prim. N ist also ein Vielfaches einer ungeraden Primzahl. Beginnen wir mit $q = 3$.

Es sei an dieser Stelle daran erinnert, daß wir unter dem **Kranzprodukt**

$$\mathfrak{G} \wr \mathfrak{H}$$

stets das sog. **Permutations-Kranzprodukt** verstehen, so wie es auch in **Magma** implementiert ist.

1.3.1 Zyklische Codes der Länge $N = 3 \cdot l$

Wir werden zunächst keine weiteren Voraussetzungen für l fordern, außer $l \geq 5$, d.h., wir werden ungerade Vielfache und gerade Vielfache von 3 gemeinsam als Codelängen betrachten.
Die Unterschiede (z.B. selbstduale Codes) werden später behandelt.

Bezeichnung 1.44
Sei $N \in \mathbb{N}$ durch 3 teilbar, ($N = 3 \cdot l$ mit $l \geq 5$)[6] und sei
$u = (1, 0, 0, 1, 0, 0, 1, 0, 0, \ldots) \in \mathbb{F}_2^N$,
$v = (0, 1, 0, 0, 1, 0, 0, 1, 0, \ldots) \in \mathbb{F}_2^N$,
$w = (0, 0, 1, 0, 0, 1, 0, 0, 1, \ldots) \in \mathbb{F}_2^N$.
Dann sei $C_3 := \langle u, v, w \rangle$ der aus u, v und w erzeugte Code.

Wir beweisen nun einen ersten einfachen Satz:

Hilfssatz 1.45
C_3 ist zyklisch. Es ist $\dim(C_3) = 3$.

Beweis. Da die Vektoren u, v und w linear unabhängig sind, erzeugen sie einen 3-dimensionalen Unterraum C_3. Man überzeugt sich leicht, daß jede zyklische Verschiebung eines jeden Vektors aus C_3 wieder einen Vektor aus C_3 ergibt. Damit erfüllt C_3 die Kriterien eines zyklischen Codes. □

Wir beweisen nun einen weiteren einfachen Satz:

Hilfssatz 1.46
Sei C_3 der in 1.44 definierte Code. Dann gilt:
C_3 hat die Minimaldistanz $d = l = \frac{N}{3}$, d.h., C_3 ist ein linearer $[N, 3, \frac{N}{3}]$-Code.

[6] Die Einschränkung $l \geq 5$ hängt mit der Forderung zusammen, daß die Automorphismengruppe nicht auflösbar sein soll. Geht man von dieser Forderung ab, so kann man auch diese Voraussetzung fallen lassen.

Beweis. Nach der Definition der Minimaldistanz in MacWilliams [16] Ch1, §3 ist leicht zu sehen, daß alle drei Basisvektoren u, v und w in genau l Positionen vom Nullvektor verschieden sind. Die Summen je zweier dieser Basisvektoren sind in genau l Positionen vom Einsvektor verschieden. Eine kleinere, von Null verschiedene Hammingdistanz wird von Codevektoren aus C_3 nicht angenommen. □

Nun wollen wir drei wichtige Sätze über die Automorphismengruppe $Aut(C_2)$ formulieren und beweisen:

Lemma 1.47
Sei C_3 der in 1.44 definierte Code. Dann gilt:

$$\mathfrak{S}_3 \leq Aut(C_3). \tag{1.68}$$

Beweis. Sei $c = (a_1, b_1, c_1, a_2, b_2, c_2, \ldots)$ ein Codevektor. Dann ist $(c_1, b_1, a_1, c_2, b_2, a_2, \ldots)$ ebenfalls ein Codevektor. Dies definiert eine Operation der symmetrischen Gruppe $\mathfrak{S}_3$ auf $\mathbb{F}_2^N$, die den Code C_3 invariant läßt. □

Lemma 1.48
Sei C_3 der in 1.44 definierte Code. Dann gilt:

$$\mathfrak{S}_l \leq Aut(C_3). \tag{1.69}$$

Beweis. Sei $c = ((a_1, b_1, c_1), (a_2, b_2, c_2), \ldots)$ ein Codevektor.
Dann ist $((a_2, b_2, c_2), (a_1, b_1, c_1), \ldots)$ ebenfalls ein Codevektor. Dies definiert eine Operation der symmetrischen Gruppe $\mathfrak{S}_l$ auf $\mathbb{F}_2^N$, die den Code C_3 invariant läßt. □

Lemma 1.49
Sei C_3 der in 1.44 definierte Code. Dann gilt:

$$\mathfrak{S}_l \times \mathfrak{S}_l \times \mathfrak{S}_l \leq Aut(C_3). \tag{1.70}$$

Beweis. Sei $c = (a_1, b_1, c_1, a_2, b_2, c_2, \ldots, a_l, b_l, c_l)$ ein Codevektor. Dann können zum einen die a_i permutiert werden und zum anderen die b_i, sowie auch die c_i. Dies definiert eine Operation der Gruppe $\mathfrak{S}_l \times \mathfrak{S}_l \times \mathfrak{S}_l$ auf $\mathbb{F}_2^N$, die den Code C_3 invariant läßt. □

Satz 1.50 (Zentraler Satz für zyklische Codes der Länge $(N = 3 \cdot l)$, Teil 1)
Sei C_3 der in 1.44 definierte Code. Dann gilt:

$$\mathfrak{S}_l \wr \mathfrak{S}_3 \cong Aut(C_3).$$

Beweis. Die Gruppe von linearen Abbildungen, die von $\mathfrak{S}_3$ und $\mathfrak{S}_l \times \mathfrak{S}_l \times \mathfrak{S}_l$ (nach Satz 1.47 und Satz 1.49) erzeugt wird, ist isomorph zum Kranzprodukt $\mathfrak{S}_l \wr \mathfrak{S}_3$.
Die Argumentation ist analog zum Beweis vom Satz 1.12. □

Bemerkung 1.51
Anders, als bei den Codes gerader Länge[7] mit $N = 2 \cdot l$ stellen wir hier ($N = 3 \cdot l$, ungerade oder gerade) fest, daß es insgesamt 4 Codes mit der Automorphismengruppe $Aut(C_3)$ gibt, nämlich:

1. der Code C_3 selbst,
2. der zu C_3 duale Code $C^{\perp}$,
3. ein zu C_3 dimensionsmäßig benachbarter Code C' mit Minimaldistanz $2 \cdot l$, also ein $[N, 2, 2l]$-Code und
4. der dazu duale Code $C'^{\perp}$, ein $[N, N-2, 2]$-Code.

Ende der Bemerkung

Wenn wir uns noch einmal den Code C_3 genauer ansehen, stellen wir fest, daß die drei erzeugenden Vektoren u, v und w zusammen eine Aneinanderreihung von l Einheitsmatrizen der Dimension 3 darstellen. Dieses Gebilde ist die Generatormatix des Codes C_3. Dieses Konstruktionsprinzip werden wir auch im Folgenden verwenden (jetzt bauen wir ein Gebilde aus 3 Einheitsmatrizen der Dimension l, das ist dann die Generatormatrix des neuen Codes C_l):

Bezeichnung 1.52
Sei $N \in \mathbb{N}$ durch 3 teilbar, ($N = 3 \cdot l$ mit $l \geq 5$) und sei
$x_1 = (1,0,0,\ldots,0,1,0,0,\ldots,0,1,0,0,\ldots,0) \in \mathbb{F}_2^N$,
$x_2 = (0,1,0,\ldots,0,0,1,0,\ldots,0,0,1,0,\ldots,0) \in \mathbb{F}_2^N$,
$\ldots\ldots\ldots\ddots\ldots\ldots\ldots$
$\ldots\ldots\ldots\ddots\ldots\ldots$
$x_l = (0,0,0,\ldots,1,0,0,0,\ldots,1,0,0,0,\ldots,1) \in \mathbb{F}_2^N$.
Dann sei $C_l := \langle x_1, x_2, \cdots, x_l \rangle$ der aus den x_i erzeugte Code.

Wir beweisen nun einen einfachen Satz:

Hilfssatz 1.53
C_l ist zyklisch. Es ist $\dim(C_l) = l = \dfrac{N}{3}$.

Beweis. Da die Vektoren x_1 bis x_l alle linear unabhängig sind, erzeugen sie einen l-dimensionalen Unterraum C_l. Man überzeugt sich leicht, daß jede zyklische Verschiebung eines jeden Vektors aus C_l wieder einen Vektor aus C_l ergibt. Damit erfüllt C_l die Kriterien eines zyklischen Codes. □

[7] dort gab es nur 2 Codes. Warum das so ist, werden wir im Abschnitt 2.1 „Elementarcodes“ im Kapitel 2 „Vererbung“ sehen.

Wir beweisen nun einen weiteren einfachen Satz:

Hilfssatz 1.54
Sei C_l der in 1.52 definierte Code. Dann gilt:
C_l hat die Minimaldistanz d=3, d.h., C_l ist ein linearer $[N, \frac{N}{3}, 3]$-Code ($l = \frac{N}{3}$).

Beweis. Nach der Definition der Minimaldistanz in MacWilliams [16] Ch1, §3 ist leicht zu sehen, daß die x_i in genau 3 Positionen vom Nullvektor verschieden sind. Auch durch Summenbildung einzelner x_i ist eine von Null verschiedene Hammingdistanz nicht unter den Wert von 3 zu bringen. □

Satz 1.55 (Zentraler Satz für zyklische Codes der Länge $(N = 3 \cdot l)$, Teil 2)
Sei C_l der in 1.52 definierte Code. Dann gilt:
Die zugehörige Automorphismengruppe des Codes C_l ist isomorph zum folgenden Kranzprodukt:

$$Aut(C_l) \cong \mathfrak{S}_3 \wr \mathfrak{S}_l. \tag{1.71}$$

Beweis. Die Argumentation ist analog zum Beweis vom Satz 1.12. □

Korollar 1.56
Es gibt insgesamt genau 4 zyklische Codes mit derselben Automorphismengruppe $Aut(C_l)$, nämlich:

1. *den Code C_l selbst,*
2. *den zu C_l dualen Code $C_l^{\perp}$, ein $[N, N-l, 2]$-Code ($\frac{2N}{3} = N - l$).*
3. *den $[N, l-1]$ - Code (dieser Code hat die Minimaldistanz $6 = 2 \cdot 3$) und*
4. *den $[N, N-l+1]$ - Code. Diese beiden letzten Codes sind nach Lemma 0.28 zueinander dual.*

Der $[N, N-l+1]$ - Code wird von dem Vektor $x = (1, 1, 1, \ldots, 1, 0, 0, 0, \ldots, 0)$ erzeugt, wobei sich die erste 0 an der Stelle $l+1$ befindet.
Der $[N, l-1]$ - Code wird von dem Vektor $x = (1, 1, 0, 0 \ldots, 0, 1, 1, 0, \ldots, 0)$ erzeugt, wobei sich die dritte 1 an der Stelle $l+1$ befindet.

Beweis. Wir werden das im Kapitel „Vererbung“ allgemein beweisen (Sätze 2.3 bis 2.2, angewandt auf den **„zweiten Elementarcode“**, s. Abschnitt 2.1). □

Bemerkung 1.57
Weiterhin wurde bemerkt, daß, sofern l kein Vielfaches von 3 ist, so existiert auch noch[8]

$$\mathfrak{S}_3 \times \mathfrak{S}_l \tag{1.72}$$

[8] die erste Aussage beweisen wir allgemein im Satz 3.3

und – sofern zusätzlich eine Spezialgruppe existiert, die auf einer Menge Ω der Kardinalität l transitiv operiert – auch

$$\mathfrak{S}_3 \times Spezialgruppe_l \tag{1.73}$$

Ein einfaches Beispiel für die zyklischen Codes ungerader Codelänge $N = 3 \cdot l$ und ihrer Automorphismengruppen finden wir anschließend:

Beispiel 1.58 ($N = 27$ **Liste der zyklischen Codes u. Automorphismengruppen)**

```
Zyklische Codes der Laenge N = 27

Lfd.Nr.  k   d     #PermGrp          #AutoGrp

   1    25   2         27 286708355039232000
   2     2  18         27 286708355039232000
   3    24   2         27 286708355039232000
   4     3   9         27 286708355039232000
   5    19   2         27      3656994324480
   6     8   6         27      3656994324480
   7    18   2         27      3656994324480
   8     9   3         27      3656994324480

Es wurden 8 verschiedene Codes gefunden
abzueglich der Codes, bei denen die Automorphismengruppe aufloesbar ist,
oder gleich der alternierenden oder der symmetrischen Gruppe vom Grad 27 ist

CPU Zeit = 2.07 Sekunden

Es wurden 2 verschiedene Automorphismengruppen ueber
alle Codes gefunden:

1 . Automorphismen-Gruppe mit 286708355039232000 Elementen  -
    Haeufigkeit dieser Gruppe: 4 mal

    G
    |  Cyclic(2)        \
    *                    >=Sym(3)
    |  Cyclic(3)        /
    * ==================
    |  Cyclic(2)        \
    *                    >=Sym(9)
    |  Alternating(9)   /
    *-------------------
    |  Cyclic(2)        \
    *                    >=Sym(9)
    |  Alternating(9)   /
    *-------------------
    |  Cyclic(2)        \
    *                    >=Sym(9)
    |  Alternating(9)   /
    *-------------------
    1
```

```
2 . Automorphismen-Gruppe mit 3656994324480 Elementen  -
    Haeufigkeit dieser Gruppe: 4 mal

    G
    |  Cyclic(2)       \
    *                   >=Sym(9)
    |  Alternating(9)  /
    *===================
    |  Cyclic(2)       \
    *                   >=Sym(3)
    |  Cyclic(3)       /
    *-------------------
    |  Cyclic(2)       \
    *                   >=Sym(3)
    |  Cyclic(3)       /
    *-------------------
    |  Cyclic(2)       \
    *                   >=Sym(3)
    |  Cyclic(3)       /
    *-------------------
    |  Cyclic(2)       \
    *                   >=Sym(3)
    |  Cyclic(3)       /
    *-------------------
    |  Cyclic(2)       \
    *                   >=Sym(3)
    |  Cyclic(3)       /
    *-------------------
    |  Cyclic(2)       \
    *                   >=Sym(3)
    |  Cyclic(3)       /
    *-------------------
    |  Cyclic(2)       \
    *                   >=Sym(3)
    |  Cyclic(3)       /
    *-------------------
    |  Cyclic(2)       \
    *                   >=Sym(3)
    |  Cyclic(3)       /
    *-------------------
    |  Cyclic(2)       \
    *                   >=Sym(3)
    |  Cyclic(3)       /
    *-------------------
    1

CPU Zeit = 0.06 Sekunden
Checksum = 8
```

Die Kompositionsfaktoren der Automorphismengruppen werden im Computeralgebrasystem Magma von oben ($G = Aut(C)$) nach unten (1) gelistet. Dies entspricht beim Bild des Kranzes der Richtung von innen nach außen. Zur Verdeutlichung habe ich in den Beispielen die innere Permutationsgruppe $\mathfrak{H}$ von dem äußeren Kranz durch eine doppelte Trennlinie

```
================
```

abgesetzt, sowie die einzelnen Kopien der äußeren Gruppe $\mathfrak{G}$ auf dem Kranz durch eine einfache Trennlinie

```
----------------
```

von einander separiert.

Bemerkung 1.59
Die im obigen Beispiel mit den laufenden Nummern 4 und 8 bezeichneten Codes entsprechen unseren Definitionen. Daher wollen wir hier die Generatormatrizen beider Codes mit aufführen:

```
Lfd.Nr.  k   d     #PermGrp          #AutoGrp

   4     3   9         27 286708355039232000

[27, 3, 9] Cyclic Linear Code over GF(2)
Generator matrix:
[1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0]
[0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0]
[0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1]

Lfd.Nr.  k   d     #PermGrp          #AutoGrp

   8     9   3         27      3656994324480

[27, 9, 3] Cyclic Linear Code over GF(2)
Generator matrix:
[1 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0]
[0 1 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0]
[0 0 1 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0]
[0 0 0 1 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 1 0 0 0 0 0]
[0 0 0 0 1 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 1 0 0 0 0]
[0 0 0 0 0 1 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 1 0 0 0]
[0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 1 0 0]
[0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 1 0]
[0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 1]
```

Wir wollen nun auf die Unterschiede zwischen ungeraden und geraden Codelängen eingehen. Dazu zunächst zwei einfache Aussagen:

Fakt 1.60
Für ungerade Codelängen existieren keine sebstdualen Codes.

Korollar 1.61
Für ungerades N ist die Anzahl der zyklischen Codes gerade.

Beweis. trivial: Da es nach Lemma 0.28 zu jedem zyklischen $[N, k]$-Code genau einen dazu dualen $[N, N-k]$-Code gibt, (und darüberhinaus für ungerades N keine selbstdualen Codes existieren) ist somit die Anzahl der zyklischen Codes ungerader Länge gerade. □

Nun wollen wir uns besonders mit den geraden Codelängen $N = 3 \cdot l$ befassen.
Das bedeutet, daß l darstellbar ist als $l = 2 \cdot m$. Man kann nun die Codelänge N einerseits als Vielfaches von 3 ($N = 3 \cdot l$), andererseits als Vielfaches von 2 ($N = 2 \cdot (3 \cdot m)$) ansehen.
Ein überschaubares Beispiel hierfür ist die Codelänge $N = 18$:
Aus der ersten Eigenschaft ($N = 3 \cdot 6$) resultieren 8 Codes mit 2 Automorphismengruppen, wie in diesem Abschnitt besprochen,
aus der zweiten Eigenschaft ($N = 2 \cdot 9$) resultieren 5 Codes mit 2 Automorphismengruppen, wie im Abschnitt 1.2 „Zyklische Codes gerader Länge“ Unterabschnitt „Zyklische Codes der Länge $N = 2 \cdot l$“ besprochen (die Variable l wird hier in dem Beispiel jetzt leider mit zwei unterschiedlichen Werten verwendet).
Damit bekommen wir aus beiden Eigenschaften insgesamt 13 Codes mit 4 Automorphismengruppen (siehe Tabelle zu $N = 18$ im Anhang). Der selbstduale Code gehört zur zweiten Eigenschaft.

Abhängig von der Zerlegung $l = 2 \cdot m$ existieren mit $m \geq 5$ für $N = 3 \cdot l$ noch weitere Codes und Automorphismengruppen. Wir wollen das jetzt hier zusammenfassen: Wie weiter oben gezeigt, existieren für die Codelängen $N = 3 \cdot l$ unter der Voraussetzung $l \geq 5$ stets die beiden Automorphismengruppen:

$$\mathfrak{S}_l \wr \mathfrak{S}_3 \tag{1.74}$$

$$\mathfrak{S}_3 \wr \mathfrak{S}_l \tag{1.75}$$

und die zugehörigen 8 zyklischen Codes.
Weiterhin finden wir – – sofern zusätzlich eine Spezialgruppe existiert, die auf einer Menge Ω der Kardinalität l transitiv operiert – auch

$$Spezialgruppe_l \wr \mathfrak{S}_3, \tag{1.76}$$

$$\mathfrak{S}_3 \wr Spezialgruppe_l. \tag{1.77}$$

Ist darüberhinaus $l = 2 \cdot m$ mit $m \geq 5$ für $N = 3 \cdot l$, so existieren noch zusätzlich die

folgenden Automorphismengruppen:

$$\mathfrak{S}_6 \wr \mathfrak{S}_m \tag{1.78}$$

$$\mathfrak{S}_m \wr \mathfrak{S}_6 \tag{1.79}$$

$$\mathfrak{S}_2 \wr \mathfrak{S}_3 \wr \mathfrak{S}_m \tag{1.80}$$

$$\mathfrak{S}_2 \wr \mathfrak{S}_m \wr \mathfrak{S}_3 \tag{1.81}$$

$$\mathfrak{S}_3 \wr \mathfrak{S}_2 \wr \mathfrak{S}_m \tag{1.82}$$

$$\mathfrak{S}_3 \wr \mathfrak{S}_m \wr \mathfrak{S}_2 \tag{1.83}$$

$$\mathfrak{S}_m \wr \mathfrak{S}_2 \wr \mathfrak{S}_3 \tag{1.84}$$

$$\mathfrak{S}_m \wr \mathfrak{S}_3 \wr \mathfrak{S}_2 \tag{1.85}$$

Dabei werden die ersten 4 Automorphismengruppen von je 4 Codes angenommen, die letzten 4 Automorphismengruppen nur jeweils von 2 Codes.
Ist m ungerade, aber kein Vielfaches von 3 (d.h., 6 teilerfremd zu m), so existiert auch noch

$$\mathfrak{S}_6 \times \mathfrak{S}_m. \tag{1.86}$$

(diese Automorphismengruppe wird ebenfalls von 4 Codes angenommen)
und – sofern zusätzlich eine Spezialgruppe existiert, die auf einer Menge Ω der Kardinalität m transitiv operiert – auch

$$\mathfrak{S}_6 \times Spezialgruppe_m \tag{1.87}$$

Der Beweis, sowie weitere zusätzlich auftretende Automorphismengruppen, die auf anderen Konstruktionen beruhen, werden im Kapitel 3 „Zusammenfassung zyklische Codes“, Abschnitt „Zerlegung der Codelänge in 3 Faktoren“ behandelt.

1.3.2 Zyklische Codes der Länge $N = 9 \cdot m$

Für Codelängen N mit $N = 9 \cdot m$ wurden noch weitere Gesetzmäßigkeiten entdeckt.
Die hier im Folgenden gemachten Aussagen stellen eine Zusammenfassung der Erkenntnisse aus dem umfangreichen Listen- und Tabellenwerk dar und sind für die Codelängen N = 45, 54, 63, 72, 81 anhand der identifizierten Automorphismengruppen und deren zugehörige Codes exemplarisch überprüft worden.

Beobachtung 1.62
Sei $N \in \mathbb{N}$ durch 9 teilbar, ($N = 9 \cdot m = 3 \cdot 3 \cdot m$ und $m \geq 5$)[9].

[9]Die Einschränkung $l \geq 5$ hängt mit der Forderung zusammen, daß die Automorphismengruppe nicht auflösbar sein soll. Geht man von dieser Forderung ab, so kann man auch diese Voraussetzung fallen lassen.

Es gilt nun: Es gibt mindestens[10] 5 *weitere Automorphismengruppen:*

$$\mathfrak{S}_3 \wr \mathfrak{S}_3 \wr \mathfrak{S}_m \tag{1.88}$$

$$\mathfrak{S}_3 \wr \mathfrak{S}_m \wr \mathfrak{S}_3 \tag{1.89}$$

$$\mathfrak{S}_m \wr \mathfrak{S}_3 \wr \mathfrak{S}_3 \tag{1.90}$$

$$\mathfrak{S}_m \wr \mathfrak{S}_9 \tag{1.91}$$

$$\mathfrak{S}_9 \wr \mathfrak{S}_m. \tag{1.92}$$

und – falls 9 *teilerfremd zu* m *– noch folgende weitere Gruppenprodukte:*

$$\mathfrak{S}_9 \times \mathfrak{S}_m \tag{1.93}$$

$$(\mathfrak{S}_3 \wr \mathfrak{S}_3) \times \mathfrak{S}_m \tag{1.94}$$

$$\mathfrak{S}_3 \wr (\mathfrak{S}_3 \times \mathfrak{S}_m) \tag{1.95}$$

$$(\mathfrak{S}_m \times \mathfrak{S}_3) \wr \mathfrak{S}_3. \tag{1.96}$$

und – sofern zusätzlich eine Spezialgruppe existiert, die auf einer Menge Ω *der Kardinalität* m *transitiv operiert – noch einmal sämtliche obige Gruppenprodukte mit*

$$Spezialgruppe_m \quad \textbf{anstatt} \quad \mathfrak{S}_m \tag{1.97}$$

Bemerkung 1.63
Die obigen Aussagen lassen sich durch Anwendung der im Kapitel 2 „Vererbung von zyklischen Codes und ihren Automorphismengruppen“ bewiesenen Sätze 2.2, 2.19, sowie Satz 3.3 beweisen.
Bei den obengenannten fünf weiteren Kranzprodukten fällt folgendes auf:
Zunächst finden wir das gleiche Verhalten, wie für $N = 4 \cdot m$:
Haben wir nur 2 Kranzfaktoren, so existieren auch beide Vertauschungen als Kranzprodukte. Zu jedem dieser beiden Kranzprodukte gehören 4 Codes, nämlich 2 bezüglich der Dimension k benachbarte Codes und deren zuhörige duale Codes.
Haben wir jedoch 3 Kranzfaktoren, so permutieren – anders als bei $N = 4 \cdot m$ – nicht nur die letzten beiden Faktoren, sondern alle !
Darum sind es hier auch 5 (statt 4) zusätzliche reine Kranzprodukte.
Darüberhinaus fällt auf, daß wir wesentlich mehr gemischte Gruppenprodukte haben, als bei den geraden Codelängen $N = 4 \cdot m$.
Beispiele: $N = 45, 54, 63, 72$.

[10] falls $m = m_1 \cdot m_2$ zerlegbar ist, so existieren natürlich zusätzlich zu den obigen Gruppen noch weitere Kranzprodukte (siehe dazu auch Kapitel „Zusammenfassung zyklische Codes“, Abschnitte 3.2 und 3.3, sowie Tabellenwerk $N = 54, 72$).

1.3.3 Zyklische Codes der Länge $N = 5 \cdot l$

Bezeichnung 1.64
Sei $N \in \mathbb{N}$ durch 5 teilbar ($N = 5 \cdot l$ mit $l \geq 3$) und sei
$u = (1,0,0,0,0,1,0,0,0,0,1,0,0,0,0,\ldots) \in \mathbb{F}_2^N$,
$v = (0,1,0,0,0,0,1,0,0,0,0,1,0,0,0,\ldots) \in \mathbb{F}_2^N$,
$w = (0,0,1,0,0,0,0,1,0,0,0,0,1,0,0,\ldots) \in \mathbb{F}_2^N$,
$x = (0,0,0,1,0,0,0,0,1,0,0,0,0,1,0,\ldots) \in \mathbb{F}_2^N$,
$y = (0,0,0,0,1,0,0,0,0,1,0,1,0,0,1,\ldots) \in \mathbb{F}_2^N$.
Dann sei $C_5 := \langle u,v,w,x,y \rangle$ der aus u,v,w,x und y erzeugte Code.

Bemerkung 1.65
Da $5 \geq 5$ gilt, konnten wir die Voraussetzung gegenüber früheren Bezeichnungen abschwächen.

Wir beweisen nun einen ersten einfachen Satz:

Hilfssatz 1.66
C_5 ist zyklisch. Es ist $\dim(C_5) = 5$.

Beweis. Da die Vektoren u,v,w,x und y linear unabhängig sind, erzeugen sie einen 5-dimensionalen Unterraum C_5. Man überzeugt sich leicht, daß jede zyklische Verschiebung eines jeden Vektors aus C_5 wieder einen Vektor aus C_5 ergibt. Damit erfüllt C_5 die Kriterien eines zyklischen Codes. □

Wir beweisen nun einen weiteren einfachen Satz:

Hilfssatz 1.67
Sei C_5 der in 1.64 definierte Code. Dann gilt:
C_5 hat die Minimaldistanz $d = l = \frac{N}{5}$, d.h., C_5 ist ein linearer $[N, 5, \frac{N}{5}]$ - Code.

Beweis. Nach der Definition der Minimaldistanz in MacWilliams [16] Ch1, §3 ist leicht zu sehen, daß alle fünf Basisvektoren u,v,w,x und y in genau l Positionen vom Nullvektor verschieden sind. Die Summen je zweier dieser Basisvektoren sind in genau l Positionen vom Einsvektor verschieden. Eine kleinere, von Null verschiedene Hammingdistanz wird von Codevektoren aus C_5 nicht angenommen. □

Nun wollen wir drei wichtige Sätze über die Automorphismengruppe $Aut(C_5)$ formulieren und beweisen:

Lemma 1.68
Sei C_5 der in 1.64 definierte Code. Dann gilt:

$$\mathfrak{S}_5 \leq Aut(C). \tag{1.98}$$

Beweis. Sei $c = (a_1, b_1, c_1, d_1, e_1, a_2, b_2, c_2, d_2, e_2, \ldots, a_l, b_l, c_l, d_l, e_l)$ ein Codevektor.
Dann ist $(e_1, d_1, c_1, b_1, a_1, e_2, d_2, c_2, b_2, a_2, \ldots, e_l, d_l, c_l, b_l, a_l)$ ebenfalls ein Codevektor.

Dies definiert eine Operation der symmetrischen Gruppe $\mathfrak{S}_5$ auf $\mathbb{F}_2^N$, die den Code C_5 invariant läßt. □

Lemma 1.69
Sei C_5 der in 1.64 definierte Code. Dann gilt:

$$\mathfrak{S}_l \leq Aut(C_5). \tag{1.99}$$

Beweis. Sei $c = ((a_1, b_1, c_1, d_1, e_1), (a_2, b_2, c_2, d_2, e_2), \ldots, (a_l, b_l, c_l, d_l, e_l))$ ein Codevektor. Dann ist $((a_2, b_2, c_2, d_2, e_2), (a_1, b_1, c_1, d_1, e_1), \ldots)$ ebenfalls ein Codevektor. Dies definiert eine Operation der symmetrischen Gruppe $\mathfrak{S}_l$ auf $\mathbb{F}_2^N$, die den Code C_5 invariant läßt. □

Lemma 1.70
Sei C_5 der in 1.64 definierte Code. Dann gilt:

$$\underbrace{\mathfrak{S}_l \times \mathfrak{S}_l \times \ldots \times \mathfrak{S}_l}_{5-mal} \leq Aut(C_5). \tag{1.100}$$

Beweis. Sei $c = (a_1, b_1, c_1, d_1, e_1, a_2, b_2, c_2, d_2, e_2, \ldots, a_l, b_l, c_l, d_l, e_l)$ ein Codevektor. Dann können zum einen die a_i permutiert werden und zum anderen die b_i, sowie auch die c_i, usw. bis hin zu den e_i. Dies definiert eine Operation der Gruppe $\underbrace{\mathfrak{S}_l \times \mathfrak{S}_l \times \ldots \times \mathfrak{S}_l}_{5-mal}$ auf $\mathbb{F}_2^N$, die den Code C_5 invariant läßt. □

Satz 1.71 (**Zentraler Satz für zyklische Codes ungerader Länge** ($N = 5 \cdot l$ **mit** $l \geq 3$)**, Teil 1)**
Sei C_5 der in 1.64 definierte Code. Dann gilt:

$$\mathfrak{S}_l \wr \mathfrak{S}_5 \cong Aut(C_5). \tag{1.101}$$

Beweis. Die Gruppe von linearen Abbildungen, die von $\mathfrak{S}_5$ und $\underbrace{\mathfrak{S}_l \times \ldots \times \mathfrak{S}_l}_{5-mal}$ (nach Satz 1.68 und Satz 1.70) erzeugt wird, ist isomorph zum Kranzprodukt $\mathfrak{S}_l \wr \mathfrak{S}_5$. Die Argumentation ist analog zum Beweis vom Satz 1.12. □

Korollar 1.72
Anders, als bei den Codes gerader Länge[11] *mit $N = 2 \cdot l$ stellen wir hier ($N = 5 \cdot l$) fest, daß es insgesamt 4 Codes mit der Automorphismengruppe Aut(C_5) gibt, nämlich:*

1. *der Code C_5 selbst,*
2. *der zu C_5 duale Code $C_5^\perp$,*
3. *ein zu C_5 dimensionsmäßig benachbarter Code C' mit Minimaldistanz $2 \cdot l$, also ein $[N, 4, 2l]$-Code und*
4. *der dazu duale Code $C'^\perp$, ein $[N, N-4, 2]$-Code.*

[11] dort gab es nur 2 Codes. Warum das so ist, werden wir im Abschnitt „Elementarcodes“ im Kapitel 2 „Vererbung“ sehen.

Wenn wir uns noch einmal den Code C_5 genauer ansehen, stellen wir fest, daß die fünf erzeugenden Vektoren u, v, w, x und y zusammen eine Aneinanderreihung von l Einheitsmatrizen der Dimension 5 darstellen. Dieses Gebilde ist die Generatormatix des Codes C_5. Dieses Konstruktionsprinzip werden wir auch im Folgenden verwenden (jetzt bauen wir ein Gebilde aus 5 Einheitsmatrizen der Dimension l, das ist dann die Generatormatrix des neuen Codes C_l):

Bezeichnung 1.73
Sei $N \in \mathbb{N}$ durch 5 teilbar ($N = 5 \cdot l$ mit $l \geq 3$) und sei
$x_1 = (1,0,0,\ldots,0,1,0,0,\ldots,0,1,0,0,\ldots,0) \in \mathbb{F}_2^N$,
$x_2 = (0,1,0,\ldots,0,0,1,0,\ldots,0,0,1,0,\ldots,0) \in \mathbb{F}_2^N$,
$\ldots\ldots\ldots\ddots\ldots\ldots\ldots$
$\ldots\ldots\ldots\ddots\ldots\ldots\ldots$
$x_l = (0,0,0,\ldots,1,0,0,0,\ldots,1,0,0,0,\ldots,1) \in \mathbb{F}_2^N$.
Dann sei $C_l := \langle x_1, x_2, \cdots, x_l \rangle$ der aus den x_i erzeugte Code.

Wir beweisen nun einen einfachen Satz:

Hilfssatz 1.74
C_l ist zyklisch. Es ist $\dim(C_l) = l = \dfrac{N}{5}$.

Beweis. Da die Vektoren x_1 bis x_l alle linear unabhängig sind, erzeugen sie einen l-dimensionalen Unterraum C_l. Man überzeugt sich leicht, daß jede zyklische Verschiebung eines jeden Vektors aus C_l wieder einen Vektor aus C_l ergibt. Damit erfüllt C_l die Kriterien eines zyklischen Codes. □

Wir beweisen nun einen weiteren einfachen Satz:

Hilfssatz 1.75
Sei C_l der in 1.73 definierte Code. Dann gilt:
C_l hat die Minimaldistanz $d = 5$, d.h., C_l ist ein linearer $[N, \dfrac{N}{5}, 5]$ *- Code* ($l = \dfrac{N}{5}$).

Beweis. Nach der Definition der Minimaldistanz in MacWilliams [16] Ch1, §3 ist leicht zu sehen, daß die x_i in genau 5 Positionen vom Nullvektor verschieden sind. Auch durch Summenbildung einzelner x_i ist eine von Null verschiedene Hammingdistanz nicht unter den Wert von 5 zu bringen. □

Satz 1.76 (**Zentraler Satz für zyklische Codes ungerader Länge** ($N = 5 \cdot l$ **mit** $l \geq 3$)**, Teil 2)**
Sei C_l der in 1.73 definierte Code. Dann gilt:
Die zugehörige Automorphismengruppe des Codes C_l ist isomorph zum folgenden Kranzprodukt:

$$Aut(C_l) \cong \mathfrak{S}_5 \wr \mathfrak{S}_l. \tag{1.102}$$

Beweis. Die Argumentation ist analog zum Beweis vom Satz 1.12. □

Korollar 1.77
Es gibt insgesamt genau 4 *zyklische Codes mit derselben Automorphismengruppe* $Aut(C_l)$*, nämlich:*

1. *den Code* C_l *selbst,*
2. *den zu* C_l *dualen Code* $C_l^{\perp}$*, ein* $[N, N-l, 2]$ *- Code.*
3. *den* $[N, l-1]$ *- Code (dieser Code hat die Minimaldistanz* $10 = 2 \cdot 5$*) und*
4. *den* $[N, N-l+1, 2]$ *- Code. Diese beiden letzten Codes sind nach Lemma 0.28 zueinander dual.*

Der $[N, N-l+1]$ *- Code wird von dem Vektor* $x = (1, 1, 1, \ldots, 1, 0, 0, 0, \ldots, 0)$ *erzeugt, wobei sich die erste* 0 *an der Stelle* $l+1$ *befindet.*
Der $[N, l-1]$ *- Code wird von dem Vektor*
$x = (1, 1, 0, 0, \ldots, 0, 1, 1, 0, \ldots, 0, 1, 1, 0, \ldots, 0)$ *erzeugt, wobei sich die beiden Einsen jeweils an den Stellen* $j \cdot l + 1$ *und* $j \cdot l + 2$ *befinden* ($j = 0, \cdots, 4$*).*

Beweis. Wir werden das im Kapitel „Vererbung“ allgemein beweisen (Sätze 2.3 bis 2.2, angewandt auf den **„zweiten Elementarcode“**, s. Abschnitt 2.1). □

Darüberhinaus finden wir – – sofern zusätzlich eine Spezialgruppe existiert, die auf einer Menge Ω der Kardinalität l transitiv operiert – auch

$$Spezialgruppe_l \wr \mathfrak{S}_5, \tag{1.103}$$

$$\mathfrak{S}_5 \wr Spezialgruppe_l. \tag{1.104}$$

Bemerkung 1.78
Weiterhin wurde bemerkt, daß – sofern l kein Vielfaches von 5 ist – so existiert auch noch[12]

$$\mathfrak{S}_5 \times \mathfrak{S}_l \tag{1.105}$$

und – sofern zusätzlich eine Spezialgruppe existiert, die auf einer Menge Ω der Kardinalität l transitiv operiert – auch

$$\mathfrak{S}_5 \times Spezialgruppe_l. \tag{1.106}$$

Beispiel für eine Spezialgruppe, die auf einer Menge Ω der Kardinalität 7 transitiv operiert, ist $PSL(3, 2)$.

[12] diese Aussage beweisen wir allgemein im Satz 3.3

1.3.4 Zyklische Codes der Länge $N = 7 \cdot l$

Bezeichnung 1.79
Sei $N \in \mathbb{N}$ durch 7 teilbar ($N = 7 \cdot l$ mit $l \geq 3$) und sei
$v_1 = (1,0,0,0,0,0,0,1,0,0,0,0,0,0,1,0,0,0,0,0,0,0,\ldots) \in \mathbb{F}_2^N$,
$v_2 = (0,1,0,0,0,0,0,0,1,0,0,0,0,0,0,0,1,0,0,0,0,0,0,\ldots) \in \mathbb{F}_2^N$,
$v_3 = (0,0,1,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,1,0,0,0,0,\ldots) \in \mathbb{F}_2^N$,
$v_4 = (0,0,0,1,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,1,0,0,0,\ldots) \in \mathbb{F}_2^N$,
$v_5 = (0,0,0,0,1,0,0,0,0,0,0,0,1,0,1,0,0,0,0,0,1,0,0,\ldots) \in \mathbb{F}_2^N$,
$v_6 = (0,0,0,0,0,1,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,1,0,\ldots) \in \mathbb{F}_2^N$,
$v_7 = (0,0,0,0,0,0,1,0,0,0,0,0,0,0,1,0,1,0,0,0,0,0,1,\ldots) \in \mathbb{F}_2^N$.
Dann sei $C_7 := \langle v_1, v_2, \cdots, v_7 \rangle$ der aus den $v_i (i = 1, \cdots, 7)$ erzeugte Code.

Bemerkung 1.80
Da $7 \geq 5$ gilt, konnten wir die Voraussetzung gegenüber früheren Bezeichnungen abschwächen.

Wir beweisen nun einen ersten einfachen Satz:

Hilfssatz 1.81
C_7 ist zyklisch. Es ist $\dim(C_7) = 7$.

Beweis. Da die Vektoren $v_i\,(i = 1, \cdots, 7)$ linear unabhängig sind, erzeugen sie einen 7-dimensionalen Unterraum C_7. Man überzeugt sich leicht, daß jede zyklische Verschiebung eines jeden Vektors aus C_7 wieder einen Vektor aus C_7 ergibt. Damit erfüllt C_7 die Kriterien eines zyklischen Codes. □

Wir beweisen nun einen weiteren einfachen Satz:

Hilfssatz 1.82
Sei C_7 der in 1.79 definierte Code. Dann gilt:
C_7 hat die Minimaldistanz $d = l = \frac{N}{7}$, d.h., C_7 ist ein linearer $[N, 7, \frac{N}{7}]$ - Code.

Beweis. Nach der Definition der Minimaldistanz in MacWilliams [16] Ch1, §3 ist leicht zu sehen, daß alle sieben Basisvektoren $v_i (i = 1, \cdots, 7)$ in genau l Positionen vom Nullvektor verschieden sind. Die Summen je zweier dieser Basisvektoren sind in genau l Positionen vom Einsvektor verschieden. Eine kleinere, von Null verschiedene Hammingdistanz wird von Codevektoren aus C_7 nicht angenommen. □

Nun wollen wir drei wichtige Sätze über die Automorphismengruppe $Aut(C_5)$ formulieren und beweisen:

Lemma 1.83
Sei C der in 1.79 definierte Code. Dann gilt:

$$\mathfrak{S}_7 \leq Aut(C_7). \tag{1.107}$$

Beweis. Sei
$c = (a_1, b_1, c_1, d_1, e_1, f_1, g_1, a_2, b_2, c_2, d_2, e_2, f_2, g_2, \ldots, a_l, b_l, c_l, d_l, e_l, f_l, g_l)$
ein Codevektor. Dann ist
$c' = (g_1, f_1, e_1, d_1, c_1, b_1, a_1, g_2, f_2, e_2, d_2, c_2, b_2, a_2, \ldots, g_l, f_l, e_l, d_l, c_l, b_l, a_l)$
ebenfalls ein Codevektor. Dies definiert eine Operation der symmetrischen Gruppe $\mathfrak{S}_7$ auf $\mathbb{F}_2^N$, die den Code C_7 invariant läßt. □

Lemma 1.84
Sei C_7 der in 1.79 definierte Code. Dann gilt:

$$\mathfrak{S}_l \leq Aut(C_7). \tag{1.108}$$

Beweis. Sei
$c = ((a_1, b_1, c_1, d_1, e_1, f_1, g_1), (a_2, b_2, c_2, d_2, e_2, f_2, g_2), \ldots, (a_l, b_l, c_l, d_l, e_l, f_l, g_l))$
ein Codevektor. Dann ist
$c' = ((a_2, b_2, c_2, d_2, e_2, f_2, g_2), (a_1, b_1, c_1, d_1, e_1, f_1, g_1), \ldots, (a_l, b_l, c_l, d_l, e_l, f_l, g_l))$
ebenfalls ein Codevektor. Dies definiert eine Operation der symmetrischen Gruppe $\mathfrak{S}_l$ auf $\mathbb{F}_2^N$, die den Code C_7 invariant läßt. □

Lemma 1.85
Sei C_7 der in 1.79 definierte Code. Dann gilt:

$$\underbrace{\mathfrak{S}_l \times \mathfrak{S}_l \times \ldots \times \mathfrak{S}_l}_{7-mal} \leq Aut(C_7). \tag{1.109}$$

Beweis. Sei
$c = (a_1, b_1, c_1, d_1, e_1, f_1, g_1, a_2, b_2, c_2, d_2, e_2, f_2, g_2, \ldots, a_l, b_l, c_l, d_l, e_l, f_l, g_l)$ ein Codevektor. Dann können zum einen die a_i permutiert werden und zum anderen die b_i, sowie auch die c_i, usw. bis hin zu den g_i. Dies definiert eine Operation der Gruppe $\underbrace{\mathfrak{S}_l \times \mathfrak{S}_l \times \ldots \times \mathfrak{S}_l}_{7-mal}$ auf $\mathbb{F}_2^N$, die den Code C_7 invariant läßt.

□

Satz 1.86 (Zentraler Satz für zyklische Codes der Länge $N = 7 \cdot l$ mit $l \geq 3$), Teil 1)
Sei C_7 der in 1.79 definierte Code. Dann gilt:

$$\mathfrak{S}_l \wr \mathfrak{S}_7 \cong Aut(C_7). \tag{1.110}$$

Beweis. Die Gruppe von linearen Abbildungen, die von $\mathfrak{S}_7$ und $\underbrace{\mathfrak{S}_l \times \ldots \times \mathfrak{S}_l}_{7-mal}$ (nach Satz 1.83 und Satz 1.85) erzeugt wird, ist isomorph zum Kranzprodukt $\mathfrak{S}_l \wr \mathfrak{S}_7$. Die Argumentation ist analog zum Beweis vom Satz 1.12. □

Bemerkung 1.87
Anders, als bei den Codes gerader Länge mit $N = 2 \cdot l$ stellen wir hier ($N = 7 \cdot l$) fest, daß es insgesamt 4 Codes mit der Automorphismengruppe $Aut(C_7)$ gibt, nämlich:

1. der Code C_7 selbst,
2. der zu C_7 duale Code $C^{\perp}$,
3. ein zu C_7 dimensionsmäßig benachbarter Code C' mit Minimaldistanz $2 \cdot l$, also ein $[N, 6, 2l]$ - Code und
4. der dazu duale Code $C'^{\perp}$, ein $[N, N-6, 2]$ - Code.

Wenn wir uns noch einmal den Code C_7 genauer ansehen, stellen wir fest, daß die sieben erzeugenden Vektoren v_i zusammen eine Aneinanderreihung von l Einheitsmatrizen der Dimension 7 darstellen. Dieses Gebilde ist die Generatormatix des Codes C_7. Dieses Konstruktionsprinzip werden wir auch im Folgenden verwenden (jetzt bauen wir ein Gebilde aus 7 Einheitsmatrizen der Dimension l, das ist dann die Generatormatrix des neuen Codes C_l):

Bezeichnung 1.88
Sei $N \in \mathbb{N}$ durch 7 teilbar ($N = 7 \cdot l$ mit $l \geq 3$) und sei
$x_1 = (1,0,0,\ldots,0,1,0,0,\ldots,0,1,0,0,\ldots,0) \in \mathbb{F}_2^N$,
$x_2 = (0,1,0,\ldots,0,0,1,0,\ldots,0,0,1,0,\ldots,0) \in \mathbb{F}_2^N$,
$\ldots\ldots\ldots\ddots\ldots\ldots\ldots$
$\ldots\ldots\ldots\ddots\ldots\ldots$
$x_l = (0,0,0,\ldots,1,0,0,0,\ldots,1,0,0,0,\ldots,1) \in \mathbb{F}_2^N$.
Dann sei $C_l := \langle x_1, x_2, \cdots, x_l \rangle$ der aus den x_i erzeugte Code.

Wir beweisen nun einen einfachen Satz:

Satz 1.89
C_l ist zyklisch. Es ist $\dim(C) = l = \dfrac{N}{7}$.

Beweis. Da die Vektoren x_1 bis x_l alle linear unabhängig sind, erzeugen sie einen l-dimensionalen Unterraum C_l. Man überzeugt sich leicht, daß jede zyklische Verschiebung eines jeden Vektors aus C_l wieder einen Vektor aus C_l ergibt. Damit erfüllt C_l die Kriterien eines zyklischen Codes. □

Wir beweisen nun einen weiteren einfachen Satz:

Satz 1.90
Sei C_l der in 1.88 definierte Code. Dann gilt:
C_l hat die Minimaldistanz $d = 7$, d.h., C_l ist ein linearer $[N, \frac{N}{7}, 7]$-Code ($l = \frac{N}{7}$).

Beweis. Nach der Definition der Minimaldistanz in MacWilliams [16] Ch1, §3 ist leicht zu sehen, daß die x_i in genau 7 Positionen vom Nullvektor verschieden sind. Auch durch Summenbildung einzelner x_i ist eine von Null verschiedene Hammingdistanz nicht unter den Wert von 7 zu bringen. □

Satz 1.91 (**Zentraler Satz für zyklische Codes der Länge** $N = 7 \cdot l$ **mit** $l \geq 3$)**, Teil 2)**
Sei C_l *der in 1.88 definierte Code. Dann gilt:*
Die zugehörige Automorphismengruppe des Codes C_l *ist isomorph zum folgenden Kranzprodukt:*

$$Aut(C_l) \cong \mathfrak{S}_7 \wr \mathfrak{S}_l. \tag{1.111}$$

Beweis. Die Argumentation ist analog zum Beweis vom Satz 1.12. □

Korollar 1.92
Es gibt insgesamt genau 4 *zyklische Codes mit derselben Automorphismengruppe* $Aut(C_l)$*, nämlich:*

1. *den Code* C_l *selbst,*
2. *den zu* C_l *dualen Code* $C_l^{\perp}$*, ein* $[N, N-l, 2]$ *- Code.*
3. *den* $[N, l-1]$ *- Code (dieser Code hat die Minimaldistanz* $14 = 2 \cdot 7$*) und*
4. *den* $[N, N-l+1]$ *- Code. Diese beiden letzten Codes sind nach Lemma 0.28 zueinander dual.*

Der $[N, N-l+1]$ *- Code wird von dem Vektor* $x = (1, 1, 1, \ldots, 1, 0, 0, 0, \ldots, 0)$ *erzeugt, wobei sich die erste* 0 *an der Stelle* $l+1$ *befindet.*
Der $[N, l-1]$ *- Code wird von dem Vektor* $x = (1, 1, 0, 0, \ldots, 0, 1, 1, 0, \ldots, 0, 1, 1, 0, \ldots, 0)$ *erzeugt, wobei sich die beiden Einsen jeweils an den Stellen* $j \cdot l + 1$ *und* $j \cdot l + 2$ *befinden* $(j = 0, \cdots, 6)$*.*

Beweis. Wir werden das im Kapitel „Vererbung“ allgemein beweisen (Sätze 2.3 bis 2.2, angewandt auf den **„zweiten Elementarcode“**, s. Abschnitt 2.1). □

Bemerkung 1.93
Weiterhin wurde bemerkt, daß – sofern l kein Vielfaches von 7 ist, so existiert auch noch[13]

$$\mathfrak{S}_7 \times \mathfrak{S}_l \tag{1.112}$$

Wie bereits weiter oben im Abschnitt 1.1 bemerkt, gibt es für $N = 7$ noch eine weitere für uns relevante Permutationsgruppe, die auf der Menge $\Omega = \{1, 2, \ldots, 7\}$ operiert, nämlich die Spezialgruppe $PSL(3, 2)$. In den Magma-Auflistungen der Kompositionsfaktoren unserer Automorphismengruppen wird an der entsprechenden Stelle immer die dazu isomorphe Gruppe $PSL(2, 7)$ notiert (auf die für die Kranzproduktbildung wichtigen Unterschiede beim *Permutationsgrad*[14] dieser beiden isomorphen Gruppen wird im Abschnitt 3.5 hingewiesen).

[13] diese Aussage beweisen wir allgemein im Satz 3.3
[14] der Begriff *Permutationsgrad* wird im Anschluß an die Definition 0.33 der *Kardinalität* erklärt.

Wir finden deshalb zusätzlich zu den obengenannten Kranzprodukten noch

$$PSL(3,2) \wr \mathfrak{S}_l, \tag{1.113}$$

$$\mathfrak{S}_l \wr PSL(3,2). \tag{1.114}$$

Diese Automorphismengruppen werden jeweils von 8 Codes angenommen.
Im Spezialfall $l = 7$ existiert sinngemäß auch noch das folgende Kranzprodukt:

$$PSL(3,2) \wr PSL(3,2). \tag{1.115}$$

Weiterhin wurde bemerkt, daß, sofern l kein Vielfaches von 7 ist, so existiert auch noch

$$PSL(3,2) \times \mathfrak{S}_l. \tag{1.116}$$

Diese Automorphismengruppe wird – abhängig von l – im Untersuchungsbereich von 20, 24 oder 32 Codes angenommen (s. Tabellen im Anhang).

Eine weitere interessante Permutationsgruppe, die auf einer Menge Ω der Kardinalität 7 transitiv operiert, ist die dritte transitive Permutationsgruppe aus der **Magma**-Datenbank, oder kurz t7n3 genannt. Es handelt sich hierbei um eine sogenannte pq-Gruppe (q teilt $p-1$, p prim), oder metazyklische Gruppe[15], die als semidirektes Produkt dargestellt werden kann:

$$\mathfrak{Z}_7 \rtimes \mathfrak{Z}_3 \tag{1.117}$$

Wir geben ihr den Namen $\mathfrak{MZ}(7,3)$. Sie selbst ist auflösbar und ist eine triviale (im Sinne dieser Arbeit) Automorphismengruppe von zyklischen Codes der Länge $N = 7$.
Sie tritt in unseren Untersuchungen nur als Komponente in einem direkten Produkt mit einer nicht-auflösbaren Gruppe auf; dadurch wird das gesamte direkte Gruppenprodukt nicht-aufösbar und vom **Magma**-Auswertungsprogramm als nichttrivial erkannt:

$$\mathfrak{MZ}(7,3) \times \mathfrak{S}_l \tag{1.118}$$

für $l \geq 5$, **ungerade** und $l \neq 7$ (s. Tabellenwerk für $N = 35, 63, 77$. $N = 91$ wurde ebenfalls positiv überprüft.)
Bei $N = 70$ finden wir unter anderem:

$$\mathfrak{MZ}(7,3) \times (\mathfrak{S}_2 \wr \mathfrak{S}_5), \tag{1.119}$$

$$\mathfrak{MZ}(7,3) \times (\mathfrak{S}_5 \wr \mathfrak{S}_2), \tag{1.120}$$

$$(\mathfrak{MZ}(7,3) \wr \mathfrak{S}_2) \times \mathfrak{S}_5), \tag{1.121}$$

$$(\mathfrak{S}_2 \wr (\mathfrak{S}_5 \times \mathfrak{MZ}(7,3)))/\mathfrak{S}_2^{15}. \tag{1.122}$$

[15] eine weitere metazyklische Gruppe, die auf einer Menge Ω der Kardinalität 17 transitiv operiert, wurde noch bei der Untersuchung der Codelängen 85, und 119 gefunden: die $\mathfrak{MZ}(17,8) \cong \mathfrak{Z}_{17} \rtimes \mathfrak{Z}_8$. Zwei weitere metazyklische Gruppen, die auf einer Menge Ω der Kardinalität 89, bzw. 127 transitiv operieren, wurden noch bei der Untersuchung der Codelängen 89 und 127 (triviale Codes) gefunden:
die Gruppen $\mathfrak{MZ}(89,11) \cong \mathfrak{Z}_{89} \rtimes \mathfrak{Z}_{11}$, sowie $\mathfrak{MZ}(127,7) \cong \mathfrak{Z}_{127} \rtimes \mathfrak{Z}_7$.

Interessant ist in diesem Zusammenhang die Feststellung, daß für $l \geq 5$ die Gruppe $\mathfrak{S}_l \wr \mathfrak{MZ}(7,3)$ – ebenso, wie die Gruppe $\mathfrak{MZ}(7,3) \wr \mathfrak{S}_l$ nicht als Automorphismengruppe für $N = 7 \cdot l$ auftritt, obwohl sie nicht-auflösbar ist (das gleiche gilt für $\mathfrak{MZ}(7,3) \times \mathfrak{S}_l$ mit **geradem** $l \geq 6$)!

Kapitel 2

Vererbung von zyklischen Codes und ihren Automorphismengruppen

In diesem Kapitel wollen wir uns mit der „Vererbung“ oder Fortpflanzung von zyklischen Codes und ihren Automorphismengruppen befassen.

Bei der Untersuchung im Rahmen dieser Arbeit fiel nämlich auf, daß einige Automorphismengruppen immer wieder als Faktoren bei doppelten, dreifachen, usw. Codelängen auftreten. Daraufhin habe ich mir die zugehörigen Codes angesehen und Zusammenhänge erkannt, die ich hier zusammenfassen möchte.

Zunächst benötigen wir einen neuen Begriff, da der Begriff „Wiederholungscode“ (englisch: „Repetition Code“) bereits in der Literatur mit einer anderen Bedeutung belegt ist.
Voraussetzung für alle Aussagen in diesem Kapitel ist $n \geq 5$, da die Automorphismengruppen nicht auflösbar sein sollen („nichttriviale“ Codes im Sinne dieser Arbeit). Geht man von dieser Forderung ab, so kann die Voraussetzung entfallen.

Definition 2.1 (**Mehrfachcode**)
Sei G die Generatormatrix eines zyklischen $[n, k, d]$-Codes C mit der zugehörigen Automorphismengruppe Aut(C). Wir erzeugen nun daraus einen neuen Code C^m, indem wir die Generatormatrix G mehrfach (m-mal) nebeneinander anordnen:

$$G_N = \underbrace{(G|\cdots|G)}_{m-mal}. \tag{2.1}$$

Wir nennen C den Basiscode *und C^m den (m-fachen)* Mehrfachcode.

Wir formulieren jetzt dazu einen wichtigen Satz, nämlich den Zentralen Satz für zyklische Codes, Teil 2 (allgemeine Fassung). Der Teil 1 wird weiter unten diskutiert

Satz 2.2 (**Zentraler Satz für zyklische Codes, Teil 2 (allgemeine Fassung)**)
Die zu C^m gehörige Automorphismengruppe $Aut(C^m)$ ist isomorph zum Kranzprodukt

$$\mathfrak{S}_m \wr Aut(C). \tag{2.2}$$

Um dies zu beweisen, müssen wir vorher noch einige Sätze formulieren und beweisen:

Hilfssatz 2.3
C^m ist zyklisch.

Beweis. Da C zyklisch ist, überzeugt man sich leicht, daß jede zyklische Verschiebung eines jeden Vektors $c \in C^m$ wieder einen Vektor $c' \in C^m$ ergibt. Damit erfüllt C^m die Kriterien eines zyklischen Codes. □

Hilfssatz 2.4
C^m ist ein $[N, k, D]$-Code mit $N = m \cdot n$ und $D = m \cdot d$.

Beweis. Wir beweisen die drei Teilaussagen der Reihe nach:

1. Da die Codelänge gleich der Spaltenanzahl der Generatormatrix ist, gilt $N = m \cdot n$.
2. Da die Zeilenzahl der Generatormatrix von C^m identisch ist mit der Zeilenzahl k der Generatormatrix von C, ist auch die Dimension des Codes C^m identisch mit der Dimension k des Codes C.
3. Sei c ein Codevektor von C mit d Einsen. Dann gibt es aufgrund der Konstruktion einen entsprechenden Codevektor $c' \in C^m$ mit $D = m \cdot d$ Einsen. Einen Codevektor $c'' \in C^m$ mit weniger Einsen kann es aufgrund der Konstruktion nicht geben.

Also ist C^m ein $[N, k, D]$-Code mit $N = m \cdot n$ und $D = m \cdot d$. □

Lemma 2.5
Es gilt: $Aut(C) \leq Aut(C^m)$.

Beweis. Sei
$c = ((a_{11}, a_{12}, \ldots, a_{1n}), (a_{21}, a_{22}, \ldots, a_{2n}), \ldots\ldots, (a_{m1}, a_{m2}, \ldots, a_{mn})) \in C^m$
ein Codevektor. Dann ist für $\sigma \in Aut(C)$ auch
$c' = (\sigma(a_{11}, a_{12}, \ldots, a_{1n}), \sigma(a_{21}, a_{22}, \ldots, a_{2n}), \ldots\ldots, \sigma(a_{m1}, a_{m2}, \ldots, a_{mn})) =: \widehat{\sigma}(c)$
ein Codevektor aus C^m.
Dies definiert eine treue Operation der Gruppe $Aut(C)$ auf $\mathbb{F}_2^N$, die den Code C^m invariant läßt. Wir erhalten einen Monomorphismus

$$Aut(C) \hookrightarrow Aut(C^m),\ \sigma \mapsto \widehat{\sigma}. \tag{2.3}$$

□

Lemma 2.6
Es gilt: $\mathfrak{S}_m \leq Aut(C^m)$.

Beweis. Sei
$c = ((a_{11}, a_{12}, \ldots, a_{1n}), (a_{21}, a_{22}, \ldots, a_{2n}), \ldots\ldots, (a_{m1}, a_{m2}, \ldots, a_{mn})) \in C^m$
ein Codevektor. Dann ist für $\sigma \in Aut(C)$ auch
$c' = ((a_{\sigma(1)1}, \ldots, a_{\sigma(1)n}), (a_{\sigma(2)1}, \ldots, a_{\sigma(2)n}), \ldots\ldots, (a_{\sigma(m)1}, \ldots, a_{\sigma(m)n})) =: \widehat{\sigma}(c)$
ein Codevektor aus C^m.
Dies definiert eine Operation der symmetrischen Gruppe $\mathfrak{S}_m$ auf $\mathbb{F}_2^N$, die den Code C^m invariant läßt. Wir erhalten einen Homomorphismus

$$\mathfrak{S}_m \hookrightarrow Aut(C^m),\ \sigma \mapsto \widehat{\sigma}. \tag{2.4}$$

□

Lemma 2.7
Es gilt:

$$\underbrace{\mathfrak{S}_m \times \mathfrak{S}_m \times \ldots \times \mathfrak{S}_m}_{n-mal} \leq Aut(C^m). \tag{2.5}$$

Beweis. Sei
$c = ((a_{11}, a_{12}, \ldots, a_{1n}), (a_{21}, a_{22}, \ldots, a_{2n}), \ldots\ldots, (a_{m1}, a_{m2}, \ldots, a_{mn})) \in C^m$
ein Codevektor.
Dann können zum einen die a_{i1} permutiert werden und zum anderen die a_{i2} sowie auch die a_{i3}, usw. bis hin zu den a_{in}.
Dies definiert eine Operation der Gruppe $\underbrace{\mathfrak{S}_m \times \mathfrak{S}_m \times \ldots \times \mathfrak{S}_m}_{n-mal}$ auf $\mathbb{F}_2^N$, die den Code C^m invariant läßt. □

Nun können wir den Satz 2.2 beweisen:

Beweis. Die Gruppe von linearen Abbildungen, die von $Aut(C)$ und $\underbrace{\mathfrak{S}_m \times \ldots \times \mathfrak{S}_m}_{n-mal}$ (nach Satz 2.5 und Satz 2.7) erzeugt wird, ist isomorph zum Kranzprodukt $\mathfrak{S}_m \wr Aut(C)$. Damit ist zunächst gezeigt, daß $Aut(C^m)$ eine Untergruppe U besitzt, die isomorph zu $\mathfrak{S}_m \wr Aut(C)$ ist, d.h. es gilt also:

$$\mathfrak{S}_m \wr Aut(C) \cong U \leq Aut(C^m). \tag{2.6}$$

Es bleibt zu zeigen, daß $Aut(C^m) = U$ gilt. Wir treffen eine Fallunterscheidung:

1. $Aut(C) = \mathfrak{S}_n$.
   Es ist $N = m \cdot n$. Da $\mathfrak{S}_m \wr \mathfrak{S}_n$ stets maximale Untergruppe unter $\mathfrak{S}_N$ ist[1], kann es keine nichttriviale Obergruppe geben. Im Kapitel 9 zeigen wir, daß die symmetrische Gruppe $\mathfrak{S}_N$ stets nur von den 4 primitiven[2] Codes angenommen wird.
   Somit ist $Aut(C^m) = \mathfrak{S}_m \wr \mathfrak{S}_n$ und wir sind fertig.

[1] die Maximalität von $\mathfrak{S}_a \wr \mathfrak{S}_b$ unter $\mathfrak{S}_N$ wird in Martin W. Liebeck, Cheryl E. Praeger, and Jan Saxl [7],S. 366 gezeigt.

[2] dieser Begriff wird einige Seiten weiter unten im Einschub 2.1 *Elementarcodes* definiert.

2. $Aut(C) \leq \mathfrak{S}_n$ (allgemeiner Fall).
   Sei $\varphi \in Aut(C^m)$ beliebig. Wegen $Aut(C^m) \leq \mathfrak{S}_N$ gilt $\varphi \in \mathfrak{S}_N$.
   Wir zeigen, daß $\varphi \in U$ gilt. Sei

$$\Lambda_1 := \{1, n+1, 2n+1, \ldots, N-n+1\},$$
$$\Lambda_2 := \{2, n+2, 2n+2, \ldots, N-n+2\},$$
$$\vdots$$
$$\Lambda_n := \{n, 2n, 3n, \ldots, N\}.$$

   Da φ den linearen Code C^m in sich überführen muß, folgt

   - $\alpha)$ $\varphi(\Lambda_1) = \Lambda_1 \quad \wedge \quad \varphi(\Lambda_2) = \Lambda_2 \quad \wedge \ldots\ldots \wedge \quad \varphi(\Lambda_n) = \Lambda_n,$ oder
   - $\beta)$ $\varphi(\Lambda_1) = \Lambda_{\sigma(1)} \quad \wedge \quad \varphi(\Lambda_2) = \Lambda_{\sigma(2)} \quad \wedge \ldots\ldots \wedge \quad \varphi(\Lambda_n) = \Lambda_{\sigma(n)}.$

   Wir führen jetzt eine Fallunterscheidung durch:

   - α : In diesem Fall ist φ das Produkt von n Permutationen aus $\mathfrak{S}_m$ und damit gilt nach Lemma 2.7 $\varphi \in U$.
   - β : In diesem Fall ist $\sigma * \varphi$ ein Element aus $Aut(C^m)$, das die Bedingung $\alpha)$ erfüllt. Das Element σ ist in Lemma 2.5 definiert. Nach dem ersten Fall folgt $\sigma * \varphi \in U$

□

Das folgende Beispiel zeigt einen zyklischen $[7, 4, 3]$-Code[3] C als Basiscode, zu dem die $PSL(3, 2)$ als Automorphismengruppe gehört. Durch Anwendung des oben erklärten Konstruktionsprinzips mit $m = 3$ erhalten wir einen zyklischen $[21, 4, 9]$-Code C^3. Seine Automorphismengruppe ist

$$\mathfrak{S}_3 \wr PSL(3, 2). \tag{2.7}$$

Beispiel 2.8 (Mehrfachcode C^3 mit $n = 7, N = 21$)

```
Lfd.Nr.  k   d     #PermGrp          #AutoGrp

   3     4   3          7                168

[7, 4, 3] Cyclic Linear Code over GF(2)
Generator matrix:
[1 0 0 0 1 0 1]
[0 1 0 0 1 1 1]
[0 0 1 0 1 1 0]
[0 0 0 1 0 1 1]
```

[3] dieser Code ist isomorph zum Hamming-Code $\mathcal{CH}_3$

```
Lfd.Nr.  k   d     #PermGrp          #AutoGrp

  10     4   9         21           47029248

[21, 4, 9] Cyclic Linear Code over GF(2)
Generator matrix:
[1 0 0 0 1 0 1 1 0 0 0 1 0 1 1 0 0 0 1 0 1]
[0 1 0 0 1 1 1 0 1 0 0 1 1 1 0 1 0 0 1 1 1]
[0 0 1 0 1 1 0 0 0 1 0 1 1 0 0 0 1 0 1 1 0]
[0 0 0 1 0 1 1 0 0 0 1 0 1 1 0 0 0 1 0 1 1]
```

Ende des Beispiels

Bemerkung 2.9
Dieser oben konstruierte $[21, 4, 9]$ - Code ist ein dreifacher Hamming-Code und kann bei der Übertragung von 4 Bits bis zu 4 Fehlern korrigieren. Mehr ist technisch nicht sinnvoll. Mathematisch ist das durchaus möglich: so finden wir z.B. den entsprechenden $[35, 4, 15]$ - Code im Listenwerk für $N = 35$.
Ende der Bemerkung

Wir hatten das Konstruktionsprinzip der *Mehrfachcodes* bereits im Abschnitt 1.2 „Zyklische Codes gerader Länge“ als Spezialfall mit $m = l$, bzw $m = 2$ benutzt, um dort die ersten Aussagen zu beweisen. Die Generatormatrizen waren die Einheitsmatrizen E_2 bzw. E_l. Die dazu entsprechenden Codes gehören nach der Aufgabenstellung dieser Arbeit zu den trivialen Codes und sind daher bislang nicht näher betrachtet worden.
Wegen der grundlegenden Bedeutung wollen wir die wesentlichen Eigenschaften dieser trivialen Codes in einem eigenen Abschnitt diskutieren und danach weitere Sätze und Folgerungen ableiten.

2.1 Elementarcodes (Einschub)

Für alle Codelängen n ($n \geq 3$) existieren stets 4 „primitive“ (Definition siehe anschließend) Codes mit $\mathfrak{S}_n$ als Automorphismengruppe[4]. Sie sind im Sinne dieser Arbeit deshalb trivial und wurden daher bislang nicht berücksichtigt. Insbesondere wurden sie in der statistischen Auswertung bei der Berechnung der „Dichte“ der Codes (siehe Kapitel 7) herausgerechnet. Da jedoch zwei dieser 4 primitiven Codes eine elementare Bedeutung für diese Arbeit haben, wollen wir diese Codes an dieser Stelle definieren:

Definition 2.10 (**Primitive Codes**)
Hier nun die 4 primitiven Codes im Einzelnen[5]*:*

1. *der Code $\mathcal{C}_{0/n}$. Es ist ein $[n, 0, n]$ - Code.*
   Er besteht nur aus dem Nullvektor („Nullcode“).
   Bezeichnung in **Magma:** `ZeroCode(GF(2),n)`

2. *der Code $\mathcal{C}_{1/n}$. Es ist ein $[n, n, 1]$ - Code.*
   Er besteht aus dem gesamten n-dimensionalen Vektorraum $\mathbb{F}_2^n$.
   Seine Generatormatrix ist daher die n-dimensionale Einheitsmatrix E_n.
   Sein Generatorpolynom ist $g_{\mathcal{C}_{1/n}}(x) \equiv 1$.
   Er ist der **erste Elementarcode**. *Er ist zum Nullcode dual.*
   Bezeichnung in **Magma:** `UniverseCode(GF(2),n)`

3. *der Code $\mathcal{C}_{2/n}$. Es ist ein $[n, n-1, 2]$ - Code.*
   Er besteht aus einem $(n-1)$-dimensionalen Untervektorraum.
   Sein Generatorpolynom ist $g_{\mathcal{C}_{2/n}}(x) = x + 1$.
   Er ist der **zweite Elementarcode**.
   Bezeichnung in **Magma:** `ZeroSumCode(GF(2),n)`, *oder* `EvenWeightCode(n)`

4. *der Code $\mathcal{C}_{n/n}$. Es ist ein $[n, 1, n]$ - Code.*
   Er besteht aus dem Nullvektor und dem Einsvektor $(1, 1, \cdots, 1)$.
   Er ist zum zweiten Elementarcode dual.
   Bezeichnung in **Magma:** `RepetitionCode(GF(2),n)`

Bemerkung 2.11
Die Voraussetzung $n \geq 3$ ist daher gemacht worden, weil für $n = 2$ die beiden primitiven Codes $\mathcal{C}_{2/n}$ und $\mathcal{C}_{n/n}$ zusammenfallen (selbstdual). Es gibt für $n = 2$ also nur 3 (statt 4) primitive Codes. Somit steht uns in diesem Fall der zweite Elementarcode für eine sinnvolle Vererbung zu einem „Mehrfachcode“ (s.u.) nicht zur Verfügung.

Daher existieren für gerade Codelängen mit $N = 2 \cdot l$ nur 2 Codes (inkl. dualem Code) mit der Automorphismengruppe $\mathfrak{S}_l \wr \mathfrak{S}_2$ als l-fache Vererbung des Elementarcodes $\mathcal{C}_{1/2}$,

[4] wir werden später sehen, daß zu $\mathfrak{S}_n$ keine weiteren zyklischen Codes gehören (s. 9.5).

[5] In der **Magma**-Dokumentation sind diese Codes unter der Rubrik „Some Trivial Linear Codes“ beschrieben – ihre jeweiligen **Magma**-Bezeichnungen wurden daher hier mit angegeben.

während die l-fache Vererbung des Elementarcodes $\mathcal{C}_{2/2}$ mit dem primitiven Code $\mathcal{C}_{N/N}$ der Länge N zusammenfällt.

Im Gegensatz dazu haben wir für $N = a \cdot l$ mit $a \geq 3$ stets 4 Codes (inkl. der dualen Codes) mit der Automorphismengruppe $\mathfrak{S}_l \wr \mathfrak{S}_a$ als l-fache Vererbung der beiden Elementarcodes $\mathcal{C}_{1/a}$ und $\mathcal{C}_{2/a}$.

Ende des Einschubs über Elementarcodes

Eine wichtige Folgerung wollen wir nun formulieren:

Folgerung 2.12
Sei N eine Codelänge mit der Faktorzerlegung $N = d \cdot k$.
Weiter sei $\mathcal{C}_{1/k}$ der oben definierte „erste Elementarcode“ der Länge k unser Basiscode.

1. *Dann existiert stets der zyklische Mehrfachcode $\mathcal{C}^d_{1/k}$ als $[N, k, d]$-Code mit der Automorphismengruppe $\mathfrak{S}_d \wr \mathfrak{S}_k$.*
2. *Der Erzeugungsvektor von $\mathcal{C}^d_{1/k}$ ist*
   $v = (1, 0, \ldots, 0; 1, 0, \ldots, 0; \ldots; 1, 0, \ldots, 0) \in \mathbb{F}_2^N$, also die d-malige Aneinanderreihung des Erzeugungsvektors von $\mathcal{C}_{1/k}$.
3. *Das zugehörige Erzeugerpolynom von $\mathcal{C}^d_{1/k}$ ist*
   $g(x) = 1 + x^k + x^{2k} + \ldots + x^{(d-1)k}$, $g(x) \in \mathbb{F}_2[x]/(x^N - 1)$,
   oder einfacher geschrieben:
   $$g(x) = \sum_{i=0}^{d-1} x^{ik}.$$

Beweis. Nach MacWilliams [16] Ch7, 3, Theorem 1 kann man die Elemente des Erzeugungsvektors v als die Koeffizienten des Erzeugerpolynoms g auffassen. Die Koeffizienten finden sich auch in der Generatormatrix[6], die nach obiger Konstruktion durch d-maliges Aneinanderreihen der Einheitsmatrix E_k entstanden ist. □

Damit können wir jetzt auch den in der Einleitung zitierten Satz 0.5 beweisen:

Satz 2.13 (Erster Hauptsatz für zyklische Codes)
Zu jedem technischen Übertragungsproblem, nämlich k Bits so zu übertragen, daß e Fehler korrigiert werden können, existiert ein zyklischer $[N, k, d]$-Code C_k, mit

$$d = 2e + 1 \quad \textit{und} \quad N = k \cdot d.$$

Die Automorphismengruppe von C_k ist

$$\mathfrak{S}_d \wr \mathfrak{S}_k,$$

[6] Wenn die Generatormatrix von „reduzierter Form“ – d.h. G=$(E_k|P)$ ist, wie bei Lütkebohmert[10], Lemma 1.14 beschrieben und in **Magma** implementiert, dann stehen die Koeffizienten stets in der letzten Zeile, und zwar beginnend mit der 1 (=x^0) von E_k, gefolgt von den Koeffizienten der nach rechts aufsteigenden x-Potenzen

das Erzeugerpolynom von C_k ist

$$g(x) = \sum_{i=0}^{d-1} x^{ik}$$

und das Kontrollpolynom von C_k ist

$$h(x) = 1 + x^k.$$

Beweis. Nach den bisher bewiesenen Aussagen bleiben nur noch 2 der obigen Aussagen zu zeigen, und zwar:

1. $d = 2e + 1$. Dies folgt unmittelbar aus MacWilliams [16] Ch1, §3, Satz 2.
2. $h(x) = 1 + x^k$. Dies folgt unmittelbar aus MacWilliams [16] Ch7, §4:
   Es gilt: $h(x) = (x^N - 1)/g(x)$.

□

Dieser erste Hauptsatz ist klar und einprägsam.
Insbesondere wird der Zusammenhang zwischen dem Code, dargestellt durch das Erzeugerpolynom, seinen Attributen (N, k, d) und der zugehörigen Automorphismengruppe anhand der Faktorenzerlegung von N durch die technische Problemstellung deutlich.
Allerdings wird meist die Effizienz (oder Rate) $R(C) = k/N$ eines solchen zyklischen Codes nicht sehr hoch sein.
Zur Verbesserung der Effizienz wollen wir daher dasselbe Konstruktionsprinzip mit dem „zweiten Elementarcode“ umsetzen und jetzt auch den in der Einleitung zitierten zweiten Satz 0.6 beweisen:

Satz 2.14 (**Zweiter Hauptsatz für zyklische Codes)**
Zu jedem technischen Übertragungsproblem, nämlich $k - 1$ Bits so zu übertragen, daß e Fehler korrigiert und bis zu $2e + 1$ Fehler erkannt werden können, existiert ein zyklischer $[N, k - 1, 2d]$-Code C, mit $\dim(C) = k - 1$ und $md(C) = 2d$, sowie

$$d = e + 1 \text{ und } N = k \cdot d.$$

Die Automorphismengruppe von C ist

$$\mathfrak{S}_d \wr \mathfrak{S}_k,$$

das Erzeugerpolynom von C ist

$$g(x) = \sum_{i=0}^{e} x^{ik} + x^{ik+1}$$

und das Kontrollpolynom von C ist

$$h(x) = \sum_{i=0}^{k-1} x^i.$$

Dieser zweite Hauptsatz ist nicht mehr ganz so klar und einprägsam, aber dafür wächst N wegen $N = k \cdot md(C)/2$ nicht mehr so schnell, d.h. die Effizienz ist besser.
Darüberhinaus gewinnen wir wegen der zusätzlichen Aussage der Fehlererkennung noch an Qualität.
Ein **Beispiel** soll das verdeutlichen: Angenommen, wir wollen 8 Bits so übertragen, daß 3 Fehler korrigiert werden können, so bekommen wir

1. nach dem ersten Hauptsatz einen $[56, 8, 7]$-Code C_1 mit $Aut(C_1) = \mathfrak{S}_7 \wr \mathfrak{S}_8$, bzw.
2. nach dem zweiten Hauptsatz einen $[36, 8, 8]$-Code C_2 mit $Aut(C_2) = \mathfrak{S}_4 \wr \mathfrak{S}_9$.

Beweis. Nach den bisher bewiesenen Aussagen bleiben nur noch 3 der obigen Aussagen zu zeigen, und zwar:

1. Fehlererkennung bis zu $2e + 1$ Fehlern: Dies folgt unmittelbar aus Grunewald [3] Kapitel 1.2, Satz 1 (siehe hierzu auch Peterson [12]).
2. Die Konstruktion mit $k - 1$ zu übertragender Bits und $md(C) = 2d = 2 \cdot (e + 1)$ folgt aus der Anwendung des Satzes 2.2 auf den „zweiten Elementarcode“ $\mathcal{C}_{2/n}$ als Basiscode (zur Erinnerung: Er ist ein $[n, n - 1, 2]$ - Code).
3. Die Formel für das Kontrollpolynom (es gilt: $h(x) = (x^N - 1)/g(x)$):
$$h(x) = \sum_{i=0}^{k-1} x^i.$$
folgt wieder unmittelbar aus MacWilliams [16] Ch7, §4.

□

Bei dem oben beschriebenen Konstruktionsprinzip des Mehrfachcodes bleibt also die Dimension des Basiscodes erhalten, während die Minimaldistanz mit demselben Faktor wächst, wie die Codelänge.
Bei der Suche nach anderen Arten der Vererbung finden wir auch zyklische Codes, bei denen die Minimaldistanz erhalten bleibt, während die Dimension mit demselben Faktor wächst, wie die Codelänge. Es ist also ein $[N, K, d]$-Code mit $N = m \cdot n$ und $K = m \cdot k$. Die zugehörige Automorphismengruppe ist dann:

$$Aut(C) \wr \mathfrak{S}_m \tag{2.8}$$

– außer, wenn $Aut(C) = \mathfrak{S}_a \wr \mathfrak{S}_2$ ist (Beweis siehe später).

Anders, als beim Prinzip der Mehrfachcodes ist die Existenz dieser zweiten Art der vererbten Codes und auch die Fortschreibung der Automorphismengruppe an bestimmte Voraussetzungen gebunden (siehe spätere Ausführungen zur „Rückwärtsvererbung“). Auch ist die Verwandtschaft zum Basiscode nicht unmittelbar aus der Generatormatrix erkennbar: Dahinter steckt das Konstruktionsprinzip der Plotkin-Summe in rekursiver Ausführung. Das wird in dem folgenden Einschub erklärt:

2.2 Die PLOTKIN-Summe (Einschub)

Definition 2.15 (PLOTKIN-**Summe)**
Seien $\mathcal{C}_1$ und $\mathcal{C}_2$ zwei Codes über demselben Alphabet (hier: über $\mathbb{F}_2$).
Dann ist $\mathcal{P}(\mathcal{C}_1, \mathcal{C}_2) := \{(u, u+v) \mid u \in \mathcal{C}_1, v \in \mathcal{C}_2\}$ die PLOTKIN-Summe *der beiden Codes.*
Das Ergebnis ist ein $[N_1 + max(N_1, N_2), k_1 + k_2, min(2 \cdot d_1, d_2)]$-Code.

Bemerkung 2.16
Man sieht sofort, daß diese Summe nicht kommutativ ist.
Auch ist die PLOTKIN-Summe von zwei zyklischen Codes nicht notwendig zyklisch. Wir müssen daher einige Vorbemerkungen mit Fallunterscheidungen machen, bevor wir die PLOTKIN-Summe zur Konstruktion von zyklischen Codes verwenden.

1. Sei $\mathcal{C}_1$ ein zyklischer Code der Länge l und $\mathcal{C}_0$ der Nullcode der Länge l. Dann ist $\mathcal{P}(\mathcal{C}_1, \mathcal{C}_0) := \{(u, u+0) \mid u \in \mathcal{C}_1\}$ zyklisch von der Länge $N = 2 \cdot l$ und er ist eine Verdopplung des Codes $\mathcal{C}_1$ (siehe obige Diskussion über Mehrfachcodes).

2. Sei $\mathcal{C}_1$ ein zyklischer Code der Länge l und $\mathcal{C}_M$ der erste Elementarcode der Länge l. Dann ist
   $\mathcal{P}(\mathcal{C}_M, \mathcal{C}_1) := \{(u, u+v) \mid u \in \mathcal{C}_M, v \in \mathcal{C}_1\}$ zyklisch und es ist $Aut(\mathcal{P}(\mathcal{C}_M, \mathcal{C}_1)) = Aut(\mathcal{P}(\mathcal{C}_1, \mathcal{C}_0))$.

3. Wegen der Bedeutung für die weitere Arbeit formulieren wir diesen Fall als

   Satz 2.17
   Seien $\mathcal{C}_1 \subseteq \mathcal{C}_2$ zwei zyklische Codes der Länge l. Dann ist
   $\mathcal{P}(\mathcal{C}_2, \mathcal{C}_1) := \{(u, u+v) \mid u \in \mathcal{C}_2, v \in \mathcal{C}_1\}$ i.a. nicht zyklisch, aber es existiert stets ein dazu isomorpher zyklischer Code $\widehat{\mathcal{C}} \cong \mathcal{P}(\mathcal{C}_2, \mathcal{C}_1)$ der Länge $N = 2 \cdot l$.

   Beweis. Ein Codevektor $z \in \mathcal{C} = \mathcal{P}(\mathcal{C}_2, \mathcal{C}_1)$ ist eine Aneinanderreihung zweier Codevektoren u und y mit $u, y \in \mathcal{C}_2$, da $\mathcal{C}_1 \subseteq \mathcal{C}_2$ nach Voraussetzung und somit $y := u + v$, $v \in \mathcal{C}_1$ definiert werden kann.
   Durch die folgende Koordinatenpermutation $\sigma \in \mathfrak{S}_N$ mit $\sigma : \mathcal{C} \longrightarrow \widehat{\mathcal{C}}$ entsprechen wir der Definition 0.36 von Code-Isomorphie. Die Abbildung $\sigma : z \mapsto \widehat{z} \in \widehat{\mathcal{C}}$ zeigt die Zyklizität von $\widehat{\mathcal{C}}$:

   $$z = (u_1, u_2, \ldots, u_l, y_1, y_2, \ldots, y_l),$$

   $$\widehat{z} = (u_1, y_1, u_2, y_2, \ldots\ldots, u_l, y_l).$$

   □

So genügen u.a. die im Abschnitt 10.2 diskutierten zyklischen Codes diesem Konstruktionsprinzip und auch die weiter unten in diesem Kapitel beschriebene „Rückwärtsvererbung“ läßt sich mithilfe der PLOTKIN-Summe verstehen:

So kann man durch wiederholte Anwendung der Summenbildung die Dimension des Basiscodes $\mathcal{C}_{Basis}$ vervielfachen – bei gleichzeitiger Beibehaltung der Minimaldistanz.
Hier nun die Rekursionsfomel (wichtig ist hier die Reihenfolge der Summanden):

$$\mathcal{C}_2 := \mathcal{P}(\mathcal{C}_{Basis}, \mathcal{C}_{Basis}) \tag{2.9}$$

$$\mathcal{C}_m := \mathcal{P}(\mathcal{C}_{Basis}, \mathcal{C}_{m-1}) \tag{2.10}$$

und es gilt – außer für $Aut(\mathcal{C}_{Basis}) = \mathfrak{S}_a \wr \mathfrak{S}_2$:[7]

$$Aut(\mathcal{C}_m) = Aut(\mathcal{C}_{Basis}) \wr \mathfrak{S}_m$$

$$\mathcal{C}_m \quad \text{ist also ein} \quad [m \cdot N_{Basis}, m \cdot k_{Basis}, d_{Basis}] - Code.$$

Als Beispiel wollen wir denselben $[7, 4, 3]$-Code wie im Beispiel 2.8 einer Rückwärtsvererbung mit der rekursiven PLOTKIN-Summe unterziehen:

Beispiel 2.18 (Rückwärtsvererbung mit der PLOTKIN-Summe)

```
Lfd.Nr.  k   d     #PermGrp          #AutoGrp

   3     4   3          7                168

[7, 4, 3] Cyclic Linear Code over GF(2)
Generator matrix:
[1 0 0 0 1 0 1]
[0 1 0 0 1 1 1]
[0 0 1 0 1 1 0]
[0 0 0 1 0 1 1]
> Cbas:=C3;
> C2x:=PlotkinSum(Cbas,Cbas);
> C3x:=PlotkinSum(Cbas,C2x);
> C3x;
[21, 12, 3] Linear Code over GF(2)
Generator matrix:
[1 0 0 0 1 0 1 | 0 0 0 0 0 0 0 | 0 0 0 0 0 0 0]
[0 1 0 0 1 1 1 | 0 0 0 0 0 0 0 | 0 0 0 0 0 0 0]
[0 0 1 0 1 1 0 | 0 0 0 0 0 0 0 | 0 0 0 0 0 0 0]
[0 0 0 1 0 1 1 | 0 0 0 0 0 0 0 | 0 0 0 0 0 0 0]
 --------------+---------------+--------------
[0 0 0 0 0 0 0 | 1 0 0 0 1 0 1 | 0 0 0 0 0 0 0]
[0 0 0 0 0 0 0 | 0 1 0 0 1 1 1 | 0 0 0 0 0 0 0]
[0 0 0 0 0 0 0 | 0 0 1 0 1 1 0 | 0 0 0 0 0 0 0]
[0 0 0 0 0 0 0 | 0 0 0 1 0 1 1 | 0 0 0 0 0 0 0]
 --------------+---------------+--------------
[0 0 0 0 0 0 0 | 0 0 0 0 0 0 0 | 1 0 0 0 1 0 1]
[0 0 0 0 0 0 0 | 0 0 0 0 0 0 0 | 0 1 0 0 1 1 1]
[0 0 0 0 0 0 0 | 0 0 0 0 0 0 0 | 0 0 1 0 1 1 0]
[0 0 0 0 0 0 0 | 0 0 0 0 0 0 0 | 0 0 0 1 0 1 1]
> IsCyclic(C3x);
false
```

[7] s. dazu auch Satz 2.19

Zwar ist dieser Code nicht zyklisch, aber dafür sieht man sehr deutlich die dreimalige Anordnung der Generatormatrix von *Cbas* auf der „Hauptdiagonalen“ der Generatormatrix von $C3x$.
Beim Vergleich der Code-Attribute mit denen der zyklischen Codes der Länge 21 finden wir Übereinstimmung beim Code mit der lfd. Nr. 39.

```
> load pgmdetailzyk;
Loading "pgmdetailzyk"
Detail-Auswertungsprogramm. Codelaenge ?
21
Code-Nummer aus der Liste ?
39
Soll der Erzeugungs-Vektor ermittelt werden ?
n

Zyklische Gruppencodes der Laenge n = 21
Detailauswertung von Code-Nummer:  39

Lfd.Nr.  k   d     #PermGrp          #AutoGrp

  39    12   3         21           28449792

[21, 12, 3] Cyclic Linear Code over GF(2)
Generator matrix:
[1 0 0 0 0 0 0 0 0 0 0 1 0 0 1 0 0 0 0 0]
[0 1 0 0 0 0 0 0 0 0 0 0 1 0 0 1 0 0 0 0]
[0 0 1 0 0 0 0 0 0 0 0 0 0 1 0 0 1 0 0 0]
[0 0 0 1 0 0 0 0 0 0 0 0 0 0 1 0 0 1 0 0]
[0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 1 0 0 1 0]
[0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 1 0 0 1]
[0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 1 0 0 1 0]
[0 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 1 0 0 1]
[0 0 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 1 0 0]
[0 0 0 0 0 0 0 0 0 1 0 0 1 0 0 0 0 0 1 0]
[0 0 0 0 0 0 0 0 0 0 1 0 0 1 0 0 0 0 0 1]

> IsIsomorphic(CS,C3x);
true Mapping from: ModTupFld: VN to ModTupFld: VN
(2, 13, 5, 11, 14, 10, 6, 19, 3, 16, 7, 4)(9, 20)(12, 18, 21, 15, 17)
>
```

Also ist der Code $C3x$ isomorph zu einem zyklischen Code und beide Codes haben die Automorphismengruppe $PSL(3,2) \wr \mathfrak{S}_3$.
Allerdings ist in der Generatormatrix des zyklischen Codes CS die Verwandschaft zum Basiscode *Cbas* nicht mehr unmittelbar erkennbar.

Ende des Beispiels
Ende des Einschubs über die PLOTKIN**-Summe**

Da wir in der Definition 2.1 des Mehrfachcodes keine weiteren Voraussetzungen zum jeweiligen Basiscode $\mathcal{C}_{Basis}$ gemacht haben, gilt der Satz 2.2 für jeden zyklischen Code und dessen Automorphismengruppe.
Wenn wir uns noch einmal das allgemeine Bild des Kranzproduktes vorstellen, so bedeutet dies, daß um die bisherige Basis-Automorphismengruppe $Aut(\mathcal{C}_{Basis})$ ein Kranz gelegt wird – mit sovielen Kopien der Gruppe $\mathfrak{S}_m$, wie die Kardinalität der Menge Ω angibt, auf der die Basis-Automorphismengruppe $Aut(\mathcal{C}_{Basis})$ operiert.
Dieses Bild erinnert sehr an die Struktur von Ahnentafeln, weshalb wir hier den Begriff der „Vererbung“ gewählt haben. Wir wollen dieses Prinzip „Vorwärtsvererbung“ nennen. Abhängig von Typ und Struktur der Basis-Automorphismengruppe gibt es aber auch eine „Rückwärtsvererbung“, bei der zusätzlich noch Ziel-Automorphismengruppen Aut_N mit

$$Aut_N \cong Aut_n \wr \mathfrak{S}_m \tag{2.11}$$

auftreten. Um beim obigen Bild zu bleiben, ist das so, wie wenn man durch Ahnenforschung noch einen Vor-Vorfahr mit dessen zusätzlichen Nachkommen in die Ahnentafel einpflegen muß. Wir wollen die beobachtete Gesetzmäßigkeit in einem Satz formulieren:

Satz 2.19 (**Zentraler Satz für zyklische Codes, Teil 1 (allgemeine Fassung)**)
Seien $n, m \in \mathbb{N}$ und C ein zyklischer $[n, k, d]$-Code.
Dann gibt es einen zyklischen $[N, K, d]$-Code $\widehat{C}_m$ der Länge $N = m \cdot n$ und Dimension $K = m \cdot k$ mit

$$Aut(\widehat{C}_m) \cong Aut(C) \wr \mathfrak{S}_m \tag{2.12}$$

außer, *wenn $m = 2$ und n gerade und gleichzeitig $Aut(C)$ ein reines Kranzprodukt aus symmetrischen Gruppen ist, bei dem $\mathfrak{S}_2$ als letzter Faktor aufgeführt ist.*

Um das zu verdeutlichen, schauen wir in das Tabellenwerk des Anhangs. So finden wir z.B. für $N = 28$ durchaus die Automorphismengruppe $PSL(3, 2) \wr \mathfrak{S}_2 \wr \mathfrak{S}_2$ als Rückwärtsvererbung einer Basis-Automorphismengruppe von $n = 14$, jedoch keine Automorphismengruppe der Gestalt $\mathfrak{S}_7 \wr \mathfrak{S}_2 \wr \mathfrak{S}_2$. Dagegen finden sich für $N = 30$ alle Rückwärtsvererbungen aller Automorphismengruppen von $n = 15$ (und natürlich auch von $n = 10$).

Beweis. Wir führen den Beweis in zwei Teilen:

1. die Existenzaussage beweisen wir zunächst durch Anwendung der PLOTKIN-Summe in rekursiver Weise zur Konstruktion des Codes C_m nach Formel (2.10).
   Die Existenz eines dazu isomorphen zyklischen Codes $\widehat{C}_m$ haben wir im Satz 2.17 bewiesen. Die Aussage zur Codelänge, Dimension und Minimaldistanz von $\widehat{C}_m \cong C_m$ ergibt sich letztlich aus der Definition 2.15 der PLOTKIN-Summe.

2. die Ausnahme-Aussage beweisen wir durch ein Gegenbeispiel und zeigen damit gleichzeitig, weshalb im Tabellenwerk nie „$\ldots \wr \mathfrak{S}_2 \wr \mathfrak{S}_2$“ am Ende eines mehrgliedrigen Kranzprodukts aus symmetrischen Gruppen auftaucht:
   Sei $n = 10$ und C_2 der $[10, 2, 5]$-Code mit Erzeugungsvektor

$Ev = (1,0,1,0,1,0,1,0,1,0)$ und Automorphismengruppe $\mathfrak{S}_5 \wr \mathfrak{S}_2$.
Nun konstruieren wir mit der PLOTKIN-Summe (s. Einschub oben) nach dem Prinzip der Rückwärtsverebung aus dem Basiscode C_2 einen Code $\mathcal{C}$ der Länge $N = 20$ mit doppelter Dimension und gleicher Minimaldistanz:

$$\mathcal{C} := \mathcal{P}(C_2, C_2) \tag{2.13}$$

Dieser $[20, 4, 5]$-Code $\mathcal{C}$ hat jedoch die Automorphismengruppe $\mathfrak{S}_5 \wr \mathfrak{S}_4$
(und eben nicht: $\mathfrak{S}_5 \wr \mathfrak{S}_2 \wr \mathfrak{S}_2$)! In der Liste der zyklischen Codes der Länge $N = 20$ kann unter der Nr. 6 der dazu isomorphe Code gefunden werden ($\mathcal{C} \cong C6$).

□

Schließlich wollen wir noch eine weitere Folgerung festhalten:

Durch die oben beschriebenen Konstruktionen der *Vorwärts-* und *Rückwärtsvererbung* entstehen zu je einem Code C der Länge n und seiner Automorphismengruppe $Aut(C)$ beim Übergang zur m-fachen Codelänge $N = m \cdot n$ je zwei vererbte Codes, nämlich C^m und C_m, sowie zwei vererbte Automorphismengruppen, nämlich $\mathfrak{S}_m \wr Aut(C)$ und $Aut(C) \wr \mathfrak{S}_m$ (abgesehen von der oben aufgeführetn Ausnahme).
Durch diese Art der „Fortpflanzung“ wird deutlich, weshalb es bei Codelängen mit vielen Faktorenzerlegungen besonders viele Codes und Automorphismengruppen gibt
(Bsp. $N = 30, 60, 80$).

Beim Studium der Automorphismengruppen für die verschiedenen Codelängen fiel auf, daß nicht nur die Anzahl, sondern auch die Komplexität der Struktur dieser Automorphismengruppen von der Primzahlzerlegung der Codelänge und damit auch von deren Teilermöglichkeiten abgängt.
Daher wollen wir zusätzlich zu den bisherigen Sätzen noch die beiden folgenden Aussagen formulieren:

Beobachtung 2.20
Sei $N = p^r$ eine Primzahlpotenz mit $r \geq 2$.
Dann bestehen die Automorphismengruppen der zyklischen Codes zur Codelänge N ausschließlich aus reinen Kranzprodukten (das gilt nicht für die kleinen Codelängen $4, 8$ und 9, für die keine nichttrivialen Codes nach unserer Definition existieren).

Satz 2.21
Sei $N = 2 \cdot p$, wobei p eine Primzahl ist mit $p \geq 5$, für die keine nichttrivialen Codes existieren.
Dann bestehen die Automorphismengruppen der zyklischen Codes zur Codelänge N ausschließlich aus den beiden Kranzprodukten $\mathfrak{S}_2 \wr \mathfrak{S}_p$ und $\mathfrak{S}_p \wr \mathfrak{S}_2$ und es existieren nur die 5 typischen nichttrivialen Codes (s. Abschnitt 1.2.1).

Beispiel: $N = 10$, 22, 26, 34, 38, 58, 74; aber nicht 14, 46 (s. Tabellenwerk)

Beweis. Nach den obigen Ausführungen über Mehrfachcodes gibt es die beiden Kranzprodukte

1. $\mathfrak{S}_2 \wr \mathfrak{S}_p$
   (a) mit der Verdopplung des „ersten Elementarcodes“ $\mathcal{C}_{1/p}$ als Basiscode. Das ergibt den selbstdualen $[N, p, 2]$ - Code.
   (b) mit der Verdopplung des „zweiten Elementarcodes“ $\mathcal{C}_{2/p}$ als Basiscode. Das ergibt den $[N, p-1, 4]$ - Code und seinen dualen $[N, p+1, 2]$ - Code.
2. $\mathfrak{S}_p \wr \mathfrak{S}_2$ mit der Ver-p-fachung des „ersten Elementarcodes“ $\mathcal{C}_{1/2}$ als Basiscode. Das ergibt den $[N, 2, p]$ - Code und seinen dualen $[N, N-2, 2]$ - Code.

Weitere Codes und weitere Automorphismengruppen können aus folgenden Gründen nicht auftreten:

1. Falls es zu der Primzahl p nur die 4 primitiven Codes gibt, so hat die Bahnzerlegung von $\Omega_p = \{1, 2, \ldots, p\}$ nur 2 Bahnen (s. auch Abschnitt 1.1, Fakt 1.4).
   Im Kapitel 6 werden wir im Satz 6.3 (1. Hauptsatz zur Anzahl der zyklischen Codes) zeigen, daß dann für $N = 2 \cdot p$ genau $3^2 = 9$ zyklische Codes existieren. Abzüglich der 4 primitiven Codes der Länge N bleiben die oben beschriebenen 5 nichttrivialen Codes übrig.
   Wegen der Konstruktion der 5 Codes kann es auch über die beiden angegebenen Automorphismengruppen hinaus keine weitere geben:
   Nach Lemma 0.28 gilt: $Aut(C) = Aut(C^{\perp})$; somit kann es bei diesen 5 Codes rein rechnerisch nicht mehr als 3 Automorphismengruppen geben. Wegen $p \geq 5$ existiert der zweite Elementarcode $\mathcal{C}_{2/p}$, der mit $\mathfrak{S}_p$ dieselbe Automorphismengruppe hat, wie der erste Elementarcode $\mathcal{C}_{1/p}$. Damit kann der eine selbstduale Code der Länge $N = 2 \cdot p$ aber keine eigenständige dritte Automorphismengruppe haben, so daß es bei den zwei angegebenen Automorphismengruppen bleibt.

2. Falls die Bahnzerlegung von $\Omega_p = \{1, 2, \ldots, p\}$ mehr als 2 Bahnen hat, so kann es nach Voraussetzung nur auflösbare Automorphismengruppen $Aut(C)$ zu den nicht-primitiven Codes der Länge p geben (Bsp.: $N = 17$). Da $\mathfrak{S}_2$ ebenfalls auflösbar ist, sind auch die nach diesem Kapitel durch Vor- bzw. Rückwärtsvererbung entstehenden Automorphismengruppen $\mathfrak{S}_2 \wr Aut(C)$, bzw. $Aut(C) \wr \mathfrak{S}_2$ auflösbar, weshalb auch die nicht-primitiven Codes der Länge $N = 2 \cdot p$ trivial (im Sinne dieser Arbeit) sind.

□

Kapitel 3

Zusammenfassung zyklische Codes

Dieses Kapitel ist umfangreich. Daher soll hier die Kapitelstruktur vorgestellt werden.

- Zusammenfassung zyklische Codes $N = a \cdot b$
- Zusammenfassung zyklische Codes $N = a \cdot b \cdot c$
- Zusammenfassung zyklische Codes $N = a \cdot b \cdot c \cdot e$
- Selbstduale zyklische Codes
- Zyklische Codes $N = 2 \cdot l$ mit Spezialgruppen

3.1 Zerlegung der Codelänge in 2 Faktoren

Nun wollen wir die Ergebnisse aus der Untersuchung der zyklischen Codes gerader und ungerader Länge zusammenfassen.
Dazu formulieren und beweisen wir den folgenden zentralen Satz:

Satz 3.1
Sei $N = k \cdot d$ eine Faktorenzerlegung mit $N, k, d \in \mathbb{N}$, wobei k und d nicht beide gleichzeitig kleiner als 5 sein dürfen.
Dann gelten folgende Aussagen:

1. *es existiert ein zyklischer $[N, k, d]$-Code C*
2. *die Generatormatrix G besteht aus der Aneinanderreihung von d Einheitsmatrizen der Dimension k*
3. *der Erzeugungsvektor[1] $v \in \mathbb{F}_2^N$ von C steht (in diesem Spezialfall) in der ersten Zeile von G. $v \in \mathbb{F}_2^N$ von C lautet $v = (1,0,0,\ldots,0;1,0,0,\ldots,0;\ldots;1,0,0,\ldots,0)$, dabei wird der k-elementige Teilvektor $u = (1,0,0,\ldots,0) \in \mathbb{F}_2^k$ d-mal wiederholt.*

[1] siehe dazu auch das folgende Kapitel 2 „Vererbung von zyklischen Codes und ihren Automorphismengruppen“

4. *das Generatorpolynom von C hat als Koeffizienten den Erzeugungsvektor*

$$g(x) = \sum_{i=1}^{N} v_i x^{i-1} = \sum_{j=0}^{d-1} x^{jk} \tag{3.1}$$

5. *die Automorphismengruppe von C ist das Kranzprodukt*

$$\mathfrak{S}_d \wr \mathfrak{S}_k \tag{3.2}$$

6. *der zu C duale Code $C^\perp$ ist ein zyklischer $[N, N-k, 2]$-Code und hat dieselbe Automorphismengruppe.*

7. *der Erzeugungsvektor $w \in \mathbb{F}_2^N$ von $C^\perp$ lautet $w = (1, 0, \ldots, 1, 0, \ldots, 0)$, mit der zweiten 1 in Position $k+1$, und er steht versetzt in der letzten Zeile von H (führende Nullen entfernen und rechts neben der Matrix wieder anfügen; die Kontrollmatrix H von C ist die Generatormatrix von $C^\perp$).*

8. *falls $k = 2$, so wird Aut(C) nur von diesen beiden Codes angenommen*

9. *falls $k = \frac{N}{2}$, so fallen C und $C^\perp$ zu einem einzigen selbstdualen $[N, \frac{N}{2}, 2]$-Code zusammen*

10. *falls $k > 2$, so wird Aut(C) zusätzlich noch von einem zyklischen $[N, k-1, 2d]$-Code B, sowie von dem zugehörigen dualen $[N, N-k+1, 2]$-Code $B^\perp$ angenommen*

11. *der Erzeugungsvektor $y \in \mathbb{F}_2^N$ von B lautet $y = (1, 1, 0, \ldots, 0; 1, 1, 0, \ldots, 0; \ldots\ldots; 1, 1, 0, \ldots, 0)$, dabei wird der k-elementige Teilvektor $u = (1, 1, 0, \ldots, 0) \in \mathbb{F}_2^k$ d-mal wiederholt.*

12. *der Erzeugungsvektor $z \in \mathbb{F}_2^N$ von $B^\perp$ lautet $z = (1, 1, 1, \ldots, 1; 0, \ldots\ldots, 0)$, mit k Einsen zu Beginn – der Rest sind Nullen*

Beweis. zu den Aussagen 1 bis 12 im Einzelnen:

- die Aussagen 1 und 2 sind im Kapitel 2 nach der Definition 2.1 des „Mehrfachcodes“ in den dort folgenden Sätzen 2.3 und 2.4 bewiesen.
- die Aussage 3 ist in Folgerung 2.12, dortige Aussage 2 gezeigt
- die Aussage 4 ist in Folgerung 2.12, dortige Aussage 3 gezeigt
- die Aussage 5 ist bewiesen mit Satz 2.2, dabei ist $Aut(C)$ die Automorphismengruppe des Basiscodes. Der Basiscode ist in diesem Fall der **erste Elementarcode** $\mathcal{C}_{1/k}$ (s. Abschnitt 2.1) und in Folgerung 9.5 zeigen wir, daß $Aut(C) = Aut(\mathcal{C}_{1/k}) = \mathfrak{S}_k$
- zur Aussage 6:

1. Nach MacWilliams [16] Ch7, §5, Theorem 4 ist der duale Code eines zyklischen Codes ebenfalls zyklisch
2. Nach W.C. Huffman [14] Kapitel „Codes and Groups“, Seite 1353 gilt $Aut(\mathcal{C}) = Aut(\mathcal{C}^{\perp})$ (s.a. Lemma 0.28)
3. Die Aussage, daß die Minimaldistanz von $\mathcal{C}^{\perp}$ stets den Wert 2 annimmt, folgt aus Punkt 7

- die Aussage 7 ist gleichbedeutend mit:

$$g(\mathcal{C}^{\perp}) = h(\mathcal{C}) = 1 + x^k \tag{3.3}$$

  zum Beweis siehe Beweis von Satz 2.13

- zu den Aussagen 8, 10 und 11: bei $k = 2$ steht als Basiscode für unseren Mehrfachcode nur der **erste Elementarcode** $\mathcal{C}_{1/2}$ (s. Abschnitt 2.1) zur Verfügung, während bei $k > 2$ auch der **zweite Elementarcode** $\mathcal{C}_{2/k}$ (s. Abschnitt 2.1) zur Verfügung steht. Da dessen Dimension um 1 kleiner ist, dafür aber die Minimaldistanz $\equiv 2$ ist, ergeben sich die hier gemachten Aussagen

- die Aussage 12 ist gleichbedeutend mit:

$$g(\mathcal{B}^{\perp}) = h(\mathcal{B}) = \sum_{i=0}^{k-1} x^i \tag{3.4}$$

  zum Beweis siehe Beweis von Satz 2.14.

□

Folgerung 3.2

Aus dem soeben bewiesenen Satz lassen sich einige Folgerungen ableiten:

1. *falls $k \neq d$, so existiert noch mindestens ein weiterer zyklischer Code C' ($[N, d, k]$) zur obigen Faktorzerlegung*
2. *es gelten dafür sinngemäß alle weiteren Aussagen des obigen Satzes*
3. *Codelängen N mit vielfältigen Faktorzerlegungsmöglichkeiten besitzen dadurch mehr zyklische Codes, als andere*
4. *für eine gewünschte Minimaldistanz d und einer benötigten Anzahl k zu übertragende Nachrichtenbits läßt sich so nach dem obigen Satz ein zyklischer Code C als $[N = k \cdot d, k, d]$-Code konstruieren, der die Anforderungen erfüllt und dessen Automorphismengruppe mit Aut(C)=$\mathfrak{S}_d \wr \mathfrak{S}_k$ bekannt ist (diese Folgerung haben wir unter der Nummer 2.13 als* **„Erster Hauptsatz für zyklische Codes“** *herausgestellt).*
5. *hat N keine Faktorenzerlegung, d.h., ist N prim, so gibt es deswegen i.a. keine nichttrivialen zyklischen Codes der Länge N. Ausnahmen gibt es durch die Existenz von speziellen Permutationsgruppen für $N = 7, 23, 31, 73, 127$, etc., die hier als Automorphismengruppen auftreten und jeweils dann von allen Codes angenommen werden. Siehe hierzu auch den Abschnitt 1.1 „Codelängen ohne zyklische Codes“.*

Außer den oben beschriebenen Kranzprodukten zweier Faktoren $\mathfrak{S}_a \wr \mathfrak{S}_b, N = a \cdot b$ tritt unter bestimmten Voraussetzungen auch das direkte Produkt der beiden Faktoren $\mathfrak{S}_a \times \mathfrak{S}_b$ als Automorphismengruppe auf.

Satz 3.3 (Zentraler Satz für zyklische Codes, Teil 3)
Sei $N = a \cdot b$ eine Faktorenzerlegung mit $N, a, b \in \mathbb{N}$. Es sei ferner $2 \neq a < b \geq 5$[2] und a sei teilerfremd zu b.
Dann gelten folgende Aussagen:
Es gibt für $a \neq 4$ weitere 4 (oder nur 2 im Fall $a = 4$) zyklische Codes der Länge N mit der Automorphismengruppe

$$\mathfrak{S}_a \times \mathfrak{S}_b, \tag{3.5}$$

nämlich:

1. *ein $[N, a+b-1, a]$-Code*
2. *der dazu duale $[N, N-a-b+1, 4]$-Code*
   mit Erzeugungsvektor $Ev = (\overbrace{\underbrace{1,1,\ldots,1}_{a-mal},0,\ldots,0}^{b-Positionen},\overbrace{1,1,\ldots,1}^{a-mal},0,\ldots,0,\ldots,0)$ *, sowie –*
   falls $4 \neq a$ –
3. *ein $[N, a+b-2, d]$-Code mit*

$$d = \begin{cases} a & : \text{ falls } a \text{ gerade} \\ b & : \text{ falls } b \text{ gerade und } b < 2a \\ 2a & : \text{ sonst} \end{cases}$$

   und
4. *der dazu duale $[N, N-a-b+2, 4]$-Code*

Anmerkungen zur Beweisführung und der weiteren Vorgehensweise:

- in der folgenden Bemerkung werden die Codes erläutert, die zur Automorphismengruppe $\mathfrak{S}_a \times \mathfrak{S}_b$ gehören. Insbesondere werden die Sonderfälle $a = 2$ und $a = 4$ diskutiert.
- Dann werden wir den ersten von vier Fällen im Satz 3.6 formulieren und allgemein beweisen. Anschließend werden wir auch die übrigen Fälle in einer Reihe von Lemmata beweisen.
- Danach folgt der Satz 3.14, in dem formuliert und exemplarisch bewiesen wird, daß für den Fall $a = 4$ eine echte Obergruppe zu $\mathfrak{S}_a \times \mathfrak{S}_b$ als Automorphismengruppe für zwei der vier o.g. Codes existiert.

[2] Die Einschränkung $b \geq 5$ hängt mit der Forderung zusammen, daß die Automorphismengruppe nicht auflösbar sein soll. Geht man von dieser Forderung ab, so kann man diese Voraussetzung fallen lassen.

- Den Abschluß bildet ein allgemeiner Teilbeweis zum Satz 3.14, in dem wir zeigen, daß $\mathfrak{S}_a \times \mathfrak{S}_b \leq Aut(D)$ für die im Satz genannten Codes gilt.

Erinnerung 3.4
Wegen der Bedeutung für die folgenden Erklärungen und die anschließenden Beweisführungen sei hier noch einmal an die beiden Elementarcodes aus dem Abschnitt 2.1 erinnert:

1. der Code $\mathcal{C}_{1/n}$. Es ist ein $[n, n, 1]$ - Code.
   Er besteht aus dem gesamten n-dimensionalen Vektorraum $\mathbb{F}_2^n$.
   Seine Generatormatrix ist daher die n-dimensionale Einheitsmatrix E_n.
   Sein Generatorpolynom ist $g_{\mathcal{C}_{1/n}}(x) \equiv 1$.
   Er ist der **erste Elementarcode**.
   Bezeichnung in **Magma:** `UniverseCode(GF(2),n)`

2. der Code $\mathcal{C}_{2/n}$. Es ist ein $[n, n-1, 2]$ - Code.
   Er besteht aus einem $(n-1)$-dimensionalen Untervektorraum.
   Sein Generatorpolynom ist $g_{\mathcal{C}_{2/n}}(x) = x + 1$.
   Er ist der **zweite Elementarcode**.
   Bezeichnung in **Magma:** `ZeroSumCode(GF(2),n)`, oder `EvenWeightCode(n)`

Bemerkung 3.5
Da wegen a teilerfremd zu b folgendes gilt:

$$\mathfrak{S}_a \times \mathfrak{S}_b = (\mathfrak{S}_a \wr \mathfrak{S}_b) \cap (\mathfrak{S}_b \wr \mathfrak{S}_a), \tag{3.6}$$

so gilt im allgemeinen (d.h., $a \neq 2, 4$), daß die Codes folgendermaßen miteinander verknüpft sind:
Sei C ein Code mit $Aut(C) = \mathfrak{S}_a \times \mathfrak{S}_b$, dann ist

$$C = C_1 + C_2, \text{ mit } Aut(C_1) = \mathfrak{S}_b \wr \mathfrak{S}_a \text{ und } \dim(C_1) < N/2, \tag{3.7}$$

$$\text{sowie } Aut(C_2) = \mathfrak{S}_a \wr \mathfrak{S}_b \text{ und } \dim(C_2) < N/2. \tag{3.8}$$

Den Aufbau der Codes C_1, C_2 als Mehrfachcodes haben wir bereits im Kapitel 2 „Vererbung von zyklischen Codes und ihren Automorphismengruppen“ diskutiert:
Dort sahen wir, daß es für $N = a \cdot b$ je einen (b-fachen) Mehrfachcode mit der Automorphismengruppe $\mathfrak{S}_b \wr \mathfrak{S}_a$ auf der Basis des ersten Elementarcodes $\mathcal{C}_{1/a}$, bzw. des zweiten Elementarcodes $\mathcal{C}_{2/a}$ gibt und je einen (a-fachen) Mehrfachcode mit der Automorphismengruppe $\mathfrak{S}_a \wr \mathfrak{S}_b$ auf der Basis des ersten Elementarcodes $\mathcal{C}_{1/b}$, bzw. des zweiten Elementarcodes $\mathcal{C}_{2/b}$ gibt.
Das heißt, es gibt jetzt hier insgesamt **vier Fälle** der Summenbildung; die zu diesen Mehrfachcodes gehörenden dualen Codes scheiden für diese Summenbildung aus: Wegen der großen Dimension folgt stets $Aut(C) = \mathfrak{S}_N$. Um diese dualen Codes von der Betrachtung auszuschließen, haben wir im Folgenden den Zusatz „mit $\dim(C_i) < N/2$“ angefügt.
Die obige Aussage läßt sich am Beispiel $N = 15$ mit $a = 3$ und $b = 5$ gut nachvollziehen (Lfd.Nr. 2, 4 (für C_1), 10, 12 (für C_2), 20, 28 (für C) aus Listezyk15, bzw. mit diesen

Indizes in Codefilezyk15 auf der beiliegenden CD verfügbar).

Wir wollen nun die beiden Sonderfälle $a = 2$, 4 diskutieren:

- Die Voraussetzung $2 \neq a$ ist erforderlich, da für $a = 2$ und a teilerfremd zu b gilt: $\mathfrak{S}_2 \times \mathfrak{S}_b$ ist maximale Untergruppe von $\mathfrak{S}_2 \wr \mathfrak{S}_b$ und alle 3 Verknüpfungen des einen (!) Codes[3] zur Automorphismengruppe $\mathfrak{S}_b \wr \mathfrak{S}_2$ mit den 3 Codes zur Automorphismengruppe $\mathfrak{S}_2 \wr \mathfrak{S}_b$ ergeben stets wieder den ersten Code zur Automorphismengruppe $\mathfrak{S}_2 \wr \mathfrak{S}_b$, siehe Bsp. 1.23 im Abschnitt 1.2.1, $b = 5$, $N = 10$, mit Cx, $x =$ Lfd.Nr. aus der Liste:

$$\mathcal{C} = C2 + C3 = C2 + C4 = C2 + C5 = C3. \tag{3.9}$$

  Noch eleganter sieht man, daß $\mathfrak{S}_2 \times \mathfrak{S}_b$ nicht als volle Automorphismengruppe existieren kann, wenn wir uns den potentiellen Erzeugungsvektor eines Codes zu dieser Gruppe nach der Konstruktionsvorschrift aus dem obigen Satz 3.3 ansehen:

$$Ev = (\underbrace{\overbrace{1,1,}^{2-mal}\ 0,\ldots,0}_{b-Positionen},\ \overbrace{1,1,}^{2-mal}\ 0,\ldots,0) \tag{3.10}$$

  Dieser Code ist jedoch die Verdopplung des „zweiten Elementarcodes“ $\mathcal{C}_{2/b}$ (s. Abschnitt 2.1) und somit als einer der 5 Standardcodes der geraden Codelänge $N = 2 \cdot b$ bereits wohlbekannt – mit der zugehörigen Automorphismengruppe $\mathfrak{S}_2 \wr \mathfrak{S}_b$. Diese Gruppe hat eine größere Ordnung als $\mathfrak{S}_2 \times \mathfrak{S}_b$; sie ist daher die volle Automorphismengruppe.

- Für den Sonderfall $a = 4$ wurde festgestellt, daß der $[N, a + b - 2, d]$-Code C aus dem obigen Satz durchaus existiert, aber es gilt:

$$\mathfrak{S}_4 \times \mathfrak{S}_b \neq Aut(C)$$

$$\mathfrak{S}_4 \wr \mathfrak{S}_b \neq Aut(C),$$

  wobei uns die zweite Ungleichung an den obigen Sonderfall mit $a = 2$ erinnert, für den sie dort noch eine Gleichung war. Wir finden (s. a. Hasse-Diagramm „Die 8 Automorphismengruppen der zykl. Codes zur Codelänge $N = 20$ im Untergruppenverband von $\mathfrak{S}_{20}$“ einige Seite weiter unten):

$$\mathfrak{S}_4 \times \mathfrak{S}_b < Aut(C) < \mathfrak{S}_4 \wr \mathfrak{S}_b. \tag{3.11}$$

  Dabei ist $Aut(C)$ eine minimale Obergruppe von $\mathfrak{S}_4 \times \mathfrak{S}_b$. Wir werden das im späteren Satz 3.14 zusammenfassen.
  Entscheidend für diese Ausnahmesituation ist hier der $[N, 3, \frac{N}{2}]$-Code C_1
  mit $Aut(C_1) = \mathfrak{S}_b \wr \mathfrak{S}_4$, der in Summe mit einem Code C_2, mit $Aut(C_2) = \mathfrak{S}_4 \wr \mathfrak{S}_b$

[3] wir sahen im Abschnitt 2.1, daß es zur Automorphismengruppe $\mathfrak{S}_b \wr \mathfrak{S}_2$ stets nur einen Code gibt. Mit dem dazu dualen Code sind es dann insgesamt 2.

und $\dim(C_2) < N/2$, den Code C ergibt. Wenn wir uns den Erzeugungsvektor Ev von C_1 ansehen

$$Ev_{C_1} = (\underbrace{\overbrace{1,1,0,0}^{4\,Positionen}\ ,1,1,0,0,\ldots\ldots,1,1,0,0,\ \overbrace{1,1,0,0}^{4\,Positionen}}_{N=4b-Positionen}), \tag{3.12}$$

dann erkennen wir b Gruppierungen von 4 Elementen $(1,1,0,0)$ – d.h., daß es sich hier beim Code C_1 um die Ver-b-fachung des **zweiten Elementarcodes** $\mathcal{C}_{2/4}$ nach unserer Vererbungslehre handelt. Durch das besondere Muster des Erzeugungsvektors, das es nur bei $a = 4$ gibt, bekommen wir eine zusätzliche Symmetrie in der Automorphismengruppe $Aut(C)$, so daß (3.11) gilt.
Wir werden das an einem Beispiel im Zusammenhang mit dem Satz 3.14 erklären.

Für den anderen Code C_3, ein $[N, 4, b]$-Code, mit $Aut(C_3) = \mathfrak{S}_b \wr \mathfrak{S}_4$, der in Summe mit einem Code C_2, mit $Aut(C_2) = \mathfrak{S}_4 \wr \mathfrak{S}_b$ und $\dim(C_2) < N/2$, den Code D ergibt, bekommen wir dann $Aut(D) = \mathfrak{S}_4 \times \mathfrak{S}_b$.

Fassen wir noch einmal zusammen: Sei $ggT(a, b) = 1, a < b,$ mit $b \geq 5$. Dann existieren zu der Gruppe

$$\mathfrak{G} = \mathfrak{S}_a \times \mathfrak{S}_b \tag{3.13}$$

- für $a = 2$ **keine** Codes C mit $\mathfrak{G}$ als Automorphismengruppe,
- für $a = 4$ **ein** Code C (und sein dualer Code $C^\perp$) mit $\mathfrak{G}$ als Automorphismengruppe,
- für $a \neq 2, 4$ **zwei** Codes C, D (und ihre dualen Codes $C^\perp$, $D^\perp$) mit $\mathfrak{G}$ als Automorphismengruppe (für diese Situation hatten wir die Redewendung „im allgemeinen“ verwendet).

Allgemein gilt noch: Wegen der Konstruktion der Automorphismengruppe als direktes Produkt $\mathfrak{S}_a \times \mathfrak{S}_b$ ist die Ordnung dieser Automorphismengruppe erheblich kleiner, als die Ordnung der Automorphismengruppen aus Kranzprodukten. Siehe dazu auch die Tabellen im Anhang für $N = 15$, 20, 21, 24, 28, 30, 33, 35, 36, 39, 40, 42, 45, usw.

Ende der Bemerkung

Wir geben nun zum obigen Satz 3.3 einen vollständigen allgemeinen Beweis, d.h., für alle vier Fälle der Summenbildung:
Wir beginnen mit dem Beweis für den ersten der vier Fälle. In diesem **ersten Fall** sind beide Summanden Mehrfachcodes aus dem ersten Elementarcode.

Satz 3.6
Sei $2 < a < b$ mit $ggT(a, b) = 1$ und $N = a \cdot b$. Sei nun
C^a der a-malige Mehrfachcode des ersten Elementarcodes $\mathcal{C}_{1/b}$ mit $Aut(C^a) = \mathfrak{S}_a \wr \mathfrak{S}_b$,

C^b der b-malige Mehrfachcode des ersten Elementarcodes $\mathcal{C}_{1/a}$ mit $Aut(C^b) = \mathfrak{S}_b \wr \mathfrak{S}_a$ und es sei $C := C^a + C^b$. Dann gilt:

$$Aut(C) = \mathfrak{S}_a \times \mathfrak{S}_b \text{ und } C \text{ ist ein } [N, a+b-1, a]\text{-Code.} \tag{3.14}$$

Beweis. Der Code C^a wird von b Vektoren $v_1, \ldots, v_b \in \mathbb{F}_2^N$ erzeugt, wobei die v_j durch zyklische Verschiebung aus einander hervorgehen. Da $N = a \cdot b$, können wir diese Vektoren auch als Matrizen mit a Zeilen und b Spalten schreiben, also als Elemente aus $M(a, b, \mathbb{F}_2)$. Das sieht dann folgendermaßen aus:

$$v_1 = \begin{pmatrix} 100\ldots0 \\ 100\ldots0 \\ \vdots \\ 100\ldots0 \end{pmatrix}, v_2 = \begin{pmatrix} 010\ldots0 \\ 010\ldots0 \\ \vdots \\ 010\ldots0 \end{pmatrix}, \ldots, v_b = \begin{pmatrix} 00\ldots01 \\ 00\ldots01 \\ \vdots \\ 00\ldots01 \end{pmatrix}. \tag{3.15}$$

Der Code C^b wird von a Vektoren $w_1, \ldots, w_a \in \mathbb{F}_2^N$ erzeugt, wobei die w_i durch zyklische Verschiebung aus einander hervorgehen. Nach Konstruktion hat jeder der a erzeugenden Vektoren w_i genau b Einsen, gefolgt von jeweils $a-1$ Nullen, also z.B.

$$w_1 = (\overbrace{\underbrace{1,0,0,\ldots,0}_{a\ Positionen},1,0,0,\ldots,0,\ldots\ldots,1,0,0,\ldots,0,\underbrace{1,0,0,\ldots,0}_{a\ Positionen}}^{N=a\cdot b\ \ Positionen}). \tag{3.16}$$

Damit die Erzeugungsvektoren auch dieses Mal nach einem bestimmten Muster in das gleiche Matrix-Schema passen, ersetzen wir den zyklischen Code C^b durch den dazu isomorphen quasi-zyklischen Code $\widehat{C}^b$, der von folgenden a Vektoren $\widehat{w}_1, \ldots, \widehat{w}_a \in \mathbb{F}_2^N$ erzeugt wird:

$$\widehat{w}_1 = (\overbrace{\underbrace{1,1,1,\ldots,1}_{b\ Positionen},0,0,0,\ldots,0,\ldots\ldots,0,0,0,\ldots,0,\underbrace{0,0,0,\ldots,0}_{b\ Positionen}}^{N=a\cdot b\ \ Positionen}),$$

$$\widehat{w}_2 = (\overbrace{\underbrace{0,0,0,\ldots,0}_{b\ Positionen},\underbrace{1,1,1,\ldots,1}_{b\ Positionen},\ldots\ldots,0,0,0,\ldots,0,\underbrace{0,0,0,\ldots,0}_{b\ Positionen}}^{N=a\cdot b\ \ Positionen}),$$

$$\ldots\ldots\ldots$$

$$\widehat{w}_a = (\overbrace{\underbrace{0,0,0,\ldots,0}_{b\ Positionen},\ldots\ldots,0,0,0,\ldots,0,\underbrace{0,0,0,\ldots,0}_{b\ Positionen},\underbrace{1,1,1,\ldots,1}_{b\ Positionen}}^{N=a\cdot b\ \ Positionen}).$$

Jetzt werden wir diese Vektoren ebenfalls als Matrizen mit a Zeilen und b Spalten schreiben, also als Elemente aus $M(a, b, \mathbb{F}_2)$. Das sieht dann folgendermaßen aus:

$$\widehat{w}_1 = \begin{pmatrix} 111\ldots1 \\ 000\ldots0 \\ \vdots \\ 000\ldots0 \end{pmatrix}, \widehat{w}_2 = \begin{pmatrix} 000\ldots0 \\ 111\ldots1 \\ \vdots \\ 000\ldots0 \end{pmatrix}, \ldots, \widehat{w}_a = \begin{pmatrix} 00\ldots00 \\ 00\ldots00 \\ \vdots \\ 11\ldots11 \end{pmatrix}. \tag{3.17}$$

Wir wollen nun zunächst zeigen, daß für $\widehat{C} := C^a + \widehat{C}^b$ gilt: $Aut(\widehat{C}) = \mathfrak{S}_a \times \mathfrak{S}_b$.

$\mathfrak{S}_a$ vertauscht die Zeilen. $\mathfrak{S}_b$ vertauscht die Spalten. Dazu genügt es, einzusehen, daß jeder Automorphismus Zeilen und Spalten jeweils als ganzes vertauscht. Dies folgt, wenn wir zeigen, daß $v_1, \ldots, v_b$ genau die b Codewörter des Gewichts a sind und $\widehat{w}_1, \ldots, \widehat{w}_a$ genau die a Codewörter des Gewichts b sind.
Dazu betrachten wir ein beliebiges Codewort c, also eine Linearkombination der Erzeugenden:

$$c = \sum_{j=1}^{b} \lambda_j \cdot v_j + \sum_{i=1}^{a} \mu_i \cdot \widehat{w}_i \quad \text{mit } x := \sum_{j=1}^{b} \lambda_j \text{ und } y := \sum_{i=1}^{a} \mu_i. \tag{3.18}$$

Das Gewicht von c ist dann

$$md(c) = (b - x) \cdot y + (a - y) \cdot x. \tag{3.19}$$

Ist $0 < x < b$, dann ist das Gewicht $md(c)$ mindestens $1 \cdot y + (a - y) \cdot 1 = a$. Gleichheit gilt nur, falls $b = 2$ (ausgeschlossen), oder $y = 0$, oder $y = a$ ist.
Ist $x = 0$, oder $x = b$, so ist das Gewicht $md(c)$ ein Vielfaches von b. Daraus folgt, daß die Codeworte des Gewichts a genau die v_j sind.
Genauso zeigt man, daß die Codeworte des Gewichts b genau die $\widehat{w}_i$ sind.
Abschließend müssen wir noch den Isomorphismus

$$\sigma : C^b \longrightarrow \widehat{C}^b, \ \sigma : w_i \mapsto \widehat{w}_i \tag{3.20}$$

diskutieren: Zunächst gilt $\sigma \in \mathfrak{S}_N$. Wir wollen jedoch σ so wählen, daß

$$\sigma(C^a) = C^a \text{ gilt, d.h., } \sigma \in Aut(C^a) = \mathfrak{S}_a \wr \mathfrak{S}_b. \tag{3.21}$$

In Lemma 2.7 hatten wir bewiesen, daß

$$\underbrace{\mathfrak{S}_a \times \mathfrak{S}_a \times \ldots \times \mathfrak{S}_a}_{b-mal} \leq Aut(C^a). \tag{3.22}$$

Die Komponenten operieren auf den Spalten in der Schreibweise 3.15 und lassen daher den Code C^a invariant.
Beim Code C^b steht bei der Matrixschreibweise der Erzeugungsvektoren w_i in jeder Spalte genau eine Eins (wegen $ggT(a, b) = 1$). Also können wir Elemente $\sigma \in \underbrace{\mathfrak{S}_a \times \mathfrak{S}_a \times \ldots \times \mathfrak{S}_a}_{b-mal}$ benutzen, um

$$\widehat{w}_1 = \begin{pmatrix} 111\ldots1 \\ 000\ldots0 \\ \vdots \\ 000\ldots0 \end{pmatrix}, \widehat{w}_2 = \begin{pmatrix} 000\ldots0 \\ 111\ldots1 \\ \vdots \\ 000\ldots0 \end{pmatrix}, \ldots, \widehat{w}_a = \begin{pmatrix} 00\ldots00 \\ 00\ldots00 \\ \vdots \\ 11\ldots11 \end{pmatrix}. \tag{3.23}$$

aus den w_i zu erzeugen. Somit haben wir gezeigt:

$$\widehat{C} = \sigma(C) = \sigma(C^a + C^b) = \sigma(C^a) + \sigma(C^b) = C^a + \widehat{C}^b \text{ und es gilt: } Aut(\widehat{C}) = \mathfrak{S}_a \times \mathfrak{S}_b.$$

Wegen $\widehat{C} \cong C$ folgt dann: $Aut(C) = Aut(\widehat{C}) = \mathfrak{S}_a \times \mathfrak{S}_b$.

Abschließend müssen wir noch die Aussagen zur Dimension und Minimaldistanz des Codes C zeigen:
Es gilt $md(C^a) = a$ und $md(C^b) = b$ nach Konstruktion. Da $a < b$ nach Voraussetzung und wegen $C^a \leq C$ gilt $md(C) = a$. Codewörter mit kleinerer Minimaldistanz als a kann es wegen der Konstruktion des Codes C nicht geben.

Wenn wir uns noch einmal die obigen Matrizen der Erzeugungsvektoren der v_j und $\widehat{w}_i$ ansehen, erkennen wir, daß sich z.B. der Vektor $\widehat{w}_a$ linear aus allen übrigen Vektoren v_j und $\widehat{w}_i$, $(i = 1, \ldots, a-1)$ kombinieren läßt. Daraus folgt $\dim(\widehat{C}) = a + b - 1$ und wegen $C \cong \widehat{C}$ folgt:

$$\dim(C) = a + b - 1. \tag{3.24}$$

□

Für die weitere Diskussion müssen wir nun die Fälle $C := C^a + C^b$ behandeln, bei denen einer der beiden Summanden ein Mehrfachcode des zweiten Elementarcodes ist.
Bei dem folgenden **zweiten Fall** sind a und b beide ungerade und es werden nacheinander die beiden Unterfälle bewiesen, in denen C^b, bzw. C^a der Mehrfachcode des zweiten Elementarcodes ist.

Lemma 3.7
Sei $2 < a < b$ mit $ggT(a, b) = 1$ und $N = a \cdot b$. a und b seien beide **ungerade**. *Sei nun C^a der a-malige Mehrfachcode des ersten Elementarcodes $\mathcal{C}_{1/b}$ mit $Aut(C^a) = \mathfrak{S}_a \wr \mathfrak{S}_b$, C^b der b-malige Mehrfachcode des zweiten Elementarcodes $\mathcal{C}_{2/a}$ mit $Aut(C^b) = \mathfrak{S}_b \wr \mathfrak{S}_a$ und es sei $C := C^a + C^b$. Dann gilt:*

$$Aut(C) = \mathfrak{S}_a \times \mathfrak{S}_b \text{ und } C \text{ ist ein } [N, a + b - 1, a]\text{-Code.} \tag{3.25}$$

Beweis. Der Code C^a wird von b Vektoren $v_1, \ldots, v_b \in \mathbb{F}_2^N$ erzeugt, wobei die v_j durch zyklische Verschiebung aus einander hervorgehen. Da $N = a \cdot b$, können wir diese Vektoren auch als Matrizen mit a Zeilen und b Spalten schreiben, also als Elemente aus $M(a, b, \mathbb{F}_2)$. Das sieht dann folgendermaßen aus:

$$v_1 = \begin{pmatrix} 100\ldots0 \\ 100\ldots0 \\ \vdots \\ 100\ldots0 \end{pmatrix}, v_2 = \begin{pmatrix} 010\ldots0 \\ 010\ldots0 \\ \vdots \\ 010\ldots0 \end{pmatrix}, \ldots, v_b = \begin{pmatrix} 00\ldots01 \\ 00\ldots01 \\ \vdots \\ 00\ldots01 \end{pmatrix}. \tag{3.26}$$

Der Code C^b wird von $a - 1$ Vektoren $w_1, \ldots, w_{a-1} \in \mathbb{F}_2^N$ erzeugt, wobei die w_i durch zyklische Verschiebung aus einander hervorgehen. Nach Konstruktion hat jeder der $a - 1$ erzeugenden Vektoren w_i genau $2 \cdot b$ Einsen, gefolgt von jeweils $a - 2$ Nullen, also z.B.

$$w_1 = (\overbrace{1,1,0,\ldots,0}^{a\ Positionen},1,1,0,\ldots,0,\ldots\ldots,1,1,0,\ldots,0,\overbrace{1,1,0,\ldots,0}^{a\ Positionen}). \tag{3.27}$$
$$\underbrace{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad}_{N=a\cdot b\ Positionen}$$

Damit die Erzeugungsvektoren auch dieses Mal nach einem bestimmten Muster in das gleiche Matrix-Schema passen, ersetzen wir den zyklischen Code C^b durch den dazu isomorphen quasi-zyklischen Code $\widehat{C}^b$, der von folgenden $a-1$ Vektoren $\widehat{w}_1, \ldots, \widehat{w}_{a-1} \in \mathbb{F}_2^N$ erzeugt wird:

$$\widehat{w}_1 = (\overbrace{1,1,1,\ldots,1}^{b\ Positionen}, \overbrace{1,1,1,\ldots,1}^{b\ Positionen}, 0,0,0,\ldots,0,\ldots\ldots,\overbrace{0,0,0,\ldots,0}^{b\ Positionen}),$$
$$N=a\cdot b\ \ Positionen$$

$$\widehat{w}_2 = (\overbrace{0,0,0,\ldots,0}^{b\ Positionen}, \overbrace{1,1,1,\ldots,1}^{b\ Positionen}, \overbrace{1,1,1,\ldots,1}^{b\ Positionen}, 0,0,0,\ldots,0,\ldots\ldots,\overbrace{0,0,0,\ldots,0}^{b\ Positionen}),$$
$$N=a\cdot b\ \ Positionen$$

$$\ldots\ldots\ldots$$

$$\widehat{w}_{a-1} = (\overbrace{0,0,0,\ldots,0}^{b\ Positionen},\ldots\ldots,0,0,0,\ldots,0,\overbrace{1,1,1,\ldots,1}^{b\ Positionen},\overbrace{1,1,1,\ldots,1}^{b\ Positionen}).$$
$$N=a\cdot b\ \ Positionen$$

Jetzt werden wir diese Vektoren ebenfalls als Matrizen mit a Zeilen und b Spalten schreiben, also als Elemente aus $M(a,b,\mathbb{F}_2)$. Das sieht dann folgendermaßen aus:

$$\widehat{w}_1 = \begin{pmatrix} 111\ldots1 \\ 111\ldots1 \\ 000\ldots0 \\ \vdots \\ 000\ldots0 \end{pmatrix}, \widehat{w}_2 = \begin{pmatrix} 000\ldots0 \\ 111\ldots1 \\ 111\ldots1 \\ \vdots \\ 000\ldots0 \end{pmatrix}, \ldots, \widehat{w}_{a-1} = \begin{pmatrix} 000\ldots0 \\ 000\ldots0 \\ \vdots \\ 111\ldots1 \\ 111\ldots1 \end{pmatrix}. \tag{3.28}$$

Wir wollen nun zunächst zeigen, daß für $\widehat{C} := C^a + \widehat{C}^b$ gilt: $Aut(\widehat{C}) = \mathfrak{S}_a \times \mathfrak{S}_b$.

$\mathfrak{S}_a$ vertauscht die Zeilen. $\mathfrak{S}_b$ vertauscht die Spalten. Dazu genügt es, einzusehen, daß jeder Automorphismus Zeilen und Spalten jeweils als ganzes vertauscht. Dies folgt, wenn wir zeigen, daß $v_1, \ldots, v_b$ genau die b Codewörter des Gewichts a sind und die Linearkombinationen der $\widehat{w}_1, \ldots, \widehat{w}_a$ genau die $\binom{a}{2}$ Codewörter des Gewichts b sind.
Das ist ähnlich elementar, wie im Beweis von Satz 3.6.
Den Isomorphismus

$$\sigma : C^b \longrightarrow \widehat{C}^b,\ \sigma : w_i \mapsto \widehat{w}_i$$

konstruieren wir sinngemäß, wie im Beweis von Satz 3.6. Somit haben wir gezeigt:

$$\widehat{C} = \sigma(C) = \sigma(C^a + C^b) = \sigma(C^a) + \sigma(C^b) = C^a + \widehat{C}^b \text{ und es gilt: } Aut(\widehat{C}) = \mathfrak{S}_a \times \mathfrak{S}_b.$$

Wegen $\widehat{C} \cong C$ folgt dann: $Aut(C) = Aut(\widehat{C}) = \mathfrak{S}_a \times \mathfrak{S}_b$.

Abschließend müssen wir noch die Aussagen zur Dimension und Minimaldistanz des Codes C zeigen:
Es gilt $md(C^a) = a$ und $md(C^b) = 2 \cdot b$ nach Konstruktion. Da $a < b$ nach Voraussetzung und wegen $C^a \leq C$ gilt $md(C) = a$. Codewörter mit kleinerer Minimaldistanz als a kann

es wegen der Konstruktion des Codes C nicht geben.

Wenn wir uns noch einmal die obigen Matrizen der Erzeugungsvektoren der v_j und $\widehat{w}_i$ ansehen, erkennen wir, daß sie linear unabhängig sind. Wegen $\dim(\widehat{C}^b) = a - 1$ folgt $\dim(\widehat{C}) = a + b - 1$ und wegen $C \cong \widehat{C}$ folgt dann:

$$\dim(C) = a + b - 1. \tag{3.29}$$

□

Lemma 3.8
Sei $2 < a < b$ mit $ggT(a, b) = 1$ und $N = a \cdot b$. a und b seien beide **ungerade**. *Sei nun C^a der a-malige Mehrfachcode des zweiten Elementarcodes $\mathcal{C}_{2/b}$ mit $Aut(C^a) = \mathfrak{S}_a \wr \mathfrak{S}_b$, C^b der b-malige Mehrfachcode des ersten Elementarcodes $\mathcal{C}_{1/a}$ mit $Aut(C^b) = \mathfrak{S}_b \wr \mathfrak{S}_a$ und es sei $C := C^a + C^b$. Dann gilt:*

$$Aut(C) = \mathfrak{S}_a \times \mathfrak{S}_b \text{ und } C \text{ ist ein } [N, a + b - 1, a]\text{-Code.} \tag{3.30}$$

Beweis. Der Beweis geht sinngemäß so, wie der Beweis zum obigen Lemma 3.7. Auch hier sind die Matrizen der Erzeugungsvektoren der v_j und $\widehat{w}_i$ linear unabhängig und wegen $\dim(C^a) = b - 1$ folgt $\dim(\widehat{C}) = a + b - 1$ und wegen $C \cong \widehat{C}$ folgt dann:

$$\dim(C) = a + b - 1. \tag{3.31}$$

Nun zeigen wir noch, daß auch hier $md(C) = a$ gilt:
Dazu summieren wir zunächst sämtliche $\widehat{w}_i$ und erhalten eine Matrix, die nur aus Einsen besteht. Anschließend addieren wir noch $v_2, v_4, \ldots, v_{b-1}$ und es bleibt nur die erste Spalte mit a Einsen übrig, der Rest sind Nullen. Codewörter mit kleinerer Minimaldistanz als a kann es wegen der Konstruktion des Codes C nicht geben.

□

Wir kommen nun zum zweiten Code, einem $[N, a+b-2]$-Code mit der Automorphismengruppe $\mathfrak{S}_a \times \mathfrak{S}_b$:
Bei dem folgenden **dritten Fall** ist $b > 4$ gerade und es werden nacheinander die beiden Unterfälle bewiesen, in denen C^a, bzw. C^b der Mehrfachcode des zweiten Elementarcodes ist.

Lemma 3.9
Sei $2 < a < b$ mit $ggT(a, b) = 1$ und $N = a \cdot b$. Es sei $b > 4$ **gerade**. *Sei nun C^a der a-malige Mehrfachcode des zweiten Elementarcodes $\mathcal{C}_{2/b}$ mit $Aut(C^a) = \mathfrak{S}_a \wr \mathfrak{S}_b$, C^b der b-malige Mehrfachcode des ersten Elementarcodes $\mathcal{C}_{1/a}$ mit $Aut(C^b) = \mathfrak{S}_b \wr \mathfrak{S}_a$ und es sei $C := C^a + C^b$. Dann gilt:*

$$Aut(C) = \mathfrak{S}_a \times \mathfrak{S}_b \text{ und } C \text{ ist ein } [N, a + b - 2, min(2a, b)]\text{-Code.} \tag{3.32}$$

Beweis. Der Code C^a wird von $b-1$ Vektoren $v_1, \ldots, v_{b-1} \in \mathbb{F}_2^N$ erzeugt, wobei die v_j durch zyklische Verschiebung aus einander hervorgehen. Da $N = a \cdot b$, können wir diese Vektoren auch als Matrizen mit a Zeilen und b Spalten schreiben, also als Elemente aus $M(a, b, \mathbb{F}_2)$. Das sieht dann folgendermaßen aus:

$$v_1 = \begin{pmatrix} 110\ldots0 \\ 110\ldots0 \\ \vdots \\ 110\ldots0 \end{pmatrix}, v_2 = \begin{pmatrix} 011\ldots0 \\ 011\ldots0 \\ \vdots \\ 011\ldots0 \end{pmatrix}, \ldots, v_{b-1} = \begin{pmatrix} 00\ldots11 \\ 00\ldots11 \\ \vdots \\ 00\ldots11 \end{pmatrix}. \tag{3.33}$$

Der Code C^b wird von a Vektoren $w_1, \ldots, w_a \in \mathbb{F}_2^N$ erzeugt, wobei die w_i durch zyklische Verschiebung aus einander hervorgehen. Nach Konstruktion hat jeder der a erzeugenden Vektoren w_i genau b Einsen, gefolgt von jeweils $a-1$ Nullen. Die Vektoren w_i, sowie die Vektoren $\widehat{w}_i$ des zu C^b isomorphen Codes $\widehat{C}^b$ sind bereits oben im Satz 3.6 dargestellt worden.
Wir wollen nun zunächst zeigen, daß für $\widehat{C} := C^a + \widehat{C}^b$ gilt: $Aut(\widehat{C}) = \mathfrak{S}_a \times \mathfrak{S}_b$.

$\mathfrak{S}_a$ vertauscht die Zeilen. $\mathfrak{S}_b$ vertauscht die Spalten. Dazu genügt es, einzusehen, daß jeder Automorphismus Zeilen und Spalten jeweils als ganzes vertauscht. Dies folgt, wenn wir zeigen, daß die Linearkombinationen der $v_1, \ldots, v_{b-1}$ genau die $\binom{b}{2}$ Codewörter des Gewichts $2a$ sind und $\widehat{w}_1, \ldots, \widehat{w}_a$ genau die a Codewörter des Gewichts b sind.
Das ist ähnlich elementar, wie im Beweis von Satz 3.6.
Den Isomorphismus

$$\sigma : C^b \longrightarrow \widehat{C}^b,\ \sigma : w_i \mapsto \widehat{w}_i$$

konstruieren wir sinngemäß, wie im Beweis von Satz 3.6. Somit haben wir gezeigt:

$\widehat{C} = \sigma(C) = \sigma(C^a + C^b) = \sigma(C^a) + \sigma(C^b) = C^a + \widehat{C}^b$ und es gilt: $Aut(\widehat{C}) = \mathfrak{S}_a \times \mathfrak{S}_b$.

Wegen $\widehat{C} \cong C$ folgt dann: $Aut(C) = Aut(\widehat{C}) = \mathfrak{S}_a \times \mathfrak{S}_b$.

Abschließend müssen wir noch die Aussagen zur Dimension und Minimaldistanz des Codes C zeigen:

Es gilt $md(C^a) = 2a$ und $md(C^b) = b$ nach Konstruktion. Also gilt $md(C) = min(2a, b)$. Codewörter mit kleinerer Minimaldistanz kann es wegen der Konstruktion des Codes C nicht geben.
Wenn wir uns noch einmal die obigen Matrizen der Erzeugungsvektoren der v_j und $\widehat{w}_i$ ansehen, erkennen wir, daß sie linear abhängig sind:
Zunächst summieren wir die Vektoren $v_1, v_3, \ldots, v_{b-1}$ und erhalten so eine Matrix, die nur aus Einsen besteht. Anschließend addieren wir noch $\widehat{w}_1, \widehat{w}_2, \ldots, \widehat{w}_{a-1}$ und es bleibt nur die letzte Zeile mit b Einsen übrig, der Rest sind Nullen. Das genau ist der Vektor $\widehat{w}_a$. Aus diesem Grund und wegen $\dim(\widehat{C}^a) = b-1$ folgt $\dim(\widehat{C}) = a+b-2$ und wegen $C \cong \widehat{C}$ folgt dann:

$$\dim(C) = a + b - 2. \tag{3.34}$$

□

Lemma 3.10
Sei $2 < a < b$ mit $ggT(a,b) = 1$ und $N = a \cdot b$. Es sei $b > 4$ **gerade**. *Sei nun*
C^a der a-malige Mehrfachcode des ersten Elementarcodes $\mathcal{C}_{1/b}$ mit $Aut(C^a) = \mathfrak{S}_a \wr \mathfrak{S}_b$,
C^b der b-malige Mehrfachcode des zweiten Elementarcodes $\mathcal{C}_{2/a}$ mit $Aut(C^b) = \mathfrak{S}_b \wr \mathfrak{S}_a$
und es sei $C := C^a + C^b$. Dann gilt:

$$Aut(C) = \mathfrak{S}_a \times \mathfrak{S}_b \text{ und } C \text{ ist ein } [N, a+b-1, a]\text{-Code.} \tag{3.35}$$

Beweis. Der Beweis geht genau so, wie der Beweis zum Lemma 3.7 weiter oben (zweiter Fall). □

Wir sind noch beim zweiten Code, einem $[N, a+b-2]$-Code mit der Automorphismengruppe $\mathfrak{S}_a \times \mathfrak{S}_b$:
Bei dem folgenden **Fall 3a** ist $a > 4$ gerade und es werden nacheinander die beiden Unterfälle bewiesen, in denen C^a, bzw. C^b der Mehrfachcode des zweiten Elementarcodes ist.

Lemma 3.11
Sei $2 < a < b$ mit $ggT(a,b) = 1$ und $N = a \cdot b$. Es sei $a > 4$ **gerade**. *Sei nun*
C^a der a-malige Mehrfachcode des ersten Elementarcodes $\mathcal{C}_{1/b}$ mit $Aut(C^a) = \mathfrak{S}_a \wr \mathfrak{S}_b$,
C^b der b-malige Mehrfachcode des zweiten Elementarcodes $\mathcal{C}_{2/a}$ mit $Aut(C^b) = \mathfrak{S}_b \wr \mathfrak{S}_a$
und es sei $C := C^a + C^b$. Dann gilt:

$$Aut(C) = \mathfrak{S}_a \times \mathfrak{S}_b \text{ und } C \text{ ist ein } [N, a+b-2, a]\text{-Code.} \tag{3.36}$$

Beweis. Der Code C^a wird von b Vektoren $v_1, \ldots, v_b \in \mathbb{F}_2^N$ erzeugt, wobei die v_j durch zyklische Verschiebung aus einander hervorgehen. Da $N = a \cdot b$, können wir diese Vektoren auch als Matrizen mit a Zeilen und b Spalten schreiben, also als Elemente aus $M(a, b, \mathbb{F}_2)$. Das haben wir bereits im Beweis zu Satz 3.6 gezeigt.
Der Code C^b wird von a Vektoren $w_1, \ldots, w_{a-1} \in \mathbb{F}_2^N$ erzeugt, wobei die w_i durch zyklische Verschiebung aus einander hervorgehen. Nach Konstruktion hat jeder der $a-1$ erzeugenden Vektoren w_i genau $2b$ Einsen, gefolgt von jeweils $a-2$ Nullen. Die Vektoren w_i, sowie die Vektoren $\widehat{w}_i$ des zu C^b isomorphen Codes $\widehat{C}^b$ sind bereits oben im Lemma 3.7 dargestellt worden.
Wir wollen nun zunächst zeigen, daß für $\widehat{C} := C^a + \widehat{C}^b$ gilt: $Aut(\widehat{C}) = \mathfrak{S}_a \times \mathfrak{S}_b$.

$\mathfrak{S}_a$ vertauscht die Zeilen. $\mathfrak{S}_b$ vertauscht die Spalten. Dazu genügt es, einzusehen, daß jeder Automorphismus Zeilen und Spalten jeweils als ganzes vertauscht. Dies folgt, wenn wir zeigen, daß die $v_1, \ldots, v_b$ genau die b Codewörter des Gewichts a sind und die Linearkombinationen der $\widehat{w}_1, \ldots, \widehat{w}_a$ genau die $\binom{a}{2}$ Codewörter des Gewichts $2b$ sind.
Das ist ähnlich elementar, wie im Beweis von Satz 3.6.
Den Isomorphismus

$$\sigma : C^b \longrightarrow \widehat{C}^b,\ \sigma : w_i \mapsto \widehat{w}_i$$

konstruieren wir sinngemäß, wie im Beweis von Satz 3.6. Somit haben wir gezeigt:

$\widehat{C} = \sigma(C) = \sigma(C^a + C^b) = \sigma(C^a) + \sigma(C^b) = C^a + \widehat{C}^b$ und es gilt: $Aut(\widehat{C}) = \mathfrak{S}_a \times \mathfrak{S}_b$.

Wegen $\widehat{C} \cong C$ folgt dann: $Aut(C) = Aut(\widehat{C}) = \mathfrak{S}_a \times \mathfrak{S}_b$.

Abschließend müssen wir noch die Aussagen zur Dimension und Minimaldistanz des Codes C zeigen:

Es gilt $md(C^a) = a$ und $md(C^b) = 2b$ nach Konstruktion. Wegen $a < b$ nach Voraussetzung folgt $a < 2b$. Also gilt $md(C) = a$. Codewörter mit kleinerer Minimaldistanz kann es wegen der Konstruktion des Codes C nicht geben.
Wenn wir uns noch einmal die obigen Matrizen der Erzeugungsvektoren der v_j und $\widehat{w}_i$ ansehen, erkennen wir, daß sie linear abhängig sind:
Zunächst summieren wir die Vektoren $v_1, v_3, \ldots, v_b$ und erhalten so eine Matrix, die nur aus Einsen besteht. Anschließend addieren wir noch $\widehat{w}_3, \widehat{w}_5, \ldots, \widehat{w}_{a-1}$ und es bleiben nur die ersten beiden Zeile mit je b Einsen übrig, der Rest sind Nullen. Das genau ist der Vektor $\widehat{w}_1$. Aus diesem Grund und wegen $\dim(\widehat{C}^b) = a - 1$ folgt $\dim(\widehat{C}) = a + b - 2$ und wegen $C \cong \widehat{C}$ folgt dann:

$$\dim(C) = a + b - 2. \tag{3.37}$$

□

Lemma 3.12
Sei $2 < a < b$ mit $ggT(a, b) = 1$ und $N = a \cdot b$. Es sei $a > 4$ **gerade**. *Sei nun*
C^a der a-malige Mehrfachcode des zweiten Elementarcodes $\mathcal{C}_{2/b}$ mit $Aut(C^a) = \mathfrak{S}_a \wr \mathfrak{S}_b$,
C^b der b-malige Mehrfachcode des ersten Elementarcodes $\mathcal{C}_{1/a}$ mit $Aut(C^b) = \mathfrak{S}_b \wr \mathfrak{S}_a$ und es sei $C := C^a + C^b$. Dann gilt:

$$Aut(C) = \mathfrak{S}_a \times \mathfrak{S}_b \text{ und } C \text{ ist ein } [N, a + b - 1, a]\text{-Code.} \tag{3.38}$$

Beweis. Der Beweis geht genau so, wie der Beweis zum Lemma 3.7 weiter oben (zweiter Fall).

□

Wir sind noch beim zweiten Code, einem $[N, a + b - 2]$-Code mit der Automorphismengruppe $\mathfrak{S}_a \times \mathfrak{S}_b$:
Bei dem folgenden **vierten Fall** sind beide Summanden Mehrfachcodes aus dem zweiten Elementarcode.

Lemma 3.13
Sei $2 < a < b$ mit $ggT(a, b) = 1$ und $N = a \cdot b$. Es sei $a \neq 4$. Sei nun
C^a der a-malige Mehrfachcode des zweiten Elementarcodes $\mathcal{C}_{2/b}$ mit $Aut(C^a) = \mathfrak{S}_a \wr \mathfrak{S}_b$,
C^b der b-malige Mehrfachcode des zweiten Elementarcodes $\mathcal{C}_{2/a}$ mit $Aut(C^b) = \mathfrak{S}_b \wr \mathfrak{S}_a$ und es sei $C := C^a + C^b$. Dann gilt:

$$Aut(C) = \mathfrak{S}_a \times \mathfrak{S}_b \text{ und } C \text{ ist ein } [N, a + b - 2, 2a]\text{-Code.} \tag{3.39}$$

Beweis. Der Code C^a wird von $b-1$ Vektoren $v_1, \ldots, v_{b-1} \in \mathbb{F}_2^N$ erzeugt, wobei die v_j durch zyklische Verschiebung aus einander hervorgehen. Da $N = a \cdot b$, können wir diese Vektoren auch als Matrizen mit a Zeilen und b Spalten schreiben, also als Elemente aus $M(a, b, \mathbb{F}_2)$. Das haben wir bereits im Beweis zu Lemma 3.9 gezeigt.
Der Code C^b wird von $a-1$ Vektoren $w_1, \ldots, w_{a-1} \in \mathbb{F}_2^N$ erzeugt, wobei die w_i durch zyklische Verschiebung aus einander hervorgehen. Nach Konstruktion hat jeder der $a-1$ erzeugenden Vektoren w_i genau $2b$ Einsen, gefolgt von jeweils $a-2$ Nullen. Die Vektoren w_i, sowie die Vektoren $\widehat{w}_i$ des zu C^b isomorphen Codes $\widehat{C}^b$ sind bereits oben im Lemma 3.7 dargestellt worden.
Wir wollen nun zunächst zeigen, daß für $\widehat{C} := C^a + \widehat{C}^b$ gilt: $Aut(\widehat{C}) = \mathfrak{S}_a \times \mathfrak{S}_b$.

$\mathfrak{S}_a$ vertauscht die Zeilen. $\mathfrak{S}_b$ vertauscht die Spalten. Dazu genügt es, einzusehen, daß jeder Automorphismus Zeilen und Spalten jeweils als ganzes vertauscht. Dies folgt, wenn wir zeigen, daß die Linearkombinationen der $v_1, \ldots, v_{b-1}$ genau die $\binom{b}{2}$ Codewörter des Gewichts $2a$ sind und die Linearkombinationen der $\widehat{w}_1, \ldots, \widehat{w}_a$ genau die $\binom{a}{2}$ Codewörter des Gewichts $2b$ sind.
Das ist ähnlich elementar, wie im Beweis von Satz 3.6.
Den Isomorphismus

$$\sigma : C^b \longrightarrow \widehat{C}^b,\ \sigma : w_i \mapsto \widehat{w}_i$$

konstruieren wir sinngemäß, wie im Beweis von Satz 3.6. Somit haben wir gezeigt:

$$\widehat{C} = \sigma(C) = \sigma(C^a + C^b) = \sigma(C^a) + \sigma(C^b) = C^a + \widehat{C}^b \text{ und es gilt: } Aut(\widehat{C}) = \mathfrak{S}_a \times \mathfrak{S}_b.$$

Wegen $\widehat{C} \cong C$ folgt dann: $Aut(C) = Aut(\widehat{C}) = \mathfrak{S}_a \times \mathfrak{S}_b$.

Abschließend müssen wir noch die Aussagen zur Dimension und Minimaldistanz des Codes C zeigen:

Es gilt $md(C^a) = 2a$ und $md(C^b) = 2b$ nach Konstruktion. Wegen $a < b$ nach Voraussetzung folgt $2a < 2b$. Also gilt $md(C) = 2a$. Codewörter mit kleinerer Minimaldistanz kann es wegen der Konstruktion des Codes C nicht geben.
Wenn wir uns noch einmal die obigen Matrizen der Erzeugungsvektoren der v_j und $\widehat{w}_i$ ansehen, erkennen wir, daß sie linear unabhängig sind.
Aus diesem Grund und wegen $\dim(\widehat{C}^b) = a-1$, sowie $\dim(\widehat{C}^a) = b-1$ folgt
$\dim(\widehat{C}) = a + b - 2$ und wegen $C \cong \widehat{C}$ folgt dann:

$$\dim(C) = a + b - 2.$$

□

Damit ist der Satz 3.3 bewiesen.

Zum Abschluß benötigen wir noch den folgenden angekündigten interessanten Satz. Da es sich hierbei um Codelängen handelt, die durch 4 teilbar sind, haben wir in der Nomenklatur das allgemeine b wieder durch m ersetzt – so, wie im Abschnitt 1.2.2. Es heißt also nun für den Rest dieses Abschnitts $N = 4 \cdot m$, statt – wie bisher allgemein $N = a \cdot b$.

Satz 3.14
Sei $N \leqq 100$. Sei ferner $N = 4 \cdot m$ eine Faktorenzerlegung mit $N, m \in \mathbb{N}$, wobei m ungerade ist und nicht kleiner als 5[4] sein darf.
Dann gelten folgende Aussagen:
Es gibt weitere 2 zyklische Codes der Länge N mit der Automorphismengruppe

$$\underbrace{(\mathfrak{S}_2 \times \cdots \times \mathfrak{S}_2)}_{(2m)-mal} \rtimes (\mathfrak{S}_m \times \mathfrak{S}_3), \tag{1.25}$$

oder einfacher geschrieben als vermindertes Kranzprodukt:

$$(\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_m))/\mathfrak{S}_2^m \tag{1.28}$$

nämlich:

1. *einen $[N, m+2, 4]$-Code*
2. *und den dazu dualen $[N, N-m-2, 4]$-Code.*

Bemerkung 3.15
Diese Automorphismengruppe ist eine minimale Obergruppe von $\mathfrak{S}_4 \times \mathfrak{S}_m$ und sie ist Untergruppe von $\mathfrak{S}_4 \wr \mathfrak{S}_m$.
Die Verwandschaft zu $\mathfrak{S}_4 \wr \mathfrak{S}_m$ sieht man, wenn man die **Magma**-Kompositionslisten vergleicht. Man kann diese Gruppe daher auch so darstellen:

$$(\mathfrak{K}_4 \wr \mathfrak{S}_m) \rtimes \mathfrak{S}_3. \tag{1.29}$$

Es besteht ein direkter Zusammenhang zur Automorphismengruppe $\mathfrak{S}_4 \times \mathfrak{S}_m$:
Wie wir weiter oben gesehen haben, existieren zur Automorphismengruppe $\mathfrak{S}_a \times \mathfrak{S}_b$ für $a \neq 2, 4$ stets insgesamt 4 Codes (2 + 2 duale), für $a = 4$ aber nur 2 (1 + 1 dual) Codes. Es sind genau diese beiden fehlenden Codes, welche die hier diskutierte minimale Obergruppe als Automorphismengruppe haben. Hier ist die Konstruktion des einen[5] Codes:

Dabei ist $C4$ der $[N, 3, \frac{N}{2}]$-Code mit der Automorphismengruppe $\mathfrak{S}_m \wr \mathfrak{S}_4$, während $C8$ und $C10$ die beiden Codes mit der Automorphismengruppe $\mathfrak{S}_4 \wr \mathfrak{S}_m$ sind (Obergruppe von $(\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_m))/\mathfrak{S}_2^m$).

[4] Die Einschränkung $m \geq 5$ hängt mit der Forderung zusammen, daß die Automorphismengruppe nicht auflösbar sein soll. Geht man von dieser Forderung ab, so kann man diese Voraussetzung durch $m \geq 3$ ersetzen.

[5] mit dem dazu dualen Code sind es dann die beiden fehlenden Codes.

$C8$ ist der $[N, m-1, 8]$-Code, $C10$ ist der $[N, m, 4]$-Code; siehe Bsp. 1.32 im Abschnitt 1.2.2, $m = 5$, $N = 20$, mit Cx, x = Lfd.Nr. aus der Liste:

$$\mathcal{C} = C4 + C8 = C4 + C10 = C14. \tag{3.40}$$

Falls es eine Spezialgruppe gibt (z.B. $PSL(r, 2)$, oder $M23$), die auf einer Menge Ω der Kardinalität m transitiv operiert, so existieren sinngemäß auch noch

$$\mathfrak{S}_4 \times Spezialgruppe_m \quad und \tag{1.26}$$

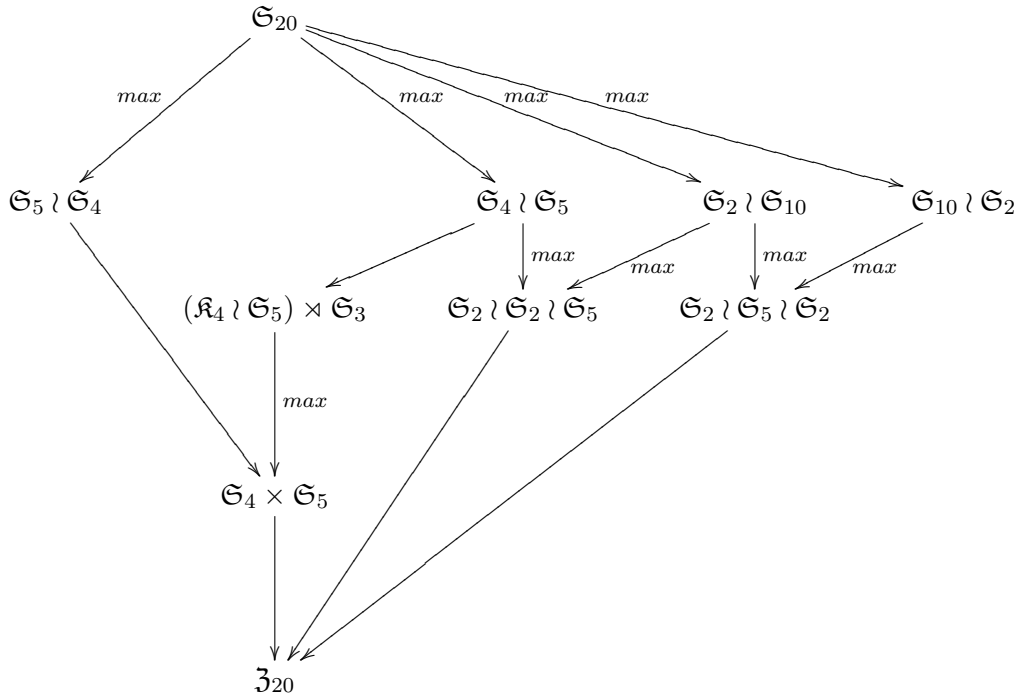
$$(\mathfrak{K}_4 \wr Spezialgruppe_m) \rtimes \mathfrak{S}_3. \tag{1.31}$$

Wegen der Konstruktion der Automorphismengruppe als semidirektes Produkt muß noch ein Homomorphismus angegeben werden. Siehe dazu auch das Kapitel 5. Bei der Darstellung als vermindertes Kranzprodukt ist das nicht erforderlich.

Beweis. Sowohl die Codes, wie auch die Automorphismengruppen wurden durch **Magma**-Berechnungen exemplarisch und präzise für folgende Codelängen $N \leqq 100$ nachgewiesen: N = 20, 28, 36, 44, 52, 60, 68, 76, 92 und 100. (s. Tabellenwerk im Anhang). Den Fall $N = 84$ behandeln wir gesondert am Ende von Kapitel 9 im Abschnitt 9.1. □

Vermutung 3.16
Die Aussagen von Satz 3.14 gelten auch für $N \geq 100$.

Als Beispiel haben wir anschließend die Automorphismengruppe $(\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_5))/\mathfrak{S}_2^5 \cong (\mathfrak{K}_4 \wr \mathfrak{S}_5) \rtimes \mathfrak{S}_3$ zusammen mit den übrigen Automorphismengruppen zur Codelänge $N = 20$ in einem Hasse-Diagramm als Teilverband des Untergruppenverbands von $\mathfrak{S}_{20}$ dargestellt.



Die 8 Automorphismengruppen der zyklischen Codes zur Codelänge $N = 20$ im Untergruppenverband von $\mathfrak{S}_{20}$

Man beachte:
$(\mathfrak{K}_4 \wr \mathfrak{S}_5) \rtimes \mathfrak{S}_3 \cong (\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_5))/\mathfrak{S}_2^5$
$\mathfrak{S}_4 \times \mathfrak{S}_5 = \mathfrak{S}_4 \wr \mathfrak{S}_5 \cap \mathfrak{S}_5 \wr \mathfrak{S}_4$

> **Legende:** *max* an einer Verbandslinie bedeutet:
> Die jeweils untere Gruppe ist maximale Untergruppe der oberen Gruppe.
> $G_i \longleftarrow G_j$ bedeutet: $G_i < G_j$

Anhand eines kleinen Beispiels für $N = 12$ wollen wir zeigen, weshalb bei $a = 4$ diese besondere Automorphismengruppe existiert. Dabei lassen wir zugunsten der Übersichtlichkeit $b < a < 5$ zu:

Beispiel 3.17
Dazu sehen wir die Erzeugungsvektoren der Codes an, die als Summanden involviert sind. Wir benutzen wieder die Matrixschreibweise, wie in der Beweisfolge zum Satz 3.3.
Es ist also $a = 4$, $b = 3$ und C^4 der 3-malige Mehrfachcode des zweiten Elementarcodes $\mathcal{C}_{2/4}$ mit $Aut(C^4) = \mathfrak{S}_3 \wr \mathfrak{S}_4$,
C^3 der 4-malige Mehrfachcode des ersten Elementarcodes $\mathcal{C}_{1/3}$ mit $Aut(C^3) = \mathfrak{S}_4 \wr \mathfrak{S}_3$ und es sei $C := C^4 + C^3$. Dann gilt:

Der Code C^4 wird von 3 Vektoren $v_1, v_2, v_3 \in \mathbb{F}_2^{12}$ erzeugt, wobei die v_j durch zyklische Verschiebung aus einander hervorgehen. Das sieht dann folgendermaßen aus:

$$v_1 = \begin{pmatrix} 1100 \\ 1100 \\ 1100 \end{pmatrix}, v_2 = \begin{pmatrix} 0110 \\ 0110 \\ 0110 \end{pmatrix}, v_3 = \begin{pmatrix} 0011 \\ 0011 \\ 0011 \end{pmatrix}. \tag{3.41}$$

Der Code C^3 wird von 3 Vektoren $w_1, w_2, w_3 \in \mathbb{F}_{12}^N$ erzeugt, wobei die w_i durch zyklische Verschiebung aus einander hervorgehen. Nach Konstruktion hat jeder der 3 erzeugenden Vektoren w_i genau 4 Einsen, gefolgt von jeweils 3 Nullen. Auch hier erzeugen wir wieder einen zu C^3 isomorphen quasizyklischen Code $\widehat{C}^3$, dessen Erzeugungsvektoren $\widehat{w}_i$ folgendermaßen aussehen:

$$\widehat{w}_1 = \begin{pmatrix} 1111 \\ 0000 \\ 0000 \end{pmatrix}, \widehat{w}_2 = \begin{pmatrix} 0000 \\ 1111 \\ 0000 \end{pmatrix}, \widehat{w}_3 = \begin{pmatrix} 0000 \\ 0000 \\ 1111 \end{pmatrix}. \tag{3.42}$$

Anders, als in der Beweiskette zum Satz 3.3, wo Codevektoren mit dem Gewicht $2b$ eines Erzeugungsvektors auch nur von einer Linearkombination dieser Erzeugungsvektoren des einen Codes gebildet werden konnten, finden wir hier jetzt eine Möglichkeit, Codevektoren mit einem solchen Gewicht zu erzeugen, bei denen die Erzeugungsvektoren beider Codes C^4 und C^3 kombiniert werden: So ergibt z.B. $v_2 + \widehat{w}_3$ den folgenden Codevektor c mit Gewicht $2b$:

$$c = \begin{pmatrix} 0110 \\ 0110 \\ 1001 \end{pmatrix}. \tag{3.43}$$

Dieses Beispiel zeigt, daß $Aut(C) \neq \mathfrak{S}_3 \times \mathfrak{S}_4$.
Ende des Beispiels

Da wir den obigen Satz 3.14 nur exemplarisch bewiesen haben, wollen wir abschließend noch einen allgemeinen Satz ergänzend dazu beweisen:

Satz 3.18
Sei $N = a \cdot b$ mit $2 \neq a < b$, sowie a und b teilerfremd. Dann gilt:

$$\mathfrak{S}_a \times \mathfrak{S}_b \leq Aut(D) \tag{3.44}$$

für alle zyklischen Codes $D = E + F$ der Länge N
mit $Aut(E) = \mathfrak{S}_a \wr \mathfrak{S}_b$ und $\dim(E2) < N/2$, sowie $Aut(F) = \mathfrak{S}_b \wr \mathfrak{S}_a$ und $\dim(F) < N/2$.

Beweis. Unter der Voraussetzung a, b teilerfremd gilt:

$$\mathfrak{S}_a \times \mathfrak{S}_b = (\mathfrak{S}_a \wr \mathfrak{S}_b) \cap (\mathfrak{S}_b \wr \mathfrak{S}_a). \tag{3.45}$$

Dies sieht man so:
Sei $\Omega := \{1, \ldots, a \cdot b = N\}$ die Menge der Elemente, auf denen $\mathfrak{S}_N$ operiert.
Wir bilden nun die Elemente von Ω auf ihre Restklassen modulo a und modulo b ab und ordnen die Elemente entsprechend zeilen- und spaltenweise an (Beispiel siehe Tabelle 3.1).

Bahn	$\mathcal{B}_1$	$\mathcal{B}_2$	$\mathcal{B}_3$	$\mathcal{B}_4$	$\mathcal{B}_5$
$\mathcal{C}_1$	1	7	13	4	10
$\mathcal{C}_2$	6	12	3	9	15
$\mathcal{C}_3$	11	2	8	14	5

Tabelle 3.1: Tabelle der Bahnen von $\mathfrak{S}_3 \times \mathfrak{S}_5$

Dabei ist

- $\mathcal{B}_i$ = die Restklasse von i mod b, $(i = 1, \ldots, b)$:
  Das ergibt insgesamt b Bahnen mit je a Elementen,
- $\mathcal{C}_j$ = die Restklasse von j mod a, $(j = 1, \ldots, a)$:
  Das ergibt insgesamt a Bahnen mit je b Elementen.

Eine Operation von $\mathfrak{S}_a \times \mathfrak{S}_b$ auf $N = a \cdot b$ Elementen $\{1, \ldots, a \cdot b\}$ ist folgendermaßen definiert:

$$(\sigma, \tau) \in \mathfrak{S}_a \times \mathfrak{S}_b, \quad \sigma \in \mathfrak{S}_a, \tau \in \mathfrak{S}_b. \tag{3.46}$$

und es operiert $\mathfrak{S}_a$ auf $\{\mathcal{C}_1, \ldots, \mathcal{C}_a\}$, sowie $\mathfrak{S}_b$ auf $\{\mathcal{B}_1, \ldots, \mathcal{B}_b\}$ wie folgt:

$$\sigma(\mathcal{C}_j) = \mathcal{C}_{\sigma(j)}, \quad \tau(\mathcal{B}_i) = \mathcal{B}_{\tau(i)}. \tag{3.47}$$

Nun sei:

$$c_{kt} \in \mathcal{C}_k \cap \mathcal{B}_t, \quad (k = 1, \ldots, a; \quad t = 1, \ldots, b). \tag{3.48}$$

c_{kt} ist eindeutig bestimmt, weil a und b teilerfremd sind.
Dabei gilt:

$$\sigma(c_{kt}) = c_{\sigma(k)t}, \quad \tau(c_{kt}) = c_{k\tau(t)} \tag{3.49}$$

und letztlich

$$(\sigma, \tau)c_{kt} = c_{\sigma(k)\tau(t)}. \tag{3.50}$$

Die zugehörigen Codes lassen sich als Summe von je zwei Codes der Länge N konstruieren, deren Automorphismengruppe zum einen $\mathfrak{S}_a \wr \mathfrak{S}_b$ und zum anderen $\mathfrak{S}_b \wr \mathfrak{S}_a$ ist (s. dazu auch Kap. 9). Als Permutationen, welche die Summe von je zweien dieser Codes invariant lassen, kommen nur diejenigen Permutationen $\varrho \in \mathfrak{S}_N$ infrage, für die gilt:

$$\varrho \in \mathfrak{S}_a \wr \mathfrak{S}_b \wedge \varrho \in \mathfrak{S}_b \wr \mathfrak{S}_a \Longrightarrow \varrho \in (\mathfrak{S}_a \wr \mathfrak{S}_b) \cap (\mathfrak{S}_b \wr \mathfrak{S}_a) = \mathfrak{S}_a \times \mathfrak{S}_b. \tag{3.51}$$

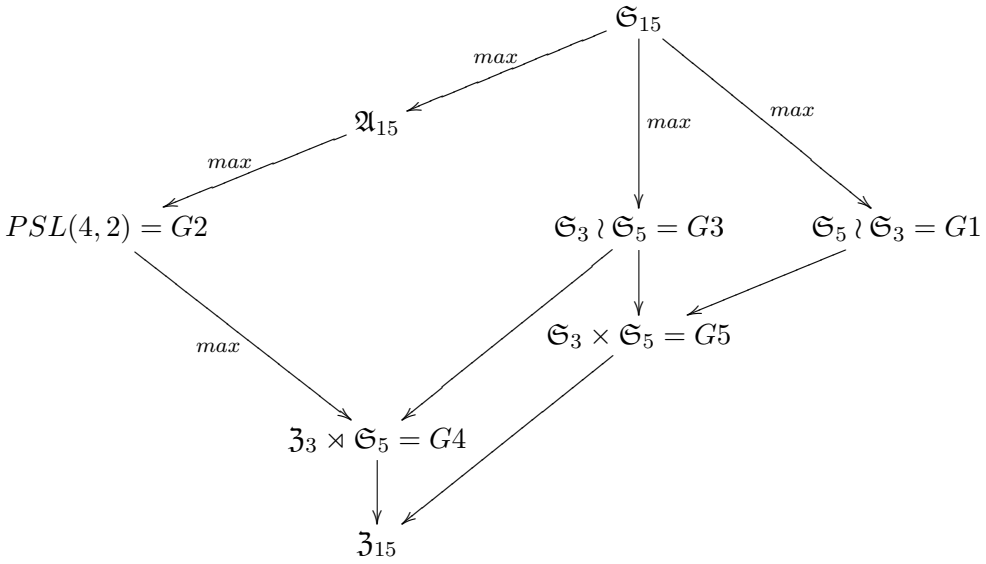
Damit ist gezeigt, daß

$$\mathfrak{S}_a \times \mathfrak{S}_b \leq Aut(D) \tag{3.52}$$

für alle zyklischen Codes $D = E + F$ der Länge N
mit $Aut(E) = \mathfrak{S}_a \wr \mathfrak{S}_b$ und $\dim(E2) < N/2$, sowie $Aut(F) = \mathfrak{S}_b \wr \mathfrak{S}_a$ und $\dim(F) < N/2$. □

Daß $Aut(C)$ eine echte Obergruppe von $\mathfrak{S}_a \times \mathfrak{S}_b$ sein kann, sahen wir im Satz 3.14.

Als Beispiel haben wir anschließend die Automorphismengruppe $\mathfrak{S}_3 \times \mathfrak{S}_5$ zusammen mit den übrigen Automorphismengruppen zur Codelänge $N = 15$ in einem Hasse-Diagramm als Teilverband des Untergruppenverbands von $\mathfrak{S}_{15}$ dargestellt.
Darüberhinaus haben wir für diese Automorphismengruppe $\mathfrak{S}_3 \times \mathfrak{S}_5$ die Bahnen der $\mathcal{B}_i$ und $\mathcal{C}_j$ in der obigen Tabelle 3.1 zum besseren Verständnis der Beweisführung zusammengestellt.



Die 5 Automorphismengruppen $G1, \ldots, G5$ zur Codelänge $N = 15$ im Untergruppenverband von $\mathfrak{S}_{15}$
Man beachte:
$G5 = G1 \cap G3$,
$G4 = G2 \cap G3$

> **Legende:** *max* an einer Verbandslinie bedeutet:
> Die jeweils untere Gruppe ist maximale Untergruppe der oberen Gruppe.
> $G_i \longleftarrow G_j$ bedeutet: $G_i < G_j$

Soweit die Erkenntnisse bezüglich der Zerlegung von N in 2 Faktoren.

3.2 Zerlegung der Codelänge in 3 Faktoren

Wir wollen jetzt die Erkenntnisse aus dem umfangreichen Listen- und Tabellenwerk bezüglich der Zerlegung von N in 3 Faktoren zusammenfassen:
Auch hier ist die Minimaldistanz des Codes eine Funktion des **äußeren Gruppenkranzes**, d.h., des ersten Faktors im dreifachen Kranzprodukt und die Dimension des Codes ist eine Funktion des **Kranz-Zentrums**, welches hier durch die letzten beiden Faktoren gebildet wird.

Die hier im Folgenden gemachten Aussagen sind für die angegebenen Codelängen anhand der identifizierten Automorphismengruppen und deren zugehörige Codes exemplarisch überprüft worden.

Beobachtung 3.19
Sei $N = a \cdot b \cdot c$ eine Faktorenzerlegung mit $N, a, b, c \in \mathbb{N}$, wobei a, b und c nicht alle gleichzeitig kleiner als 5 sein dürfen. Sei oBdA $a \leq b \leq c$.
Dann gelten folgende Aussagen:
In den folgenden Fallunterscheidungen werden wir Kranzprodukte der Form

$$\mathfrak{S}_x \wr \mathfrak{S}_y \wr \mathfrak{S}_z \tag{3.53}$$

diskutieren, wobei die x, y, z in Permutationen die Werte a, b, c annehmen. Hier geht es jetzt aber zunächst um die Positionen im Kranzprodukt:
Der zu einer Automorphismengruppe mit dem Kranzprodukt 3.53 gehörende Code ist ein zyklischer $[N, k, d]$-Code, für den gilt

$$d = 2 \cdot x \tag{3.54}$$

und

$$k = (y-1) \cdot z, y \neq 2 \tag{3.55}$$

$$k = z + 1, y = 2. \tag{3.56}$$

Der zugehörige duale Code ist dann also ein $[N, N-k, 2]$-Code.
In einigen Fällen (s.u.) gibt es noch einen weiteren zyklischen Code zu derselben Automorphismengruppe. Dieser hat dieselbe Minimaldistanz, aber die Dimension ist um 1 größer – also ein $[N, k+1, d]$-Code, wobei für k die obige Formel $k = (y-1) \cdot z$ gilt.

Wir kommen nun zu den **Fallunterscheidungen**.

- 1. Fall: $a \neq b \neq c$: Es existieren 8 (falls $a = 2$, s.u.) oder 12 weitere zyklische Codes (sowie die dazugehörigen dualen Codes). Die zugehörigen Automorphismengruppen werden durch dreifache Kranzprodukte aller Vertauschungen der symmetrischen

Gruppen gebildet, also:

$$\mathfrak{S}_a \wr \mathfrak{S}_b \wr \mathfrak{S}_c \tag{3.57}$$

$$\mathfrak{S}_a \wr \mathfrak{S}_c \wr \mathfrak{S}_b \tag{3.58}$$

$$\mathfrak{S}_b \wr \mathfrak{S}_a \wr \mathfrak{S}_c \tag{3.59}$$

$$\mathfrak{S}_b \wr \mathfrak{S}_c \wr \mathfrak{S}_a \tag{3.60}$$

$$\mathfrak{S}_c \wr \mathfrak{S}_b \wr \mathfrak{S}_a \tag{3.61}$$

$$\mathfrak{S}_c \wr \mathfrak{S}_a \wr \mathfrak{S}_b. \tag{3.62}$$

Ist zudem $a = 2$, so werden die ersten beiden Automorphismmengruppen je 4-mal angenommen, die übrigen nur je 2-mal.
Beispiele: $N = 30, 60$.

- 2. Fall: $2 = a = b \neq c$: Es existieren genau 2 weitere zyklische Codes (und die dazugehörigen 2 dualen Codes). Die zugehörigen Automorphismengruppen werden durch die folgenden dreifachen Kranzprodukte (nicht aller Vertauschungen der symmetrischen Gruppen) gebildet, nämlich:

$$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_c \tag{3.63}$$

Der zugehörige Code ist ein zyklischer $[N, c+1, 4 = 2a]$-Code. Sein dualer Partner ist ein zyklischer $[N, N-c-1, 2]$-Code.

$$\mathfrak{S}_2 \wr \mathfrak{S}_c \wr \mathfrak{S}_2. \tag{3.64}$$

Der zugehörige Code ist ein zyklischer $[N, 2 \cdot (c-1), 4 = 2a]$-Code. Sein dualer Partner ist ein zyklischer $[N, N - 2 \cdot (c-1), 2]$-Code.
Beispiele: $N = 20, 24, 28, 32, 36$, usw.

- 3. Fall: $2 \neq a = b \neq c$: Es existieren 6 weitere zyklische Codes (und die dazugehörigen 6 dualen Codes). Die zugehörigen drei Automorphismengruppen werden also jeweils insgesamt 4-mal angenommen. Sie werden durch die folgenden dreifachen Kranzprodukte aller Vertauschungen der symmetrischen Gruppen gebildet, nämlich:

$$\mathfrak{S}_a \wr \mathfrak{S}_a \wr \mathfrak{S}_c \tag{3.65}$$

Die zugehörigen Codes sind einmal ein zyklischer $[N, c \cdot (a-1), 2a]$-Code. Sein dualer Partner ist ein zyklischer $[N, N - c \cdot (a-1), 2]$-Code.
Der zweite zugehörige Code ist ein zyklischer $[N, c \cdot (a-1)+1, 2a]$-Code. Sein dualer Partner ist ein zyklischer $[N, N - c \cdot (a-1) - 1, 2]$-Code.

$$\mathfrak{S}_a \wr \mathfrak{S}_c \wr \mathfrak{S}_a \tag{3.66}$$

Die zugehörigen Codes sind einmal ein zyklischer $[N, a \cdot (c-1), 2a]$-Code. Sein dualer Partner ist ein zyklischer $[N, N - a \cdot (c-1), 2]$-Code.

Der zweite zugehörige Code ist ein zyklischer $[N, a \cdot (c-1)+1, 2a]$-Code. Sein dualer Partner ist ein zyklischer $[N, N - a \cdot (c-1) - 1, 2]$-Code.

$$\mathfrak{S}_c \wr \mathfrak{S}_a \wr \mathfrak{S}_a. \tag{3.67}$$

Die zugehörigen Codes sind einmal ein zyklischer $[N, a \cdot (a-1), 2c]$-Code. Sein dualer Partner ist ein zyklischer $[N, N - a \cdot (a-1), 2]$-Code.
Der zweite zugehörige Code ist ein zyklischer $[N, a \cdot (a-1)+1, 2c]$-Code. Sein dualer Partner ist ein zyklischer $[N, N - a \cdot (a-1) - 1, 2]$-Code.
Beispiele: $N = 45$, 54, 63, 72, 80.

- 4. Fall: $2 \neq a \neq b = c$: Es existieren 6 weitere zyklische Codes (und die dazugehörigen 6 dualen Codes). Die zugehörigen drei Automorphismengruppen werden durch die folgenden dreifache Kranzprodukte aller Vertauschungen der symmetrischen Gruppen gebildet, nämlich:

$$\mathfrak{S}_a \wr \mathfrak{S}_c \wr \mathfrak{S}_c \tag{3.68}$$

Die zugehörigen Codes sind einmal ein zyklischer $[N, c \cdot (c-1), 2a]$-Code. Sein dualer Partner ist ein zyklischer $[N, N - c \cdot (c-1), 2]$-Code.
Der zweite zugehörige Code ist ein zyklischer $[N, c \cdot (c-1)+1, 2a]$-Code. Sein dualer Partner ist ein zyklischer $[N, N - c \cdot (c-1) - 1, 2]$-Code.

$$\mathfrak{S}_c \wr \mathfrak{S}_c \wr \mathfrak{S}_a \tag{3.69}$$

Die zugehörigen Codes sind einmal ein zyklischer $[N, a \cdot (c-1), 2c]$-Code. Sein dualer Partner ist ein zyklischer $[N, N - a \cdot (c-1), 2]$-Code.
Der zweite zugehörige Code ist ein zyklischer $[N, a \cdot (c-1)+1, 2c]$-Code. Sein dualer Partner ist ein zyklischer $[N, N - a \cdot (c-1) - 1, 2]$-Code.

$$\mathfrak{S}_c \wr \mathfrak{S}_a \wr \mathfrak{S}_c. \tag{3.70}$$

Die zugehörigen Codes sind einmal ein zyklischer $[N, c \cdot (a-1), 2c]$-Code. Sein dualer Partner ist ein zyklischer $[N, N - c \cdot (a-1), 2]$-Code.
Der zweite zugehörige Code ist ein zyklischer $[N, c \cdot (a-1)+1, 2c]$-Code. Sein dualer Partner ist ein zyklischer $[N, N - c \cdot (a-1) - 1, 2]$-Code.
Beispiele: $N = 75$.

- 5. Fall: $2 = a \neq b = c$: Es existieren 4 weitere zyklische Codes (und die dazugehörigen 4 dualen Codes). Die zugehörigen drei Automorphismengruppen werden durch die folgenden dreifache Kranzprodukte aller Vertauschungen der symmetrischen Gruppen gebildet, nämlich:

$$\mathfrak{S}_2 \wr \mathfrak{S}_c \wr \mathfrak{S}_c \tag{3.71}$$

Die zugehörigen Codes sind einmal ein zyklischer $[N, c \cdot (c-1), 4]$-Code. Sein dualer Partner ist ein zyklischer $[N, N - c \cdot (c-1), 2]$-Code.

Der zweite zugehörige Code ist ein zyklischer $[N, c \cdot (c-1)+1, 4]$-Code. Sein dualer Partner ist ein zyklischer $[N, N - c \cdot (c-1) - 1, 2]$-Code.

$$\mathfrak{S}_c \wr \mathfrak{S}_c \wr \mathfrak{S}_2 \tag{3.72}$$

Der zugehörige Code ist ein zyklischer $[N, 2 \cdot (c-1), 2c]$-Code. Sein dualer Partner ist ein zyklischer $[N, N - 2 \cdot (c-1), 2]$-Code.

$$\mathfrak{S}_c \wr \mathfrak{S}_2 \wr \mathfrak{S}_c. \tag{3.73}$$

Der zugehörige Code ist ein zyklischer $[N, c+1, 2c]$-Code. Sein dualer Partner ist ein zyklischer $[N, N - c - 1, 2]$-Code.
Beispiele: $N = 50,\ 72$.

- 6. Fall: $2 \neq a = b = c$: Es existieren 2 weitere zyklische Codes (und die dazugehörigen 2 dualen Codes). Die zugehörige Automorphismengruppe wird durch das folgenden dreifache Kranzprodukt der symmetrischen Gruppe $\mathfrak{S}_a$ mit sich selbst gebildet, nämlich:

$$\mathfrak{S}_a \wr \mathfrak{S}_a \wr \mathfrak{S}_a \tag{3.74}$$

Die zugehörigen Codes sind einmal ein zyklischer $[N, a \cdot (a-1), 2a]$-Code. Sein dualer Partner ist ein zyklischer $[N, N - a \cdot (a-1), 2]$-Code.
Der zweite zugehörige Code ist ein zyklischer $[N, a \cdot (a-1)+1, 2a]$-Code. Sein dualer Partner ist ein zyklischer $[N, N - a \cdot (a-1) - 1, 2]$-Code.

Beispiel: $N = 125$.

3.2.1 Verminderte Kranzprodukte

Bei der Untersuchung der zyklischen Codes gerader Länge fiel mir auf, daß ab $N = 30$ Automorphismengruppen auftraten, die sich zunächst nicht erklären ließen[6].
Um dies besser zu verdeutlichen, wollen wir hier bereits die Voraussetzungen angeben:

Sei $N = 2 \cdot b \cdot c$ eine Faktorenzerlegung mit $N, b, c \in \mathbb{N}$, wobei b und c nicht beide gleichzeitig kleiner als 5 sein dürfen. Sei ferner c ungerade. Sei außerdem $2 \neq b$.
Diese Automorphismengruppen sehen fast aus, wie ein dreistufiges Kranzprodukt $\mathfrak{S}_2 \wr \mathfrak{S}_b \wr \mathfrak{S}_c$, bei dem also die äußersten Schalen der Kränze um die c Kopien der Gruppe $\mathfrak{S}_b$ aus Kopien der Gruppe $\mathfrak{S}_2$ bestehen. Allerdings sind es nicht – wie üblich – jeweils b Kopien der Gruppe $\mathfrak{S}_2$, sondern bei allen äußeren Kränzen – bis auf einen – fehlt jeweils eine Kopie der Gruppe $\mathfrak{S}_2$.
Ich möchte dies ein „Vermindertes Kranzprodukt“ nennen und den folgenden Satz dazu formulieren:

[6] wie wir im Tabellenteil sehen, treten diese verminderten Kranzprodukte bereits bei $N = 14, 20, 28$ auf und ihnen liegt ggfs. auch nur die Faktorenzerlegung $N = 2 \cdot a$ zugrunde. Mehr dazu im Kapitel 10

Satz 3.20

Sei $N \leq 80$. Seien ferner die Voraussetzungen, wie oben aufgeführt, gegeben.
Dann existiert zu $N = 2 \cdot b \cdot c$ eine Automorphismengruppe mit dem verminderten Kranzprodukt:

$$(\mathfrak{S}_2 \wr \mathfrak{S}_b \wr \mathfrak{S}_c)/\mathfrak{S}_2^{c-1} \tag{3.75}$$

Dazu gehört genau ein zyklischer $[N, \frac{N}{2} - c + 2, 4]$-Code und sein dualer Code (mit $d = 4$). Ist außerdem auch b ungerade, so existiert zusätzlich auch noch eine Automorphismengruppe mit dem verminderten Kranzprodukt:

$$(\mathfrak{S}_2 \wr \mathfrak{S}_c \wr \mathfrak{S}_b)/\mathfrak{S}_2^{b-1} \tag{3.76}$$

Dazu gehört genau ein zyklischer $[N, \frac{N}{2} - b + 2, 4]$-Code und sein dualer Code (mit $d = 4$).

Beweis. exemplarisch durch folgende Codelängen: $N = 30$, 36, 40, 42, 48, 50, 54, 56, 60, 66, 70, 72, 78 und 80 (s. Tabellenwerk im Anhang). □

Bemerkung 3.21

Eine Sonderstellung nimmt auch hier wieder der Fall $c = 7$ ein:
Zusätzlich zu den oben beschriebenen verminderten Kranzprodukten existieren auch noch weitere, bei denen die Permutationsgruppe $PSL(3, 2)$ anstelle der symmetrischen Gruppe $\mathfrak{S}_7$ auftritt. So finden wir z.B. für $N = 42$ nach dem obigen Satz erwartungsgemäß:

$$(\mathfrak{S}_2 \wr \mathfrak{S}_3 \wr \mathfrak{S}_7)/\mathfrak{S}_2^6$$

$$(\mathfrak{S}_2 \wr \mathfrak{S}_7 \wr \mathfrak{S}_3)/\mathfrak{S}_2^2$$

aber auch zusätzlich noch:

$$(\mathfrak{S}_2 \wr \mathfrak{S}_b \wr PSL(3, 2))/\mathfrak{S}_2^6 \tag{3.77}$$

$$(\mathfrak{S}_2 \wr \mathfrak{S}_b \wr PSL(3, 2))/\mathfrak{S}_2^3 \tag{3.78}$$

und, da b ungerade ist, auch noch

$$(((\mathfrak{S}_2 \wr PSL(3, 2))/\mathfrak{S}_2^3) \wr \mathfrak{S}_b)/\mathfrak{S}_2^{b-1} \tag{3.79}$$

Zu den letzten drei obigen Automorphismengruppen gehören jeweils insgesamt 6, 4 und 8 zyklische Codes (s. Tabelle im Anhang).

Zur besseren Veranschaulichung habe ich auf der folgenden Seite als Beispiel die Automorphismengruppe $(\mathfrak{S}_2 \wr \mathfrak{S}_3 \wr \mathfrak{S}_5)/\mathfrak{S}_2^4$ mit Unterteilungen und Kommentaren abgedruckt. Eine ausführliche Analyse eines verminderten Kranzprodukts findet sich im Unterabschnitt 5.2.

Beispiel 3.22 ($N = 30$, **verminderte Kranzproduktstruktur** $(\mathfrak{S}_2 \wr \mathfrak{S}_3 \wr \mathfrak{S}_5)/\mathfrak{S}_2^4$)

```
29 . Automorphismen-Gruppe mit 1911029760 Elementen - Haeufigkeit dieser Gruppe: 2 mal
    G
    |  Cyclic(2)     \
    *                 >=Sym(5) innerste Permutationsgruppe des verminderten Kranzes
    |  Alternating(5)/
    * ################
    |  Cyclic(2)     \
    *                 >=Sym(3) Permutationsgruppe 1 von 5 des Zwischenkranzes
    |  Cyclic(3)     /
    * ===============
    |  Cyclic(2)       =Sym(2) Gruppe 1 des 1. Aussenkranzes zum Zwischenkranz
    * ---------------
    |  Cyclic(2)       =Sym(2) Gruppe 2 des 1. Aussenkranzes zum Zwischenkranz
    *----------------
    |  Cyclic(2)       =Sym(2) Gruppe 3 des 1. Aussenkranzes zum Zwischenkranz
    * ################
    |  Cyclic(2)     \
    *                 >=Sym(3) Permutationsgruppe 2 von 5 des Zwischenkranzes
    |  Cyclic(3)     /
    * ===============
    |  Cyclic(2)       =Sym(2) Gruppe 1 des 2. Aussenkranzes zum Zwischenkranz
    * ---------------
    |  Cyclic(2)       =Sym(2) Gruppe 2 des 2. Aussenkranzes zum Zwischenkranz
    * ################         (Gruppe 3 fehlt hier)
    |  Cyclic(2)     \
    *                 >=Sym(3) Permutationsgruppe 3 von 5 des Zwischenkranzes
    |  Cyclic(3)     /
    * ===============
    |  Cyclic(2)       =Sym(2) Gruppe 1 des 3. Aussenkranzes zum Zwischenkranz
    * ---------------
    |  Cyclic(2)       =Sym(2) Gruppe 2 des 3. Aussenkranzes zum Zwischenkranz
    * ################         (Gruppe 3 fehlt hier)
    |  Cyclic(2)     \
    *                 >=Sym(3) Permutationsgruppe 4 von 5 des Zwischenkranzes
    |  Cyclic(3)     /
    * ===============
    |  Cyclic(2)       =Sym(2) Gruppe 1 des 4. Aussenkranzes zum Zwischenkranz
    * ---------------
    |  Cyclic(2)       =Sym(2) Gruppe 2 des 4. Aussenkranzes zum Zwischenkranz
    * ################         (Gruppe 3 fehlt hier)
    |  Cyclic(2)     \
    *                 >=Sym(3) Permutationsgruppe 5 von 5 des Zwischenkranzes
    |  Cyclic(3)     /
    * ===============
    |  Cyclic(2)       =Sym(2) Gruppe 1 des 5. Aussenkranzes zum Zwischenkranz
    * ---------------
    |  Cyclic(2)       =Sym(2) Gruppe 2 des 5. Aussenkranzes zum Zwischenkranz
    1                          (Gruppe 3 fehlt hier)
```

3.2.2 Gemischte Produkte

Bei der Untersuchung der zyklischen Codes gerader Länge fiel mir auf, daß ab $N = 30$ noch weitere Automorphismengruppen auftraten, die sich jedoch etwas einfacher erklären ließen, als die oben behandelten verminderten Kranzprodukte.

Es gelten auch hier wieder die obigen Voraussetzungen, zusätzlich müssen b und c teilerfremd sein (auch hier sei zunächst $a = 2$; den allgemeinen Fall $N = a \cdot b \cdot c$ werden wir im Anschluß behandeln, siehe Bemerkung 3.24).

Sei $N = 2 \cdot b \cdot c$ eine Faktorenzerlegung mit $N, b, c \in \mathbb{N}$, wobei b und c nicht beide gleichzeitig kleiner als 5 sein dürfen. Sei ferner c ungerade. Sei außerdem $2 \neq b$ teilerfremd zu c.

Es handelt sich hierbei um **gemischte Gruppenprodukte** der drei beteiligten Permutationsgruppen, d.h., wir haben als Verknüpfung zwischen je zwei dieser drei Permutationsgruppen zum einen die Kranzproduktfunktion und zum anderen die Funktion des direkten Produktes.
Da das direkte Produkt im Gegensatz zum Kranzprodukt kommutativ ist, ist bei drei beteiligten Gruppenfaktoren die Anzahl der auftretenden Varianten noch überschaubar.

Die hier im Folgenden gemachten Aussagen stellen eine Zusammenfassung der Erkenntnisse aus dem umfangreichen Listen- und Tabellenwerk dar und sind für die angegebenen Codelängen anhand der identifizierten Automorphismengruppen und deren zugehörige Codes exemplarisch überprüft worden.

Beobachtung 3.23
Seien die Voraussetzungen, wie oben aufgeführt, gegeben.
Dann existieren zu $N = 2 \cdot b \cdot c$ die folgenden 4 Automorphismengruppen mit dem gemischten Produkt:

$$\mathfrak{S}_2 \wr (\mathfrak{S}_b \times \mathfrak{S}_c)$$

$$(\mathfrak{S}_b \times \mathfrak{S}_c) \wr \mathfrak{S}_2$$

$$(\mathfrak{S}_b \wr \mathfrak{S}_2) \times \mathfrak{S}_c$$

$$(\mathfrak{S}_2 \wr \mathfrak{S}_b) \times \mathfrak{S}_c$$

Ist außerdem auch b ungerade, so existieren zusätzlich auch noch die folgenden 2 Automorphismengruppen mit dem gemischten Produkt:

$$(\mathfrak{S}_c \wr \mathfrak{S}_2) \times \mathfrak{S}_b$$

$$(\mathfrak{S}_2 \wr \mathfrak{S}_c) \times \mathfrak{S}_b$$

Wir wollen nun die obigen 6 Automorphismengruppen mit ihren zugehörigen Codes im Detail diskutieren:

1.
$$\mathfrak{S}_2 \wr (\mathfrak{S}_b \times \mathfrak{S}_c) \tag{3.80}$$

Falls $b \neq 4$, so wird diese Automorphismengruppe von insgesamt 8 Codes angenommen, sonst von 4 Codes (beide Angaben inklusive der dualen Codes).
Also, im Fall $b \neq 4$ sehen die 8 Codes folgendermaßen aus (in den Formeln ist stets $a = 2$):

(a) ein zyklischer $[N, c + b - 2, 2ab]$ - Code,

(b) ein zyklischer $[N, c + b - 1, ab]$ - Code,

(c) ein zyklischer $[N, (b-1)(c-1), 4a]$ - Code,

(d) ein zyklischer $[N, (b-1)(c-1) + 1, 4a]$ - Code,

(e) sowie die zu diesen 4 Codes zugehörigen dualen Codes, sämtlich mit $d = 2$.

Dies wurde mit folgenden Codelängen überprüft: 30, 42, 48, 66, 70, 78, 60 und $a = 2$.

Also, im Fall $b = 4$ sehen die 4 Codes folgendermaßen aus (in den Formeln ist i.a. $a = 2$):

(a) ein zyklischer $[N, c + b - 1, ab]$ - Code (gleich dem zweiten Code der vorigen Liste),

(b) ein zyklischer $[N, (b-1)(c-1), 4a]$ - Code (gleich dem dritten Code der vorigen Liste),

(c) sowie die zu diesen 2 Codes zugehörigen dualen Codes, sämtlich mit $d = 2$.

Dies wurde mit folgenden Codelängen überprüft: 40, 56, 72; 80 ($a = 4$).

2.
$$(\mathfrak{S}_b \times \mathfrak{S}_c) \wr \mathfrak{S}_2 \tag{3.81}$$

Falls $b \neq 4$, so wird diese Automorphismengruppe von insgesamt 6 Codes angenommen, sonst von 4 Codes (beide Angaben inklusive der dualen Codes).
Also, im Fall $b \neq 4$ sehen die 6 Codes folgendermaßen aus (in den Formeln ist stets $a = 2$):

(a) ein zyklischer $[N, a(c + b - 1) - 2, 2b]$ - Code,

(b) ein zyklischer $[N, a(c + b - 1) - 1, 2b]$ - Code,

(c) ein zyklischer $[N, a(c + b - 1), b]$ - Code,

(d) sowie die zu diesen 3 Codes zugehörigen dualen Codes, sämtlich mit $d = 4$.

Dies wurde mit folgenden Codelängen überprüft: 30, 42, 48, 60 (a=2), 66, 70, 78, 80.
Also, im Fall $b = 4$ sehen die 4 Codes folgendermaßen aus (in den Formeln ist stets $a = 2$):

(a) ein zyklischer $[N, a(c+b-1)-1, b]$ - Code (ähnlich dem zweiten Code der vorigen Liste),

(b) ein zyklischer $[N, a(c+b-1), b]$ - Code (gleich dem dritten Code der vorigen Liste),

(c) sowie die zu diesen 2 Codes zugehörigen dualen Codes, sämtlich mit $d = 4$.

Dies wurde mit folgenden Codelängen überprüft: 40, 56, 72.

3.

$$(\mathfrak{S}_b \wr \mathfrak{S}_2) \times \mathfrak{S}_c \tag{3.82}$$

Zu dieser Automorphismengruppe gehört genau ein zyklischer Code und sein dualer Code. Sie sehen folgendermaßen aus (in den Formeln ist stets $a = 2$):

(a) ein zyklischer $[N, c-3+2b, d]$ - Code, dabei ist d=min(2c,2ab), falls b $\neq 4$ und $d = min(2c, ab)$, falls $b = 4$.

(b) sowie der zu diesem Code zugehörige duale Code, mit $d = 4$.

Dies wurde mit folgenden Codelängen überprüft: 30, 40, 42, 56, 66, 70, 72, 78; 60 ($b = 6$); 48, 80 ($b = 8$).

4.

$$(\mathfrak{S}_2 \wr \mathfrak{S}_b) \times \mathfrak{S}_c \tag{3.83}$$

$$\cong (\mathfrak{S}_2 \wr (\mathfrak{S}_b \times \mathfrak{S}_c))/\mathfrak{S}_2^{b(c-1)} \tag{3.84}$$

Zu dieser Automorphismengruppe gehört genau ein zyklischer Code und sein dualer Code. Sie sehen folgendermaßen aus:

(a) ein zyklischer $[N, (c-1)(b+1), 4]$ - Code.

(b) sowie der zu diesem Code zugehörige duale Code, mit $d = 4$.

Dies wurde mit folgenden Codelängen überprüft: 30, 40, 42, 56, 66, 70, 72, 78; 60 ($b = 6$); 48, 80 ($b = 8$).

5.

$$(\mathfrak{S}_c \wr \mathfrak{S}_2) \times \mathfrak{S}_b \tag{3.85}$$

Zu dieser Automorphismengruppe gehört genau ein zyklischer Code und sein dualer Code. Sie sehen folgendermaßen aus (in der Formel ist stets $a = 2$ und b ungerade):

(a) ein zyklischer $[N, 2c+b-3, 2b]$ - Code.

(b) sowie der zu diesem Code zugehörige duale Code, mit $d = 4$.

Dies wurde mit folgenden Codelängen überprüft: 30, 42, 66, 70, 78.

6.

$$(\mathfrak{S}_2 \wr \mathfrak{S}_c) \times \mathfrak{S}_b \tag{3.86}$$

$$\cong (\mathfrak{S}_2 \wr (\mathfrak{S}_b \times \mathfrak{S}_c))/\mathfrak{S}_2^{(b-1)c} \tag{3.87}$$

Zu dieser Automorphismengruppe gehört genau ein zyklischer Code und sein dualer Code. Sie sehen folgendermaßen aus (in der Formel ist stets $a = 2$ und b ungerade):

(a) ein zyklischer $[N, (c+1)(b-1), 4]$ - Code.

(b) sowie der zu diesem Code zugehörige duale Code, mit $d = 3$.

Dies wurde mit folgenden Codelängen überprüft: 30, 42, 66, 70, 78.

Bemerkung 3.24

Bei größeren Codelängen im Untersuchungsbereich (ab $N = 45$) treten gemischte Produkte auf mit $a \geq 3$. Dadurch sind bei 3 Faktoren (z.B. $N = 60$ mit $a = 4$, $b = 3$, $c = 5$) alle 12 Kombinationen vertreten (falls $a \neq b \neq c$).
Im Fall $a = b$ oder $a = c$ reduziert sich die Anzahl der verschiedenen gemischten Produkte auf 3 (Bsp. N =45, 75, 80 mit $a = b = 4$, $c = 5$).
Auch ist bei einigen Produkten die Anzahl der zugehörigen Codes größer als für $a = 2$: So finden wir bei obigem Beispiel ($N = 60$ mit $a = 4$, $b = 3$, $c = 5$) durchaus 4 Produkte mit je 12 Codes, sowie 2 Produkte mit 8 Codes; dabei sind dies die weiter oben diskutierten bisherigen 6 Produkttypen.
Solange $a = 2$ ist, treten die Komponenten $(\mathfrak{S}_2 \times \mathfrak{S}_b)$ oder $(\mathfrak{S}_2 \times \mathfrak{S}_c)$ nicht auf und es bleibt bei 6, oder im Fall $a = 2$ und b gerade, nur bei 4 Kombinationen dieser gemischten Produkte (Bsp. $N = 60$, $a = 2$, $b = 6$, $c = 5$).

Der Vollständigkeit halber wollen wir hier alle 12 Produkttypen zusammenstellen:

$$\mathfrak{S}_a \wr (\mathfrak{S}_b \times \mathfrak{S}_c) \tag{3.88}$$

$$(\mathfrak{S}_b \times \mathfrak{S}_c) \wr \mathfrak{S}_a \tag{3.89}$$

$$(\mathfrak{S}_b \wr \mathfrak{S}_a) \times \mathfrak{S}_c \tag{3.90}$$

$$(\mathfrak{S}_a \wr \mathfrak{S}_b) \times \mathfrak{S}_c \tag{3.91}$$

$$(\mathfrak{S}_c \wr \mathfrak{S}_a) \times \mathfrak{S}_b \tag{3.92}$$

$$(\mathfrak{S}_a \wr \mathfrak{S}_c) \times \mathfrak{S}_b \tag{3.93}$$

$$\mathfrak{S}_c \wr (\mathfrak{S}_a \times \mathfrak{S}_b) \tag{3.94}$$

$$(\mathfrak{S}_a \times \mathfrak{S}_b) \wr \mathfrak{S}_c \tag{3.95}$$

$$\mathfrak{S}_b \wr (\mathfrak{S}_a \times \mathfrak{S}_c) \tag{3.96}$$

$$(\mathfrak{S}_a \times \mathfrak{S}_c) \wr \mathfrak{S}_b \tag{3.97}$$

$$(\mathfrak{S}_b \wr \mathfrak{S}_c) \times \mathfrak{S}_a \tag{3.98}$$

$$(\mathfrak{S}_c \wr \mathfrak{S}_b) \times \mathfrak{S}_a \tag{3.99}$$

Darüberhinaus treten bei großen Codelängen im Untersuchungsbereich (ab $N = 60$) auch gemischte Produkte mit 4 und mehr Faktoren auf. Es würde jedoch den Rahmen dieser Arbeit sprengen, auch diese Gruppen mit ihren Codes im Detail zu behandeln.
Ende der Bemerkung

Weiterhin existiert für b und c ungerade, sowie b teilerfremd zu c, auch noch eine Automorphismengruppe mit einem verminderten Kranzprodukt aus einem gemischten Produkt:

$$(\mathfrak{S}_2 \wr (\mathfrak{S}_b \times \mathfrak{S}_c))/\mathfrak{S}_2^{(b-1)+(c-1)} \tag{3.100}$$

Zu dieser Automorphismengruppe gehört ein zyklischer Code und sein dualer Code. Sie sehen folgendermaßen aus:

1. ein zyklischer $[N, 2c + (b-3)(c-1), 8]$ - Code,
2. sowie der zu diesem Code zugehörige duale Code, mit $d = 4$.

Dies wurde mit folgenden Codelängen überprüft: 30, 42, 66, 78, 102 mit $b = 3$; sowie 70, 90 und 110 mit $b = 5$ und auch $N = 154$ mit $b = 7$.

Zusätzlich existiert noch (auch für b gerade):

$$(\mathfrak{S}_2 \wr (\mathfrak{S}_b \times \mathfrak{S}_c))/\mathfrak{S}_2^{(b-1)(c-1)} \tag{3.101}$$

(Diese Automorphismengruppe existiert zusätzlich auch für $b = 3$; sie wird dort oft durch die isomorphe Gruppe $\mathfrak{S}_4 \times (\mathfrak{S}_2 \wr \mathfrak{S}_c)$, siehe unten (3.102) mit kürzerer Schreibweise dargestellt.)

Zu dieser Automorphismengruppe gehören zwei zyklische Codes und ihre dualen Codes. Sie sehen folgendermaßen aus:

1. ein zyklischer $[N, b + c, 2b]$ - Code,
2. sowie der zu diesem Code zugehörige duale Code, mit $d = 4$.
3. ein zyklischer $[N, (b - 1)(c + 1) + 1, 4]$ - Code,
4. sowie der zu diesem Code zugehörige duale Code, mit $d = 4$.

Dies wurde mit folgenden Codelängen überprüft: 30, 42, 48, 60, 66, 78 und 102 mit $b = 3$; 40, 56 und 88 mit $b = 4$, sowie 70, 90 und 110 mit $b = 5$ und auch $N = 154$ mit $b = 7$.

Die oben bereits erwähnte Automorphismengruppe zum folgenden gemischten Produkt (nur für $b = 3$) ist wesentlich leichter auf Isomorphie zu überprüfen (s. Anhang, „Magma-Besonderheiten, Gruppendivision“):

$$\mathfrak{S}_4 \times (\mathfrak{S}_2 \wr \mathfrak{S}_c) \tag{3.102}$$

Bemerkung 3.25
Die Isomorphie zum weiter oben angegebenen gemischten Produkt (3.101) ergibt sich aus der Verwandtschaft der Kompositionsreihen von $\mathfrak{S}_3$ und $\mathfrak{S}_4$. Es gilt:

$$\mathfrak{S}_4 \cong \mathfrak{K}_4 \rtimes \mathfrak{S}_3 \cong (\mathfrak{S}_2 \times \mathfrak{S}_2) \rtimes \mathfrak{S}_3 \cong \mathfrak{S}_2^2 \rtimes \mathfrak{S}_3. \tag{3.103}$$

In den Tabellen des Anhangs sind beide Darstellungen des gemischten Produkts angegeben.
Ende der Bemerkung

Zu dieser Automorphismengruppe gehören genau zwei zyklischer Codes und ihre dualen Codes. Sie sehen erwartungsgemäß folgendermaßen aus:

1. ein zyklischer $[N, c + 3, 6]$ - Code.
2. sowie der zu diesem Code zugehörige duale Code, mit $d = 4$.
3. ein zyklischer $[N, 2c + 3, 4]$ - Code.
4. sowie der zu diesem Code zugehörige duale Code, mit $d = 4$.

Dies wurde mit folgenden Codelängen überprüft: 30, 42, 66, 78, 102, 48, 60.

Interessanterweise gibt es für den Fall $b = 3$, $c = 7$ auch je ein Analogon mit der Gruppe $PSL(3, 2)$ anstatt $\mathfrak{S}_7$ zu den letzten beiden aufgeführten Automorphismengruppen (s. $N = 42$, Automorphismengruppen Nr. 23 und 41, bzw. 39 und 37):

$$\mathfrak{S}_4 \times (\mathfrak{S}_2 \wr PSL(3, 2)) \tag{3.104}$$

$$(\mathfrak{S}_2 \wr (\mathfrak{S}_b \times PSL(3, 2))/\mathfrak{S}_2^8 \tag{3.105}$$

Sinngemäß gilt dies auch für $b = 4$ und $b = 5$ (soweit untersucht).

Bemerkung 3.26
Wie bereits im Abschnitt 1.2.3 bewiesen, existiert im Fall $b = 4$ noch zustzlich

$$\mathfrak{S}_2 \wr (\mathfrak{S}_c \times (\mathfrak{S}_2 \wr \mathfrak{S}_2)) \tag{3.106}$$

Eine Sonderstellung nimmt auch hier wieder der Fall $c = 7$ ein:
Zusätzlich zu den oben beschriebenen gemischten Produkten existieren auch noch weitere, bei denen die Permutationsgruppe $PSL(3,2)$ anstelle der symmetrischen Gruppe $\mathfrak{S}_7$ auftritt. So finden wir z.B. für $N = 42$ ($b = 3$), oder $N = 56$ ($b = 4$), oder $N = 70$ (b =5) zusätzlich noch:

$$\mathfrak{S}_2 \wr (\mathfrak{S}_b \times PSL(3,2)) \tag{3.107}$$

$$(\mathfrak{S}_b \times PSL(3,2)) \wr \mathfrak{S}_2 \tag{3.108}$$

$$(\mathfrak{S}_2 \wr \mathfrak{S}_b) \times PSL(3,2) \tag{3.109}$$

$$\cong (\mathfrak{S}_2 \wr (\mathfrak{S}_b \times PSL(3,2))/\mathfrak{S}_2^{6b} \tag{3.110}$$

$$(\mathfrak{S}_b \wr \mathfrak{S}_2) \times PSL(3,2) \tag{3.111}$$

Ist außerdem auch b ungerade, so existieren zusätzlich auch noch die folgenden 2 Automorphismengruppen mit dem gemischten Produkt:

$$(\mathfrak{S}_2 \wr PSL(3,2)) \times \mathfrak{S}_b \tag{3.112}$$

$$\cong (\mathfrak{S}_2 \wr (\mathfrak{S}_b \times PSL(3,2))/\mathfrak{S}_2^{7(b-1)} \tag{3.113}$$

$$(PSL(3,2) \wr \mathfrak{S}_2) \times \mathfrak{S}_b. \tag{3.114}$$

Diese letzten 4 oder 6 Automorphismengruppen werden von sehr vielen Codes angenommen (s. Tabellen im Anhang), zwischen jeweils 24 bis über 50 Codes insgesamt (d.h., inklusive der dualen Codes).

Weiterhin existieren für die Codelängen $N = 42$, 56, 70 auch noch eine Reihe von Automorphismengruppen mit je einem verminderten Kranzprodukt aus einem gemischten Produkt:

$$(\mathfrak{S}_2 \wr (\mathfrak{S}_b \times PSL(3,2))/\mathfrak{S}_2^y \tag{3.115}$$

Dabei werden bei den Codelängen $N = 42$ und $N = 56$ für y Werte in Dreiersprüngen beobachtet:
$N = 42$: $y = 6$, 9, 12 (zweimal), 15, 18; sowie 5, 8, 11, 14 (zweimal), 17, 20.
$N = 56$: $y = 6$, 9, 12, 15, 18, 21.
Speziell bei $N = 56$ beobachten wir noch einen ähnlichen Produkttyp:

$$(\mathfrak{S}_2 \wr (PSL(3,2) \times (\mathfrak{S}_2 \wr \mathfrak{S}_2)))/\mathfrak{S}_2^y \tag{3.116}$$

Auch hier beobachten wir für y Werte in Dreiersprüngen:
$N = 56$: $y = 9, 12, 15, 18, 21, 24$.

Diese Sonderstellung, wie für $c = 7$ ist ggfs. auch für weitere Spezialfälle – wie z.B. $c = 15$ und die zugehörige Gruppe $PSL(4, 2)$ zu erwarten.

Grundsätzlich lassen sich all diese zuletzt dokumentierten Automorphismengruppen auf das folgende Grundmuster zurückführen:

$$(\mathfrak{S}_2 \wr Aut(C))/\mathfrak{S}_2^y, \quad bzw. \tag{3.117}$$

$$\mathfrak{S}_2^x \rtimes Aut(C), \quad x = n - y; n = N/2. \tag{3.118}$$

Wir werden in den späteren Kapiteln 10 und 9 sehen, daß wir einen Aut(C)-Modul $\mathbb{F}_2[\Omega]$ erzeugen können, dessen **Untermoduln** zyklische Codes sind. Die „Addition“ zweier solcher Codes mit der Plotkin-Summe führt dann zu neuen zyklischen Codes der doppelten Codelänge und den Automorphismengruppen $(\mathfrak{S}_2 \wr Aut(C))/\mathfrak{S}_2^y$. Im Kapitel 10 ist das detailliert für $Aut(C) = PSL(r, 2)$ ausgearbeitet.
Für $N = 42$ und $Aut(C) = \mathfrak{S}_3 \times PSL(3, 2)$, bzw. $Aut(C) = \mathfrak{S}_3 \times \mathfrak{S}_7$ habe ich das beispielhaft mit **Magma** gerechnet und verifiziert. Es würde jedoch den Rahmen dieser Arbeit sprengen, alle verminderten gemischten Produkte (bzw. semidirekte gemischte Produkte) aus dem Tabellenwerk hier im Detail zu diskutieren.
Um aber wenigstens ein Gefühl für die Vielfältigkeit dieser Konstruktonen zu entwickeln, sei hier in einer kleinen Tabelle 3.2 zumindest die Anzahl der Untermoduln einiger Aut(C)-Moduln $\mathbb{F}_2[\Omega]$ angegeben.
Ich könnte mir aber durchaus eine eigenständige wissenschaftliche Arbeit zu diesem Thema auf der Basis meiner Ergebnisse und gesammelten Daten vorstellen.

Soweit die Erkenntnisse bezüglich der Zerlegung von N in 3 Faktoren.

Für $N = 56$ finden wir zusätzlich zu den obigen 4 Automorphismengruppen noch

$$((\mathfrak{S}_2 \wr \mathfrak{S}_2) \times PSL(3, 2)) \wr \mathfrak{S}_2 \tag{3.119}$$

$$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr (\mathfrak{S}_2 \times PSL(3, 2)) \tag{3.120}$$

$$(\mathfrak{S}_2 \wr (\mathfrak{S}_2 \times PSL(3, 2))) \wr \mathfrak{S}_2 \tag{3.121}$$

$$(\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_2) \times PSL(3, 2) \tag{3.122}$$

die im wesentlichen durch Vererbung aus Automorphismengruppen mit gemischten Produkten der Codelänge $N = 28$ hervorgehen (siehe dazu auch das Kapitel „Vererbung von Codes und Automorphismengruppen“).

Anzahl der Untermoduln	Code-Länge	Automorphismengruppe
2	7	$PSL(3,2)$
4	15	$PSL(4,2)$
4	21	$\mathfrak{S}_7 \times \mathfrak{S}_3$
12	21	$PSL(3,2) \times \mathfrak{S}_3$
2	23	$M23$
10	28	$PSL(3,2) \times \mathfrak{S}_4$
6	31	$PSL(5,2)$
16	51	$PSL(2,16) \rtimes \mathfrak{Q}_3$
8	63	$PSL(6,2)$
6	73	$PSL(3,8) \rtimes \mathfrak{Z}_3$
8	85	$PSL(4,4) \rtimes \mathfrak{Z}_2$
60	89	$\mathfrak{MZ}(89,11)$, auflösbar

Tabelle 3.2: Tabelle der Anzahlen einiger $Aut(C)$-Modul $\mathbb{F}_2[\Omega]$-Untermoduln (abzüglich der vier trivialen Untermoduln mit Dimension $k = 0, 1, N-1, N$)

3.3 Zerlegung der Codelänge in 4 Faktoren

Wir wollen jetzt nur noch einige Erkenntnisse bezüglich der Zerlegung von N in 4 Faktoren zusammenfassen, ohne näher auf die zugehörigen Codes und deren Attribute einzugehen:

Lemma 3.27
Sei $N = a \cdot b \cdot c \cdot e$ eine Faktorenzerlegung mit $N, a, b, c, e \in \mathbb{N}$, wobei a, b, c und e nicht alle gleichzeitig kleiner als 5 sein dürfen. Sei oBdA $a \leq b \leq c \leq e$.
Dann gilt folgende Aussage:
Zu den zyklischen Codes der Länge N existieren Automorphismengruppen als Kranzprodukte der Form

$$\mathfrak{S}_x \wr \mathfrak{S}_y \wr \mathfrak{S}_z \wr \mathfrak{S}_w, \tag{3.123}$$

wobei die x, y, z, w in Permutationen die Werte a, b, c, e annehmen.

Das ergibt grundsätzlich 24 verschiedene 4-fache Kranzprodukte.
Falls $a \neq b \neq c \neq e$, so sollten diese auch als Automorphismengruppen auftreten. Die zugehörige Codelänge wäre dann $\geq$120. In unserem Tabellenwerk finden sich jedoch nur Codelängen mit Zerlegungen in 4 Faktoren, wie z.B. N = 40, 48, 56, 60, 72 und 80, bei denen die Werte a bis e nicht alle verschieden sind. Wir finden im Fall $a = b = 2$ nur 10 der vierfachen Kranzprodukte und im Fall $a = b = c = 2$ nur die beiden vierfachen Kranzprodukte, die bereits im Abschnitt 1.2.3 beschrieben wurden. Auch hierbei fällt wieder auf, daß Kranzprodukte aus symmetrischen Gruppen nicht auftreten, bei denen

am Schluß $\mathfrak{S}_2 \wr \mathfrak{S}_2$ stehen würde. Dadurch reduziert sich die Anzahl der unterschiedlichen vierfachen Kranzprodukte im Fall $a = b = 2$ von 12 auf 10, sowie im Fall $a = b = c = 2$ von 4 auf 2. Es folgen nun die 10 vierfachen Kranzprodukte in der Reihenfolge ihres Auftretens im Tabellenwerk (Bsp. $N = 60, 72$) :

$$\mathfrak{S}_e \wr \mathfrak{S}_2 \wr \mathfrak{S}_c \wr \mathfrak{S}_2 \tag{3.124}$$

$$\mathfrak{S}_e \wr \mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_c \tag{3.125}$$

$$\mathfrak{S}_c \wr \mathfrak{S}_2 \wr \mathfrak{S}_e \wr \mathfrak{S}_2 \tag{3.126}$$

$$\mathfrak{S}_c \wr \mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_e \tag{3.127}$$

$$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_e \wr \mathfrak{S}_c \tag{3.128}$$

$$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_c \wr \mathfrak{S}_e \tag{3.129}$$

$$\mathfrak{S}_2 \wr \mathfrak{S}_c \wr \mathfrak{S}_e \wr \mathfrak{S}_2 \tag{3.130}$$

$$\mathfrak{S}_2 \wr \mathfrak{S}_c \wr \mathfrak{S}_2 \wr \mathfrak{S}_e \tag{3.131}$$

$$\mathfrak{S}_2 \wr \mathfrak{S}_e \wr \mathfrak{S}_c \wr \mathfrak{S}_2 \tag{3.132}$$

$$\mathfrak{S}_2 \wr \mathfrak{S}_e \wr \mathfrak{S}_2 \wr \mathfrak{S}_c. \tag{3.133}$$

Beweis. Der Beweis ergibt sich durch Anwendung der im Kapitel 2 „Vererbung von zyklischen Codes und ihren Automorphismengruppen“ bewiesenen Sätze. □

3.4 Selbstduale Codes

Zunächst wollen wir die in dem obigen Satz 1.16 gemachte Existenzaussage zum Selbstdualen Code noch einmal umformulieren:
Zu jeder geraden Codelänge $N = 2 \cdot l$ existiert genau ein zyklischer selbstdualer Code C_l (mit der Dimension $k = l = \frac{N}{2}$) mit der Automorphismengruppe $Aut(C_l) = \mathfrak{S}_2 \wr \mathfrak{S}_l$.

Beim Studium der umfangreichen Listen der gerechneten Codes fiel mir folgendes Phänomen auf:

So gibt es bei den meisten geraden Codelängen immer nur einen Code mit der Dimension $k = \frac{N}{2}$, der nach dem Satz 1.16 dann auch selbstdual ist; aber bei einigen Codelängen ($N = 14$, 28, 30, 40, 42, 46, 56, 60, 62, 70, 90, 138, etc.) mit vergleichsweise vielen Codes gibt es mehrere Codes mit der Dimension $k = \frac{N}{2}$, von denen einige, aber nicht immer alle selbstdual sind, wie das folgende Beispiel auf der nächsten Seite für die Codelänge $N = 42$ zeigt.
Das heißt, die Voraussetzung $k = \frac{N}{2}$ für die Selbstdualität eines zyklischen Codes ist zwar notwendig, aber nicht hinreichend.
Die Eigenschaft eines zyklischen Codes, selbstdual zu sein, ist anscheinend von seiner zugehörigen Automorphismengruppe abhängig. So finden wir zumindest in dem folgenden Beispiel, daß alle Codes mit $k = \frac{N}{2}$, die zu einer bestimmten Automorphismengruppe gehören, entweder sämtlich selbstdual sind, oder sämtlich nicht-selbstdual sind.
Die nähere Untersuchung dieser Codes kommt zu folgendem Ergebnis:

1. alle Codelängen mit mehr als einem selbstdualen Code besitzen eine spezielle Permutationsgruppe (z.B. $PSL(r, s)$, M23, metazyklische Gruppe), die auch in den Automorphismengruppen zu den selbstdualen Codes involviert ist. Ein Blick in die Tabelle im Anhang B bestätigt diese Aussage.

2. umgekehrt gilt auch: besitzt eine gerade Codelänge eine spezielle Permutationsgruppe, die in den Automorphismengruppen auftritt, so hat sie weitere selbstduale Codes.

3. diese zusätzlichen selbstdualen Codes treten stets in gerader Anzahl auf, d.h. die Gesamtheit der Codes (und auch der selbstdualen Codes) ist für gerade Codelängen stets eine ungerade Zahl (s. a. Folgerung 1.17).

4. diese zusätzlichen selbstdualen Codes treten stets in Pärchen (oder Paketen von 6, 18, 48, etc. Codes) auf, wobei je zwei (oder 6, 18, 48, etc.) Codes zu derselben Automorphismengruppe gehören und überdies noch dieselbe Minimaldistanz $d > 2$ besitzen (d gerade) und jeweils untereinander isomorph sind. Die Größe der Pakete ändert sich sprunghaft mit zunehmendem r bei $PSL(r, 2)$. Wir werden das an späterer Stelle noch näher untersuchen (s. Kapitel 0.1 „Isomorphien von Codes“).

5. diese zusätzlichen selbstdualen Codes vererben ihre Eigenschaft der Selbstdualität auf die Vielfachen ihrer Codelänge. Hier ein Beispiel:

So gibt es 2 zusätzliche selbstduale Codes für $N = 14$ mit der Automorphismengruppe

$$PSL(3,2) \wr \mathfrak{S}_2,$$

und wiederum 2 zusätzliche selbstduale Codes für $N = 28$ mit der Automorphismengruppe

$$PSL(3,2) \wr \mathfrak{S}_2 \wr \mathfrak{S}_2,$$

sowie wiederum 2 zusätzliche selbstduale Codes für $N = 42$ mit der Automorphismengruppe

$$PSL(3,2) \wr \mathfrak{S}_2 \wr \mathfrak{S}_3,$$

usw.
Im Tabellenwerk des Anhangs kann man dieses Beispiel noch über $N = 56$ bis $N = 70$ verfolgen.

6. Für die Mathieu-Gruppe $M23$, sowie für die Spezialgruppen $PSL(r,2)$, r ungerade[7] konnte im Bereich der Untersuchung noch folgendes festgestellt werden:
ist die Codelänge $N = 2 \cdot l$ und l ist die Kardinalität der Menge Ω, auf der die spezielle Permutationsgruppe transitiv operiert, so existieren selbstduale Codes der Dimension $k = l$ mit der Automorphismengruppe

$$Spezialgruppe \wr \mathfrak{S}_2 \tag{3.134}$$

Sinngemäß finden wir das gleiche für die Spezialgruppe $PSL(3,4)$ bei $N = 42$, sowie für $\mathfrak{MZ}(7,3)$ bei $N = 70$.

7. Darüberhinaus treten im Zusammenhang mit den Spezialgruppen $PSL(r,2)$ für $r \geq 4$ noch selbstduale Codes mit einer Automorphismengruppe
$Aut(C) \cong (\mathfrak{S}_2 \wr PSL(r,2))/\mathfrak{S}_2^y$ auf. Mehr dazu später im Abschnitt 10.2.

8. gerade Codelängen ohne Spezialgruppe haben nur den einen selbstdualen Code C_l mit der Minimaldistanz $d = 2$, wie in Satz 1.16 beschrieben.

[7] diese Einschränkung wird klar, wenn wir uns den Untermodulverband z.B. von $PSL(4,2)$ ansehen (s. dazu Abschnitt 10.2).

Beispiel 3.28 ($N = 42$ **Liste der selbstdualen Codes)**

```
Zyklische Codes der Laenge N = 42

Lfd.Nr.  k   d     selbstdual          #AutoGrp

   1    40   2             52205687439859162185381835702272000000000
   2     2  21             52205687439859162185381835702272000000000
 ......................
 ......................
 576    20   4                       129024
 577    22   6                        12096
 578    20   6                        12096
 579    22   2           10714547155728479551488000000
 580    20   4           10714547155728479551488000000
 581    21   2        ja 10714547155728479551488000000
 582    21   4        ja   1079187553124352
 583    21   4        ja   1079187553124352          isomorph zu Nr. 582
 584    21   4      nein            129024
 585    21   6      nein            129024
 586    21   6      nein            129024          isomorph zu Nr. 585
 587    21   4      nein            129024          isomorph zu Nr. 584
 588    21   4      nein           4128768
 589    21   4      nein           4128768
 590    21   4      nein           4128768          isomorph zu Nr. 589
 591    21   4      nein           4128768          isomorph zu Nr. 588
 592    21   6      nein            120960
 593    21   4      nein            120960
 594    21   8        ja         4877107200
 595    21   4      nein            120960          isomorph zu Nr. 593
 596    21   6      nein            120960          isomorph zu Nr. 592
 597    21   8        ja         4877107200          isomorph zu Nr. 594
 598    21   6      nein             64512
 599    21   8      nein             64512
 600    21   4        ja      1541054398464
 601    21   6        ja              8064
 602    21   6      nein             64512          isomorph zu Nr. 598
 603    21   8      nein             64512          isomorph zu Nr. 599
 604    21   6        ja              8064          isomorph zu Nr. 601
 605    21   4        ja      1541054398464          isomorph zu Nr. 600

Es wurden 605 verschiedene Codes gefunden (davon 9 selbstdual)
abzueglich der Codes, bei denen die Automorphismengruppe aufloesbar ist,
oder gleich der alternierenden oder der symmetrischen Gruppe vom Grad 42 ist
```

3.5 Zyklische Codes gerader Länge (mit Spezialgruppen)

Für die doppelte Codelänge der Zahlen $l = 7$, 15, 23, 31, 63, 73, etc. tritt neben der bislang behandelten Permutationsgruppe $\mathfrak{S}_l$ noch jeweils eine weitere Permutationsgruppe als Faktor in unseren Automorphismengruppen auf, nämlich die $PSL(3,2) \cong PSL(2,7)$, $PSL(4,2) \cong \mathfrak{A}_8$, $M23$, $PSL(5,2)$, etc. [8]
Dadurch ergeben sich folgende zusätzliche Kranzprodukte, z.B. für $N = 14$:

$$\mathfrak{S}_2 \wr PSL(3,2) \tag{3.135}$$

$$PSL(3,2) \wr \mathfrak{S}_2 \tag{3.136}$$

dabei wird (für $l = 7$ und 23) ersteres von 8 Codes angenommen, das zweite von 6 Codes.
Für $l = 15$, bzw. 31 erhöhen sich diese Häufigkeiten um ein ganzes Vielfaches[9]:
bei $l = 15$ sind es 16 und 12 Codes,
bei $l = 31$ sind es 72 und 54 Codes.
Für den beobachteten Bereich fanden sich für l prim (also $l \neq 15$) in den Codes zur zweiten Automorphismengruppe zusätzliche selbstduale Codes (s. dazu auch Abschnitt 3.4).

Bemerkung 3.29
Anders, als bei den Symmetrischen Permutationsgruppen, bei denen der Index stets die Anzahl $|\Omega|$ der Elemente angibt, auf der die Permutationsgruppe operiert (Kardinalität), müssen wir hier bei diesen Spezialgruppen die Kardinalität $|\Omega|$ genau untersuchen, um das Kranzprodukt richtig konstruieren zu können. So hat man beim Betrachten der Kompositionsliste in der **Magma**-Ausgabe bei dem obigen zweiten Beispiel für $N = 14$ durchaus den Eindruck, dies sei das Kranzprodukt $\mathfrak{S}_2 \wr PSL(2,7)$. Dieses hätte aber die Ordnung 43008 und wäre damit doppelt so groß. Der Grund liegt darin, daß die Gruppe $PSL(2,7)$ den Permutationsgrad 8 hat. Wir müssen also eine zu $PSL(2,7)$ isomorphe Permutationsgruppe mit dem Permutationsgrad 7 suchen. Mit der Spezialgruppe $PSL(3,2)$ haben wir diese gefunden.
In der Definition des Kranzprodukts 0.31 ist dies die Permutationsgruppe $\mathfrak{H}$. Die Anzahl $|\Omega|$ gibt an, wie oft die Gruppe $\mathfrak{G}$ (hier die $\mathfrak{S}_2$) als Kopie in dem Kranz auftritt.
Ende der Bemerkung

Außer den oben besprochenen zwei zusätzlichen Automorphismengruppen mit Kranzproduktstruktur gibt noch eine weitere Automorphismengruppe mit einem semidirekten Produkt:

$$\underbrace{(\mathfrak{S}_2 \times \cdots \times \mathfrak{S}_2)}_{(l+1)/2-mal} \rtimes PSL(3,2). \tag{3.137}$$

Diese Automorphismengruppe wird von 4 Codes angenommen.

[8] für $N = 15$ gilt überdies noch: $\mathfrak{A}_8 \cong PSL(4,2)$. Die Formeln 3.136 und 3.135 gelten sinngemäß auch dafür, nicht jedoch die Formeln 3.137 und 3.139. Das wird auf der übernächsten Seite erklärt.
[9] die Ursache dafür sind Code-Isomorphien mit wachsenden Iso-Faktoren, s. Kapitel 0.1

Die Faktoren in diesem Produkt sind von links nach rechts in derselben Reihenfolge angeordnet, wie sie in der Magma-Kompositionsliste von unten nach oben auftreten - also so, wie wir das von den Kranzprodukten her gewohnt sind. Man achte auf das asymmetrische Symbol für das semidirekte Produkt: Der Normalteiler befindet sich links davon.

Man kann dieselbe Automorphismengruppe aber auch einfacher als „vermindertes“ Kranzprodukt schreiben. Insbesondere benötigen wir hier keinen Homomorphismus, wie beim semidirekten Produkt:

$$(\mathfrak{S}_2 \wr PSL(3,2))/\mathfrak{S}_2^3. \tag{3.138}$$

Für l=7, 23 und 31 finden wir auch die folgende Gesetzmäßigkeit: Es existiert die Automorphismengruppe

$$(\mathfrak{S}_2 \wr \mathit{Spezialgruppe})/\mathfrak{S}_2^{(l-1)/2}. \tag{3.139}$$

Wir werden das „verminderte“ Kranzprodukt später in der Zusammenfassung noch genauer erläutern.

Im Kapitel 8 werden wir sehen, daß für $l = 2^r - 1$, $r \geq 2$ diese Spezialgruppe die projektive spezielle lineare Gruppe $PSL(r, 2)$ ist.
Aus den Beobachtungen der Codelängen $N = 14$, 30 und 62 formulieren wir den folgenden Fakt zur Verallgemeinerung der Formel (3.138):

Fakt 3.30
Für Codelängen $N = 2 \cdot l$ mit $l = 2^r - 1$, $r \geq 3$ existiert eine Automorphismengruppe der Gestalt

$$(\mathfrak{S}_2 \wr PSL(r,2))/\mathfrak{S}_2^r. \tag{3.140}$$

Weiterhin beobachten wir, daß mit zunehmendem r auch je ein weiteres verschiedenes vermindertes Kranzprodukt als Automorphismengruppe auftritt.
Dieses interessante Phänomen wird später wegen seiner Komplexität in einem separaten Kapitel behandelt (s. Kap. 10: „Das Magische Dreieck“).

Abschließend sei zu Codelängen mit Spezialgruppen noch folgendes bemerkt:

Bemerkung 3.31
Die Anzahl von insgesamt 23 nichttrivialen zyklischen Codes für $N = 14$ und $N = 46$ scheint typisch, ist aber von der Anzahl der Untermoduln des entsprechenden G-Moduls $\mathbb{F}_2[\Omega]$ abhängig (s. a. Tabelle 3.2, weiter oben). Wir bekommen also durch die Spezialgruppen als zusätzliche Permutationsgruppen wesentlich mehr Codes, als für vergleichbare doppelte Codelängen anderer Primzahlen, dort sind es stets nur jeweils 5 Codes ($N = 10$, 22, 26, 34, 38, 58).
Für andere Codelängen in diesem Zusammenhang ist statt der Gruppe $PSL(3, 2)$ in den obigen Gruppenprodukten die jeweils entsprechende spezielle Permutationsgruppe einzusetzen, also z.B. für $N = 46$ wäre es die Gruppe M23, für $N = 62$ die Gruppe $PSL(5, 2)$,

oder für $N = 146$ wäre es die Gruppe $PSL(3,8) \rtimes \mathfrak{Z}_3$.
Ende der Bemerkung

Gerade die zuletzt genannte Codelänge $N = 146$ mit 19683 Rohcodes ist mit **Magma** nicht mehr in einem geschlossenen Programmdurchlauf auswertbar: Man findet wohl zu Beginn erwartungsgemäß die Automorphismengruppen $\mathfrak{S}_{73} \wr \mathfrak{S}_2$, sowie $\mathfrak{S}_2 \wr (PSL(3,8) \rtimes \mathfrak{Z}_3)$, aber danach stößt die Berechnung der jeweiligen Automorphismengruppe an die Grenzen.
Da wir jedoch genauso viele Untermoduln beim $(PSL(3,8) \rtimes \mathfrak{Z}_3)$-Modul $\mathbb{F}_2[\Omega]$ haben, wie beim $PSL(5,2)$-Modul $\mathbb{F}_2[\Theta]$ (s. a. Tabelle 3.2, weiter oben), erwarten wir eine gleichartige Landschaft der Codes und Automorphismengruppen, wie für $N = 62$, nur mit anderen Attributen k, d.
Das heißt, wir erwarten die folgenden 7 Automorphismengruppen:

1. $\mathfrak{S}_{73} \wr \mathfrak{S}_2$,
2. $\mathfrak{S}_2 \wr (PSL(3,8) \rtimes \mathfrak{Z}_3)$,
3. $(\mathfrak{S}_2 \wr (PSL(3,8) \rtimes \mathfrak{Z}_3))/\mathfrak{S}_2^{45}$,
4. $(\mathfrak{S}_2 \wr (PSL(3,8) \rtimes \mathfrak{Z}_3))/\mathfrak{S}_2^{36}$,
5. $(\mathfrak{S}_2 \wr (PSL(3,8) \rtimes \mathfrak{Z}_3))/\mathfrak{S}_2^{27}$,
6. $(PSL(3,8) \rtimes \mathfrak{Z}_3) \wr \mathfrak{S}_2$,
7. $\mathfrak{S}_2 \wr \mathfrak{S}_{73}$

Daher sei hier auf die detaillierten Ausführungen im Kapitel 10 verwiesen.

Kapitel 4

Test

In diesem Kapitel wollen wir abschließend die herausgefundenen Gesetzmäßigkeiten auf Praktikabilität überprüfen.
Dazu wollen wir versuchen, die Codes und die Automorphismengruppen für eine bestimmte Codelänge vorherzusagen. Das Beispiel sollte nicht zu trivial, aber dennoch überschaubar sein. Wir wählen $N = 66$ und folgen den Ausführungen im Abschnitt 3 „Zusammenfassung zyklische Codes“.
Dazu sind alle Faktorenzerlegungen zu beachten – zuerst die in zwei Faktoren (Punkte 1 bis 8) und danach die in drei Faktoren (die in den beiden Listen gefundenen tatsächlichen Codes und Automorphismengruppen geben wir mit ihren laufenden Nummern in Klammern an):

1. $N = 2 \cdot 33$. Nach Satz 3.1, Punkte 1, 5, 6, 7 ist also $k = 2$ und $d = 33$.
   Als zugehörige Automorphismengruppe erwarten wir $\mathfrak{S}_{33} \wr \mathfrak{S}_2$ (1). Wir erwarten also folgende 2 Codes:
   (a) einen $[66, 2, 33]$-Code (2),
   (b) sowie den dazu dualen $[66, 64, 2]$-Code (1).
2. $N = 33 \cdot 2$. Nach Satz 3.1, Punkte 1, 5, 6, 8, 9 ist also $k = 33$ und $d = 2$.
   Als zugehörige Automorphismengruppe erwarten wir $\mathfrak{S}_2 \wr \mathfrak{S}_{33}$ (24).
   Wir erwarten also folgende 3 Codes:
   (a) einen selbstdualen $[66, 33, 2]$-Code (77).
   (b) Nach Punkt 8 erwarten wir zusätzlich noch einen $[66, 32, 4]$-Code (76),
   (c) sowie den dazu dualen $[66, 34, 2]$-Code (75)
   zur selben Automorphismengruppe.
3. $N = 3 \cdot 22$. Nach Satz 3.1, Punkte 1, 5, 6, 8 ist also $k = 3$ und $d = 22$.
   Als zugehörige Automorphismengruppe erwarten wir $\mathfrak{S}_{22} \wr \mathfrak{S}_3$ (2).
   Wir erwarten also folgende 4 Codes:
   (a) einen $[66, 3, 22]$-Code (6),

(b) sowie den dazu dualen $[66, 63, 2]$-Code (5).

(c) Nach Punkt 8 erwarten wir zusätzlich noch einen $[66, 2, 44]$-Code (4),

(d) sowie den dazu dualen $[66, 64, 2]$-Code (3)
zur selben Automorphismengruppe.

4. $N = 22 \cdot 3$. Nach Satz 3.1, Punkte 1, 5, 6, 8 ist also $k = 22$ und $d = 3$.
Als zugehörige Automorphismengruppe erwarten wir $\mathfrak{S}_3 \wr \mathfrak{S}_{22}$ (13).
Wir erwarten also folgende 4 Codes:

(a) einen $[66, 22, 3]$-Code (42),

(b) sowie den dazu dualen $[66, 44, 2]$-Code (41).

(c) Nach Punkt 8 erwarten wir zusätzlich noch einen $[66, 21, 6]$-Code (40),

(d) sowie den dazu dualen $[66, 45, 2]$-Code (39)
zur selben Automorphismengruppe.

5. $N = 6 \cdot 11$. Nach Satz 3.1, Punkte 1, 5, 6, 8 ist also $k = 6$ und $d = 11$.
Als zugehörige Automorphismengruppe erwarten wir $\mathfrak{S}_{11} \wr \mathfrak{S}_6$ (5).
Wir erwarten also folgende 4 Codes:

(a) einen $[66, 6, 11]$-Code (14),

(b) sowie den dazu dualen $[66, 60, 2]$-Code (13).

(c) Nach Punkt 8 erwarten wir zusätzlich noch einen $[66, 5, 22]$-Code (12),

(d) sowie den dazu dualen $[66, 61, 2]$-Code (11)
zur selben Automorphismengruppe.

6. $N = 11 \cdot 6$. Nach Satz 3.1, Punkte 1, 5, 6, 8 ist also $k = 11$ und $d = 6$.
Als zugehörige Automorphismengruppe erwarten wir $\mathfrak{S}_6 \wr \mathfrak{S}_{11}$ (6).
Wir erwarten also folgende 4 Codes:

(a) einen $[66, 11, 6]$-Code (18),

(b) sowie den dazu dualen $[66, 55, 2]$-Code (17).

(c) Nach Punkt 8 erwarten wir zusätzlich noch einen $[66, 10, 12]$-Code (16),

(d) sowie den dazu dualen $[66, 56, 2]$-Code (15)
zur selben Automorphismengruppe.

7. $N = 6 \cdot 11$. Nach Satz 3.3, Punkte 1 bis 4 ist also $a = 6$ und $b = 11$.
Als zugehörige Automorphismengruppe erwarten wir $\mathfrak{S}_{11} \times \mathfrak{S}_6$ (11).
Wir erwarten also folgende 4 Codes:

(a) einen $[66, 16, 6]$-Code (32),

(b) sowie den dazu dualen $4[66, 50, 4]$-Code (31).

(c) Nach Punkt 3, 4 erwarten wir zusätzlich noch einen $[66, 15, 6]$-Code (30),

(d) sowie den dazu dualen $[66, 51, 4]$-Code (29)
zur selben Automorphismengruppe.

8. $N = 3 \cdot 22$. Nach Satz 3.3, Punkte 1 bis 4 ist also $a = 3$ und $b = 22$.
Als zugehörige Automorphismengruppe erwarten wir $\mathfrak{S}_3 \times \mathfrak{S}_{22}$ (17).
Wir erwarten also folgende 4 Codes:

(a) einen $[66, 24, 3]$-Code (58),

(b) sowie den dazu dualen $[66, 42, 4]$-Code (57).

(c) Nach Punkt 3, 4 erwarten wir zusätzlich noch einen $[66, 23, 6]$-Code (50),

(d) sowie den dazu dualen $[66, 43, 4]$-Code (49)
zur selben Automorphismengruppe.

Soweit die Zerlegungen in zwei Faktoren.
Es folgen die Zerlegungen in drei Faktoren.

9. $N = 11 \cdot 3 \cdot 2$. Nach Satz 3.19, Punkt 1 ist also $a = 2$, $b = 3$ und $c = 11$.
Als zugehörige Automorphismengruppe erwarten wir $\mathfrak{S}_{11} \wr \mathfrak{S}_3 \wr \mathfrak{S}_2$ (3).
Außerdem ist $x = 11, y = 3$ und $z = 2$. Nach dem Satz gilt $d = 2x = 22$ und $k = 4$.
Wir erwarten also folgende 2 Codes:

(a) einen $[66, 4, 22]$-Code (8),

(b) sowie den dazu dualen $[66, 62, 2]$-Code (7).

10. $N = 11 \cdot 2 \cdot 3$. Nach Satz 3.19, Punkt 1 ist also $a = 2, b = 3$ und $c = 11$.
Als zugehörige Automorphismengruppe erwarten wir $\mathfrak{S}_{11} \wr \mathfrak{S}_2 \wr \mathfrak{S}_3$ (4).
Außerdem ist $x = 11, y = 2$ und $z = 3$. Nach dem Satz gilt $d = 2x = 22$ und $k = 4$.
Wir erwarten also folgende 2 Codes:

(a) einen $[66, 4, 22]$-Code (10),

(b) sowie den dazu dualen $[66, 62, 2]$-Code (9).

11. $N = 3 \cdot 2 \cdot 11$. Nach Satz 3.19, Punkt 1 ist also $a = 2, b = 3$ und $c = 11$.
Als zugehörige Automorphismengruppe erwarten wir $\mathfrak{S}_3 \wr \mathfrak{S}_2 \wr \mathfrak{S}_{11}$ (8).
Außerdem ist $x = 3, y = 2$ und $z = 11$. Nach dem Satz gilt $d = 2x = 6$ und $k = 12$.
Wir erwarten also folgende 2 Codes:

(a) einen $[66, 12, 6]$-Code (22),

(b) sowie den dazu dualen $[66, 54, 2]$-Code (21).

12. $N = 3 \cdot 11 \cdot 2$. Nach Satz 3.19, Punkt 1 ist also $a = 2, b = 3$ und $c = 11$.
Als zugehörige Automorphismengruppe erwarten wir $\mathfrak{S}_3 \wr \mathfrak{S}_{11} \wr \mathfrak{S}_2$ (12).
Außerdem ist $x = 3, y = 11$ und $z = 2$. Nach dem Satz gilt $d = 2x = 6$ und $k = 20$.
Wir erwarten also folgende 2 Codes:

(a) einen $[66, 20, 6]$-Code (34),

(b) sowie den dazu dualen $[66, 46, 2]$-Code (33).

13. $N = 2 \cdot 3 \cdot 11$. Nach Satz 3.19, Punkt 1 ist also $a = 2, b = 3$ und $c = 11$.
Als zugehörige Automorphismengruppe erwarten wir $\mathfrak{S}_2 \wr \mathfrak{S}_3 \wr \mathfrak{S}_{11}$ (14).
Außerdem ist $x = 2, y = 3$ und $z = 11$. Nach dem Satz gilt $d = 2x = 4$ und $k = 22$.
Wir erwarten also folgende 4 Codes:

(a) einen $[66, 22, 4]$-Code (44),

(b) sowie den dazu dualen $[66, 44, 2]$-Code (43).

(c) Wegen $a = x = 2$ erwarten wir noch zusätzlich einen $[66, 23, 4]$-Code (52),

(d) sowie den dazu dualen $[66, 43, 2]$-Code (51).

14. $N = 2 \cdot 11 \cdot 3$. Nach Satz 3.19, Punkt 1 ist also $a = 2, b = 3$ und $c = 11$.
Als zugehörige Automorphismengruppe erwarten wir $\mathfrak{S}_2 \wr \mathfrak{S}_{11} \wr \mathfrak{S}_3$ (22).
Außerdem ist $x = 2, y = 11$ und $z = 3$. Nach dem Satz gilt $d = 2x = 4$ und $k = 30$.
Wir erwarten also folgende 4 Codes:

(a) einen $[66, 30, 4]$-Code (70),

(b) sowie den dazu dualen $[66, 36, 2]$-Code (69).

(c) Wegen $a = x = 2$ erwarten wir noch zusätzlich einen $[66, 31, 4]$-Code (72),

(d) sowie den dazu dualen $[66, 35, 2]$-Code (71).

Nun wollen wir noch überprüfen, ob für die Zerlegungen in drei Faktoren verminderte Kranzprodukte zu erwarten sind.

15. $N = 2 \cdot 3 \cdot 11$. Nach Satz 3.20, Teil 1 ist also $b = 3$ und $c = 11$.
Als zugehörige Automorphismengruppe erwarten wir $(\mathfrak{S}_2 \wr \mathfrak{S}_3 \wr \mathfrak{S}_{11})/\mathfrak{S}_2^{10}$ (19).
Nach dem Satz gilt $k = 33 - 11 + 2 = 24$.
Wir erwarten also folgende 2 Codes:

(a) einen $[66, 24, 4]$-Code (56),

(b) sowie den dazu dualen $[66, 42, 4]$-Code (55).

16. $N = 2 \cdot 3 \cdot 11$. Nach Satz 3.20, Teil 2 ist also $b = 3$ und $c = 11$.
Als zugehörige Automorphismengruppe erwarten wir $(\mathfrak{S}_2 \wr \mathfrak{S}_{11} \wr \mathfrak{S}_3)/\mathfrak{S}_2^2$ (23).
Nach dem Satz gilt $k = 33 - 3 + 2 = 32$.
Wir erwarten also folgende 2 Codes:

(a) einen $[66, 32, 4]$-Code (74),

(b) sowie den dazu dualen $[66, 34, 4]$-Code (73).

Damit sind bislang die Attribute (k, d) von 49 Codes (von insgesamt 77) vorhergesagt worden.

Nun wollen wir noch überprüfen, ob für die Zerlegungen in drei Faktoren gemischte Produkte zu erwarten sind.

17. $N = 2 \cdot 3 \cdot 11$. Nach Satz 3.23, Punkt 1 ist also $b = 3$ und $c = 11$, sowie $a = 2$.
Als zugehörige Automorphismengruppe erwarten wir $\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_{11})$ (7).
Wir erwarten also folgende 8 Codes:
    (a) einen $[N, c + b - 2, 2ab]$ - Code, also einen $[66, 12, 12]$ - Code (20),
    (b) sowie den dazu dualen $[66, 54, 2]$-Code (19).
    (c) einen $[N, c + b - 1, ab]$ - Code, also einen $[66, 13, 6]$ - Code (24),
    (d) sowie den dazu dualen $[66, 53, 2]$-Code (23).
    (e) einen $[N, (b - 1)(c - 1), 4a]$ - Code, also einen $[66, 20, 8]$ - Code (36),
    (f) sowie den dazu dualen $[66, 46, 2]$-Code (35).
    (g) einen $[N, (b - 1)(c - 1) + 1, 4a]$ - Code, also einen $[66, 21, 8]$ - Code (38),
    (h) sowie den dazu dualen $[66, 45, 2]$-Code (37).

18. $N = 2 \cdot 3 \cdot 11$. Nach Satz 3.23, Punkt 2 ist also $b = 3$ und $c = 11$, sowie $a = 2$.
Als zugehörige Automorphismengruppe erwarten wir $(\mathfrak{S}_3 \times \mathfrak{S}_{11}) \wr \mathfrak{S}_2$ (18).
Wir erwarten also folgende 6 Codes:
    (a) einen $[N, a(c + b - 1) - 2, 2b]$ - Code, also einen $[66, 24, 6]$ - Code (54),
    (b) sowie den dazu dualen $[66, 42, 4]$-Code (53).
    (c) einen $[N, a(c + b - 1) - 1, 2b]$ - Code, also einen $[66, 25, 6]$ - Code (64),
    (d) sowie den dazu dualen $[66, 41, 4]$-Code (63).
    (e) einen $[N, a(c+b-1), b]$ - Code, also einen $[66, 26, 3]$ - Code (66), sowie den dazu dualen $[66, 40, 4]$-Code (65).

19. $N = 2 \cdot 3 \cdot 11$. Nach Satz 3.23, Punkt 3 ist also $b = 3$ und $c = 11$, sowie $a = 2$.
Als zugehörige Automorphismengruppe erwarten wir $(\mathfrak{S}_3 \wr \mathfrak{S}_2) \times \mathfrak{S}_{11}$ (10).
Wir erwarten also folgende 2 Codes:
    (a) einen $[N, c - 3 + 2b, d]$ - Code, also einen $[66, 14, 12]$ - Code (28),
    (b) sowie den dazu dualen $[66, 52, 4]$-Code (27).

20. $N = 2 \cdot 3 \cdot 11$. Nach Satz 3.23, Punkt 4 ist also $b = 3$ und $c = 11$, sowie $a = 2$.
Als zugehörige Automorphismengruppe erwarten wir $(\mathfrak{S}_2 \wr \mathfrak{S}_3) \times \mathfrak{S}_{11}$ (21).
Wir erwarten also folgende 2 Codes:
    (a) einen $[N, c(b - 1) + b + 1, 4]$ - Code, also einen $[66, 26, 4]$ - Code (68),

(b) sowie den dazu dualen $[66, 40, 4]$-Code (67).

21. $N = 2 \cdot 3 \cdot 11$. Nach Satz 3.23, Punkt 5 ist also $b = 3$ und $c = 11$.
Als zugehörige Automorphismengruppe erwarten wir $(\mathfrak{S}_{11} \wr \mathfrak{S}_2) \times \mathfrak{S}_3$ (15).
Wir erwarten also folgende 2 Codes:

(a) einen $[N, 2c + b - 3, 2b]$ - Code, also einen $[66, 22, 6]$ - Code (46),

(b) sowie den dazu dualen $[66, 44, 4]$-Code (45).

22. $N = 2 \cdot 3 \cdot 11$. Nach Satz 3.23, Punkt 6 ist also $b = 3$ und $c = 11$.
Als zugehörige Automorphismengruppe erwarten wir $(\mathfrak{S}_2 \wr \mathfrak{S}_{11}) \times \mathfrak{S}_3$ (20).
Wir erwarten also folgende 2 Codes:

(a) einen $[N, (c + 1)(b - 1), 4]$ - Code, also einen $[66, 24, 4]$ - Code (60),

(b) sowie den dazu dualen $[66, 42, 3]$-Code (59).

23. $N = 2 \cdot 3 \cdot 11$. Nach Satz 3.23, Punkt 7 ist also $b = 3$ und $c = 11$.
Als zugehörige Automorphismengruppe erwarten wir $(\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_{11}))/\mathfrak{S}_2^{12}$ (16).
Wir erwarten also folgende 2 Codes:

(a) einen $[N, 2c, 8]$ - Code, also einen $[66, 22, 8]$ - Code (48),

(b) sowie den dazu dualen $[66, 44, 4]$-Code (47).

24. $N = 2 \cdot 3 \cdot 11$. Nach Satz 3.23, Punkt 8 ist also $b = 3$ und $c = 11$.
Als zugehörige Automorphismengruppe erwarten wir $\mathfrak{S}_4 \times (\mathfrak{S}_2 \wr \mathfrak{S}_{11})$ (24).
Wir erwarten also folgende 4 Codes:

(a) einen $[N, c + 3, 2b]$ - Code, also einen $[66, 14, 6]$ - Code (26),

(b) sowie den dazu dualen $[66, 52, 4]$-Code (25).

(c) einen $[N, 2c + 3, 2a]$ - Code, also einen $[66, 25, 4]$ - Code (62),

(d) sowie den dazu dualen $[66, 41, 4]$-Code (61).

Damit sind bislang alle 24 Automorphismengruppen vorhergesagt worden, sowie die Attribute (k, d) von allen 77 Codes vorhergesagt worden.

Bemerkung 4.1
Die Liste der 77 zyklischen Codes ist als Referenz auf den nächsten beiden Seiten zu finden, ebenso die Tabelle der Automorphismengruppen im Anschluß daran.
Die gleiche Konstellation (Anzahl Codes, Automorphismengruppen und deren Struktur) finden wir auch für $N = 78$ und $N = 110$ (siehe Tabellenwerk), nicht jedoch für $N = 102$, da mit $n = 17$ als Teiler noch zusätzlich die Gruppen $\mathfrak{MZ}(17, 8)$ und $PSL(2, 16)$ zur Bildung von weiteren Automorphismengruppen zur Verfügung stehen.

```
Lineare Permutations-Gruppencodes der Laenge N = 66
der zyklischen Permutationsgruppe

Lfd.Nr.  k   d     #PermGrp          #AutoGrp

   1    64   2         66 150800009738337861090715981299943973199432421729435875\
331276800000000000000
   2     2  33         66 150800009738337861090715981299943973199432421729435875\
331276800000000000000
   3    64   2         66 852022429423244793431302545961881685186295637422899200\
00000000000
   4     2  44         66 852022429423244793431302545961881685186295637422899200\
00000000000
   5    63   2         66 852022429423244793431302545961881685186295637422899200\
00000000000
   6     3  22         66 852022429423244793431302545961881685186295637422899200\
00000000000
   7    62   2         66 291250583854141696973485095442710528000000000000000
   8     4  22         66 291250583854141696973485095442710528000000000000000
   9    62   2         66 194167055902761131315656730295140352000000000000000
  10     4  22         66 194167055902761131315656730295140352000000000000000
  11    61   2         66 2912505838541416969734850954427105280000000000000000
  12     5  22         66 2912505838541416969734850954427105280000000000000000
  13    60   2         66 2912505838541416969734850954427105280000000000000000
  14     6  11         66 2912505838541416969734850954427105280000000000000000
  15    56   2         66 1076002248280270605165527040000000000000000
  16    10  12         66 1076002248280270605165527040000000000000000
  17    55   2         66 1076002248280270605165527040000000000000000
  18    11   6         66 1076002248280270605165527040000000000000000
  19    54   2         66 2057296206731673600
  20    12  12         66 2057296206731673600
  21    54   2         66 107600224828027060516552704000000000000
  22    12   6         66 107600224828027060516552704000000000000
  23    53   2         66 2057296206731673600
  24    13   6         66 2057296206731673600
  25    52   4         66       1961990553600
  26    14   6         66       1961990553600
  27    52   4         66          2874009600
  28    14  12         66          2874009600
  29    51   4         66         28740096000
  30    15   6         66         28740096000
  31    50   4         66         28740096000
  32    16   6         66         28740096000
  33    46   2         66 419439126407752985276087009280000
  34    20   6         66 419439126407752985276087009280000
  35    46   2         66 2057296206731673600
  36    20   8         66 2057296206731673600
  37    45   2         66 2057296206731673600
```

```
  38    21   8          66 2057296206731673600
  39    45   2          66 14794289091003700195464030556520448000 0
  40    21   6          66 14794289091003700195464030556520448000 0
  41    44   2          66 14794289091003700195464030556520448000 0
  42    22   3          66 14794289091003700195464030556520448000 0
  43    44   2          66 12439683452036976067215360 0
  44    22   4          66 12439683452036976067215360 0
  45    44   4          66  19120211066880000
  46    22   6          66  19120211066880000
  47    44   4          66    502269581721600
  48    22   8          66    502269581721600
  49    43   4          66 6744004366665646080000
  50    23   6          66 6744004366665646080000
  51    43   2          66 12439683452036976067215360 0
  52    23   4          66 12439683452036976067215360 0
  53    42   4          66 114721266401280000
  54    24   6          66 114721266401280000
  55    42   4          66 12148128371129859440640 0
  56    24   4          66 12148128371129859440640 0
  57    42   4          66 6744004366665646080000
  58    24   3          66 6744004366665646080000
  59    42   3          66       490497638400
  60    24   4          66       490497638400
  61    41   4          66      1961990553600
  62    25   4          66      1961990553600
  63    41   4          66 114721266401280000
  64    25   6          66 114721266401280000
  65    40   4          66 114721266401280000
  66    26   3          66 114721266401280000
  67    40   4          66         1916006400
  68    26   4          66         1916006400
  69    36   2          66 3277994808316765826778660864000000
  70    30   4          66 3277994808316765826778660864000000
  71    35   2          66 3277994808316765826778660864000000
  72    31   4          66 3277994808316765826778660864000000
  73    34   4          66 8194987020791914566946652160000 00
  74    32   4          66 8194987020791914566946652160000 00
  75    34   2          66 7458913038715529374862939105293580107776000000 00
  76    32   4          66 7458913038715529374862939105293580107776000000 00
  77    33   2          66 7458913038715529374862939105293580107776000000 00

Es wurden 77 verschiedene Codes gefunden
abzueglich der Codes, bei denen die Automorphismengruppe aufloesbar ist,
oder gleich der alternierenden oder der symmetrischen Gruppe vom Grad 66 ist

CPU Zeit = 1.020 Sekunden
```

Nr.	Ordnung	Anz.	F.-typ	Produktformel
1	150800009738337861090715981299943973 1/ 994324217294358753312768000000000000000	2	(1.18)	$\mathfrak{S}_{33} \wr \mathfrak{S}_2$
2	852022429423244793431302545961 88/ 168518629563742289920000000000000	4	(1.74)	$\mathfrak{S}_{22} \wr \mathfrak{S}_3$
3	$291250583854141696973485095442710528*10^{12}$	2	(1.85)	$\mathfrak{S}_{11} \wr \mathfrak{S}_3 \wr \mathfrak{S}_2$
4	$194167055902761131315656730295140352*10^{12}$	2	(1.84)	$\mathfrak{S}_{11} \wr \mathfrak{S}_2 \wr \mathfrak{S}_3$
5	$291250583854141696973485095442710528*10^{13}$	4	(1.79)	$\mathfrak{S}_{11} \wr \mathfrak{S}_6$
6	10760022482802706051655270400000000000000	4	(1.78)	$\mathfrak{S}_6 \wr \mathfrak{S}_{11}$
7	2057296206731673600	8	(3.80)	$\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_{11})$
8	1076002248280270605165527040000	2	(1.82)	$\mathfrak{S}_3 \wr \mathfrak{S}_2 \wr \mathfrak{S}_{11}$
9	1961990553600	4	(3.101) (3.102)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_{11}))/\mathfrak{S}_2^{20}$ $\cong \mathfrak{S}_4 \times (\mathfrak{S}_2 \wr \mathfrak{S}_{11})$
10	2874009600	2	(3.82)	$(\mathfrak{S}_3 \wr \mathfrak{S}_2) \times \mathfrak{S}_{11}$
11	28740096000	4	(1.86)	$\mathfrak{S}_6 \times \mathfrak{S}_{11}$
12	41943912640775298527608700928000 0	2	(1.83)	$\mathfrak{S}_3 \wr \mathfrak{S}_{11} \wr \mathfrak{S}_2$
13	14794289091003700195464030556520448 0000	4	(1.75)	$\mathfrak{S}_3 \wr \mathfrak{S}_{22}$
14	12439683452036976067215360 0	4	(1.80)	$\mathfrak{S}_2 \wr \mathfrak{S}_3 \wr \mathfrak{S}_{11}$
15	19120211066880000	2	(3.85)	$(\mathfrak{S}_{11} \wr \mathfrak{S}_2) \times \mathfrak{S}_3$
16	502269581721600	2	(3.100)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_{11}))/\mathfrak{S}_2^{12}$
17	6744004366665646080000	4	(1.72)	$\mathfrak{S}_3 \times \mathfrak{S}_{22}$
18	114721266401280000	6	(3.81)	$(\mathfrak{S}_3 \times \mathfrak{S}_{11}) \wr \mathfrak{S}_2$
19	121481283711298594406400	2	(3.75)	$(\mathfrak{S}_2 \wr \mathfrak{S}_3 \wr \mathfrak{S}_{11})/\mathfrak{S}_2^{10}$
20	490497638400	2	(3.87) (3.86)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_{11}))/\mathfrak{S}_2^{22}$ $\cong (\mathfrak{S}_2 \wr \mathfrak{S}_{11}) \times \mathfrak{S}_3$
21	1916006400	2	(3.84) (3.83)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_{11}))/\mathfrak{S}_2^{30}$ $\cong (\mathfrak{S}_2 \wr \mathfrak{S}_3) \times \mathfrak{S}_{11}$
22	32779948083167658267786608640 00000	4	(1.81)	$\mathfrak{S}_2 \wr \mathfrak{S}_{11} \wr \mathfrak{S}_3$
23	81949870207919145669466521600 0000	2	(3.76)	$(\mathfrak{S}_2 \wr \mathfrak{S}_{11} \wr \mathfrak{S}_3)/\mathfrak{S}_2^2$
24	745891303871552937486 29/ 391052935801077760000000	3	(1.19)	$\mathfrak{S}_2 \wr \mathfrak{S}_{33}$
	Anzahl Codes:	77		

Tabelle 4.1: Tabelle der Automorphismengruppen für N=66

Kapitel 5

Das semidirekte Gruppenprodukt

In diesem Kapitel wollen wir uns mit dem semidirekten Produkt von Gruppen beschäftigen. Neben dem Kranzprodukt und dem direkten Produkt von Gruppen tritt auch das semidirekte Produkt bei der Bildung von Automorphismengruppen zu unseren Gruppencodes auf.
Im Gegensatz zu den beiden anderen Produkttypen ist dieses wesentlich komplexer. Insbesondere ist dieses Produkt auch nicht im Computeralgebrasystem Magma implementiert. Ich möchte daher nach der theoretischen Einführung des semidirekten Produkts an einem Beispiel die Analyse einer Automorphismengruppe mit einem semidirektem Produkt aufzeigen, um danach die Synthese zu beschreiben.
Wir wollen daher dessen Definition hier voranstellen (ROTMAN [15]):

Definition 5.1 (**Komplement**)
Sei $\mathfrak{K}$ *eine (nicht notwendig normale) Untergruppe der Gruppe* $\mathfrak{G}$*. Dann heißt eine Untergruppe* $\mathfrak{Q} \leq \mathfrak{G}$ *ein* Komplement *von* $\mathfrak{K}$ *in* $\mathfrak{G}$*, falls* $\mathfrak{K} \cap \mathfrak{Q} = 1$ *und* $\mathfrak{K}\mathfrak{Q} = \mathfrak{G}$*.*

Eine Gruppe $\mathfrak{G}$ ist das direkte Produkt zweier normaler Untergruppen $\mathfrak{K}$ und $\mathfrak{Q}$, falls $\mathfrak{K} \cap \mathfrak{Q} = 1$ und $\mathfrak{K}\mathfrak{Q} = \mathfrak{G}$.

Definition 5.2 (**semidirektes Produkt**)
Eine Gruppe $\mathfrak{G}$ *ist ein* semidirektes Produkt *von* $\mathfrak{K}$ *mit* $\mathfrak{Q}$*, in Zeichen* $\mathfrak{G} = \mathfrak{K} \rtimes \mathfrak{Q}$*, falls* $\mathfrak{K} \lhd \mathfrak{G}$ *und* $\mathfrak{K}$ *besitzt ein Komplement* $\mathfrak{Q}_1 \cong \mathfrak{Q}$*.*

Wir nehmen an, daß $\mathfrak{Q}_1$ keine normale Untergruppe ist. Wäre sie es doch, so wäre $\mathfrak{G}$ das direkte Produkt von $\mathfrak{K}$ mit $\mathfrak{Q}_1$, in Zeichen $\mathfrak{G} = \mathfrak{K} \times \mathfrak{Q}_1$.

Lemma 5.3
Sei $\mathfrak{K}$ *eine normale Untergruppe der Gruppe* $\mathfrak{G}$*.*
Dann sind folgende Aussagen äquivalent:

1. $\mathfrak{G}$ *ist ein semidirektes Produkt von* $\mathfrak{K}$ *mit* $\mathfrak{G}/\mathfrak{K}$*, d.h.,* $\mathfrak{K}$ *hat ein Komplement in* $\mathfrak{G}$*;*
2. *es gibt eine Untergruppe* $\mathfrak{Q} \leq \mathfrak{G}$*, so daß jedes Element* $g \in \mathfrak{G}$ *eine eindeutige Darstellung* $g = ax$ *besitzt, mit* $a \in \mathfrak{K}$ *und* $x \in \mathfrak{Q}$*;*

3. *es existiert ein Homomorphismus* $s : \mathfrak{G}/\mathfrak{K} \to \mathfrak{G}$ *mit* $\nu s = 1_{\mathfrak{G}/\mathfrak{K}}$, *wobei* $\nu : \mathfrak{G} \to \mathfrak{G}/\mathfrak{K}$ *die natürliche Abbildung ist; und*

4. *es existiert ein Homomorphismus* $\pi : \mathfrak{G} \to \mathfrak{G}$ *mit* $ker\pi = \mathfrak{K}$ *und* $\pi(x) = x, \forall x \in im\pi$.

Beweis. Der Beweis findet sich in der Literatur [15]. □

5.1 Analyse eines semidirekten Produktes

Wegen der Übersichtlichkeit nehmen wir bewußt ein kleines Beispiel.
Für $N = 14$ finden wir als dritte Automorphismengruppe die folgende[1]:

```
3 . Automorphismen-Gruppe mit 2688 Elementen  - Haeufigkeit dieser Gruppe: 2 mal

    G
    |  A(1, 7)                = L(2, 7)
    *
    |  Cyclic(2)
    *
    |  Cyclic(2)
    *
    |  Cyclic(2)
    *
    |  Cyclic(2)
    1
```

Man sieht leicht, daß es sich hierbei nicht um ein Kranzprodukt handelt – man kann es aber auch durch **Magma** überprüfen[2]. Dann versuchen wir, ob es ein direktes Produkt ist:

$$PSL(2,7) \times (\underbrace{\mathfrak{S}_2 \times \cdots \times \mathfrak{S}_2}_{4-mal})$$

Auch das führt nicht zum Erfolg[3], allenfalls ist die Ordnung dieser Gruppe gleich.

```
> AG3:=AutoGroups[3];
> TG3:=DirectProduct(Sym(2),DirectProduct(Sym(2),DirectProduct(Sym(2),
   DirectProduct(Sym(2),PSL(2,7)))));
> #TG3;
2688
> IsIsomorphic(AG3,TG3);
false
> IsWreathProduct(AG3);
Time: 0.000
There are 1 possible wreath product factorizations of the group order.
[ <2, 7, 21> ]
*** Doing triple <2, 7, 21>
*** There are 0 potential base groups for this triple.
false
```

[1] diese Gruppe wird im größeren Zusammenhang auch im Abschnitt 3.5 behandelt.

[2] der Befehl lautet: IsWreathProduct(G3);

[3] ebensowenig, wie wenn wir in den Berechnungen $PSL(2,7)$ durch die dazu isomorphe Gruppe $PSL(3,2)$ ersetzen

Also untersuchen wir nun, ob die Konstruktion ein semidirektes Produkt enthält. Diese Analyse läuft in mehreren Schritten ab:

1. wir ermitteln alle Normalteiler der Gruppe

```
> NG:=NormalSubgroups(AG3);
> NG;
Conjugacy classes of subgroups
------------------------------

[1]     Order 1             Length 1
        Permutation group acting on a set of cardinality 14
        Order = 1
            Id($)
[2]     Order 2             Length 1
        Permutation group acting on a set of cardinality 14
        Order = 2
            Id($)
            (1, 8)(2, 9)(3, 10)(4, 11)(5, 12)(6, 13)(7, 14)
[3]     Order 8             Length 1
        Permutation group acting on a set of cardinality 14
        Order = 8 = 2^3
            Id($)
            (2, 9)(3, 10)(4, 11)(7, 14)
            (2, 9)(4, 11)(5, 12)(6, 13)
            (1, 8)(2, 9)(3, 10)(6, 13)
[4]     Order 16            Length 1
        Permutation group acting on a set of cardinality 14
        Order = 16 = 2^4
            Id($)
            (4, 11)(5, 12)(7, 14)
            (3, 10)(4, 11)(6, 13)
            (1, 8)(5, 12)(6, 13)
            (2, 9)(3, 10)(5, 12)
[5]     Order 1344          Length 1
        Permutation group acting on a set of cardinality 14
        Order = 1344 = 2^6 * 3 * 7
            (1, 3)(4, 12)(5, 11)(8, 10)
            (1, 7, 9, 5)(2, 12, 8, 14)(3, 13)(6, 10)
            (2, 9)(3, 10)(4, 11)(7, 14)
            (2, 9)(4, 11)(5, 12)(6, 13)
            (1, 8)(2, 9)(3, 10)(6, 13)
[6]     Order 2688          Length 1
        Permutation group acting on a set of cardinality 14
        Order = 2688 = 2^7 * 3 * 7
            (1, 3)(4, 5)(7, 14)(8, 10)(11, 12)
            (1, 14, 2, 5)(3, 13)(4, 11)(6, 10)(7, 9, 12, 8)
            (4, 11)(5, 12)(7, 14)
            (3, 10)(4, 11)(6, 13)
            (1, 8)(5, 12)(6, 13)
```

```
            (2, 9)(3, 10)(5, 12)
>
```

2. Wir wählen den Normalteiler mit Ordnung 16 aus und prüfen, ob er isomorph dem 4-maligen direkten Produkt der Gruppe $\mathfrak{S}_2$ ist.

```
> H16:=NG[4]‘subgroup;
> TH:=DirectProduct(Sym(2),DirectProduct(Sym(2),DirectProduct
(Sym(2),Sym(2))));
> #TH;
16
> IsIsomorphic(H16,TH);
true Homomorphism of GrpPerm: H16, Degree 14, Order 2^4 into
 GrpPerm: TH, Degree 8, Order 2^4 induced by
    Id(H16) |--> Id(TH)
    (4, 11)(5, 12)(7, 14) |--> (1, 2)
    (3, 10)(4, 11)(6, 13) |--> (3, 4)
    (1, 8)(5, 12)(6, 13) |--> (5, 6)
    (2, 9)(3, 10)(5, 12) |--> (7, 8)
>
```

3. Nun bilden wir den Quotienten aus der Automorphismengruppe und dem Normalteiler.

```
> G:=AG3/H16;
> #G;
168
```

Da die Ordnung des Quotienten (168) nicht in der Liste der Normalteiler vorkommt, sehen wir hier noch einmal zur Bestätigung, daß es sich hier bei AG3 nicht um das oben diskutierte direkte Produkt handeln kann.

4. Jetzt suchen wir eine Untergruppe von AG3 mit der Ordnung 168:

```
> L:=NonsolvableSubgroups(AG3);
> L;
Conjugacy classes of subgroups
------------------------------

[1]     Order 168          Length 8
        Permutation group acting on a set of cardinality 14
        Order = 168 = 2^3 * 3 * 7
            (1, 3)(4, 12)(5, 11)(8, 10)
            (2, 11)(3, 5, 14, 6)(4, 9)(7, 13, 10, 12)
[2]     Order 168          Length 8
        Permutation group acting on a set of cardinality 14
        Order = 168 = 2^3 * 3 * 7
            (1, 10)(2, 9)(3, 8)(4, 12)(5, 11)(6, 13)
            (1, 8)(2, 11, 9, 4)(3, 5, 14, 13)(6, 10, 12, 7)
[3]     Order 336          Length 8
```

```
        Permutation group acting on a set of cardinality 14
        Order = 336 = 2^4 * 3 * 7
            (1, 3)(4, 12)(5, 11)(8, 10)
            (1, 8)(2, 4)(3, 12, 14, 13)(5, 7, 6, 10)(9, 11)
            (1, 8)(2, 9)(3, 10)(4, 11)(5, 12)(6, 13)(7, 14)
[4]     Order 336          Length 8
        Permutation group acting on a set of cardinality 14
        Order = 336 = 2^4 * 3 * 7
            (1, 3)(4, 5)(7, 14)(8, 10)(11, 12)
            (2, 11, 9, 4)(3, 12, 7, 13)(5, 14, 6, 10)
            (1, 8)(2, 9)(3, 10)(4, 11)(5, 12)(6, 13)(7, 14)
[5]     Order 1344         Length 1
        Permutation group acting on a set of cardinality 14
        Order = 1344 = 2^6 * 3 * 7
            (1, 3)(4, 12)(5, 11)(8, 10)
            (2, 4)(3, 5, 7, 13)(6, 10, 12, 14)(9, 11)
            (2, 9)(3, 10)(4, 11)(7, 14)
            (2, 9)(4, 11)(5, 12)(6, 13)
            (1, 8)(2, 9)(3, 10)(6, 13)
[6]     Order 2688         Length 1
        Permutation group acting on a set of cardinality 14
        Order = 2688 = 2^7 * 3 * 7
            (1, 3)(4, 5)(7, 14)(8, 10)(11, 12)
            (2, 11, 9, 4)(3, 12, 7, 13)(5, 14, 6, 10)
            (4, 11)(5, 12)(7, 14)
            (3, 10)(4, 11)(6, 13)
            (1, 8)(5, 12)(6, 13)
            (2, 9)(3, 10)(5, 12)
```

5. Wir finden 2 Untergruppen der Ordnung 168. Wir wählen die erste aus und überprüfen sie auf Isomorphie mit G.

```
> K:=L[1]`subgroup;
> IsIsomorphic(G,K);
true Homomorphism of GrpPerm: G, Degree 168, Order 2^3 * 3 * 7 into
     GrpPerm: K, Degree 14, Order 2^3 * 3 * 7 induced by
    Id(G) |--> Id(K)
    ..........................
> IsIsomorphic(G,PSL(2,7));
true Homomorphism of GrpPerm: G, Degree 168, Order 2^3 * 3 * 7 into
     GrpPerm: $, Degree 8, Order 2^3 * 3 * 7 induced by
    Id(G) |--> Id($)
    ..........................
```

6. Nach Definition 5.1 müssen wir noch den folgenden Durchschnitt überprüfen:

```
> K meet H16;
Permutation group acting on a set of cardinality 14
Order = 1
>
```

7. Wir wissen jetzt, daß sich unsere Automorphismengruppe als semidirektes Produkt schreiben läßt:
$$AG3 = (\underbrace{\mathfrak{S}_2 \times \cdots \times \mathfrak{S}_2}_{4-mal}) \rtimes PSL(2,7)$$

Dabei ist die gefundene Darstellung noch mit einem Schönheitsfehler behaftet: Die von **Magma** angegebene Permutationsgruppe $PSL(2,7)$ operiert normalerweise auf einer Menge der Kardinalität 8:

```
> PSL(2,7);
Permutation group acting on a set of cardinality 8
Order = 168 = 2^3 * 3 * 7
    (3, 6, 7)(4, 5, 8)
    (1, 8, 2)(4, 5, 6)
>
```

Nun ist aber 8 kein Teiler von 14. Wie bereits früher bemerkt, existiert die zu $PSL(2,7)$ isomorphe Permutationsgruppe $PSL(3,2)$; sie operiert normalerweise auf einer Menge der Kardinalität 7:

```
> PSL(3,2);
Permutation group acting on a set of cardinality 7
Order = 168 = 2^3 * 3 * 7
    (1, 4)(6, 7)
    (1, 3, 2)(4, 7, 5)
>
```

Somit lautet jetzt die korrekte Darstellung unserer Automorphismengruppe als semidirektes Produkt:
$$AG3 = (\underbrace{\mathfrak{S}_2 \times \cdots \times \mathfrak{S}_2}_{4-mal}) \rtimes PSL(3,2),$$

oder vereinfacht geschrieben:
$$\mathfrak{S}_2^4 \rtimes PSL(3,2).$$

Bemerkung 5.4
Zum tieferen Verständnis dieser Gruppenkonstruktion sei auf die Abschnitte 5.3 und 10.2 verwiesen: Dort werden wir sehen, daß der erste Teil $(\underbrace{\mathfrak{S}_2 \times \cdots \times \mathfrak{S}_2}_{4-mal})$ des obigen semidirekten Produktes zu einem $[7,4,3]$-Code (*Hamming-Code*) gehört, der als 4-dimensionaler Untermodul des $PSL(3,2)$-Moduls $\mathbb{F}_2[\{1,2,\ldots,7\}]$ aufgefaßt wird.

5.2 Analyse eines verminderten Kranzproduktes

Im Verlaufe der Anfertigung dieser Arbeit wurde von mir das „verminderte Kranzprodukt“ entdeckt (zur Definition und Erklärung siehe 3.2.1). Wegen der Übersichtlichkeit nehmen wir bewußt dasselbe kleine Beispiel, wie im Abschnitt 5.1. Für $N = 14$ finden wir als dritte Automorphismengruppe die folgende[4]:

```
3. Automorphismen-Gruppe mit 2688 Elementen - Haeufigkeit dieser Gruppe: 2 mal

    G
    |  A(1, 7)                = L(2, 7)
    *
    |  Cyclic(2)
    *
    |  Cyclic(2)
    *
    |  Cyclic(2)
    *
    |  Cyclic(2)
    1
```

Man sieht leicht, daß es sich hierbei nicht um ein (volles) Kranzprodukt handelt – es fehlen dazu noch weitere 3 Kompositionsfaktoren „Cyclic(2)“.
Wir wollen nun durch Magma untersuchen, ob es ein vermindertes Kranzprodukt ist. Diese Analyse läuft in mehreren Schritten ab:

1. wir benötigen zunächst das volle Kranzprodukt, welches diesem vermeintlichen verminderten Kranzprodukt zugrunde liegt. Mitunter tritt dieses volle Kranzprodukt ebenfalls als Automorphismengruppe zur selben Codelänge auf, so auch in unserem Fall: Hier ist es die zweite Automorphismengruppe:

   ```
   2 .Automorphismen-Gruppe mit 21504 Elementen - Haeufigkeit dieser Gruppe: 4 mal

       G
       |  A(1, 7)                = L(2, 7)
       *
       |  Cyclic(2)
       *
       |  Cyclic(2)
       *
       |  Cyclic(2)
       *
       |  Cyclic(2)
       *
       |  Cyclic(2)
       *
       |  Cyclic(2)
       *
       |  Cyclic(2)
       1
   ```

   Falls das benötigte Kranzprodukt nicht als Automorphismengruppe zur selben Codelänge auftritt, müssen wir es konstruieren. Dabei ist mit besonderer Sorgfalt auf

[4] diese Gruppe wird im größeren Zusammenhang auch im Abschnitt 3.5 behandelt.

die Kardinalität der Menge Ω zu achten, auf der das Kranzprodukt transitiv operiert.
Hier wäre es $\mathfrak{S}_2 \wr PSL(3,2)$.

2. wir ermitteln alle Normalteiler der Gruppe des vollen Kranzprodukts

```
NG2:=NormalSubgroups(AG2);
> NG2;
Conjugacy classes of subgroups
------------------------------

[1]     Order 1             Length 1
        Permutation group acting on a set of cardinality 14
        Order = 1
            Id($)
[2]     Order 2             Length 1
        Permutation group acting on a set of cardinality 14
        Order = 2
            Id($)
            (1, 8)(2, 9)(3, 10)(4, 11)(5, 12)(6, 13)(7, 14)
[3]     Order 8             Length 1
        Permutation group acting on a set of cardinality 14
        Order = 8 = 2^3
            Id($)
            (1, 8)(2, 9)(5, 12)(7, 14)
            (2, 9)(3, 10)(4, 11)(7, 14)
            (3, 10)(5, 12)(6, 13)(7, 14)
[4]     Order 16            Length 1
        Permutation group acting on a set of cardinality 14
        Order = 16 = 2^4
            Id($)
            (3, 10)(4, 11)(6, 13)
            (1, 8)(2, 9)(5, 12)(7, 14)
            (2, 9)(3, 10)(4, 11)(7, 14)
            (3, 10)(5, 12)(6, 13)(7, 14)
[5]     Order 64            Length 1
.........................................................
[8]     Order 21504         Length 1
        Permutation group acting on a set of cardinality 14
        Order = 21504 = 2^10 * 3 * 7
            (2, 14)(3, 4)(7, 9)(10, 11)
            (1, 11, 7, 13)(2, 5, 9, 12)(3, 10)(4, 14, 6, 8)
            (7, 14)
            (6, 13)(7, 14)
            (5, 12)(6, 13)
            (3, 10)(4, 11)
```

```
              (1, 8)(2, 9)(5, 12)(7, 14)
              (2, 9)(3, 10)(4, 11)(7, 14)
              (3, 10)(5, 12)(6, 13)(7, 1)
>
```

3. Wir wählen den Normalteiler mit Ordnung 8 aus (da 3 Faktoren $\mathfrak{S}_2$ fehlten) und prüfen, ob er isomorph dem 3-maligen direkten Produkt der Gruppe $\mathfrak{S}_2$ ist.

```
> H3:=NG2[3]‘subgroup;
> TH3:=DirectProduct(Sym(2),DirectProduct(Sym(2),Sym(2)));
> if IsIsomorphic(TH3,H3) eq true then print "isomorph"; end if;
isomorph
>
```

   Bei der Auswahl des Normalteilers ist ebenfalls besondere Sorgfalt geboten, wenn es mehrere Normalteiler derselben Ordnung gibt. Sogar, wenn diese untereinander isomorph sind, kann es zu unterschiedlichen Quotienten (s.u.) führen !

4. nun bilden wir den Quotienten aus der Gruppe des vollen Kranzprodukts und dem ausgewählten Normalteiler, d.h., wir dividieren jetzt die drei fehlenden Faktoren aus dem vollen Kranz raus:

```
> Q3:=AG2/H3;
> #Q3;
2688
>
```

5. jetzt überprüfen wir, ob dieser Quotient mit unserem vermeintlichen verminderten Kranzprodukt isomorph ist:

```
> if IsIsomorphic(AG3,Q3) eq true then print "isomorph"; end if;
isomorph
>
```

6. Wir wissen jetzt, daß sich unsere Automorphismengruppe AG3 als vermindertes Kranzprodukt schreiben läßt:

$$AG3 = (\mathfrak{S}_2 \wr PSL(3,2))/\mathfrak{S}_2^3 \tag{5.1}$$

Dabei ist die gefundene Darstellung als vermindertes Kranzprodukt gegenüber der Darstellung als semidirektes Produkt insofern vorzuziehen, als hier kein Homomorphismus angegeben werden muß, wie beim semidirekten Produkt. Allerdings ist die Darstellung nicht immer eindeutig (s. dazu auch Anhang C: „Tabellenwerk der Automorphismengruppen für zyklische Codes, Einführung“, letzter Punkt).
Ich habe daher – wo immer möglich und durch Isomorphie-Test verifiziert – im Tabellenwerk des Anhangs die entsprechenden Automorphismengruppen in dieser Weise dargestellt.

5.3 Vermindertes Kranzprodukt und G-Modul

Im Verlaufe der Anfertigung dieser Arbeit stellte sich mir die Frage, warum das „verminderte Kranzprodukt“ (zur Definition und Erklärung siehe 0.32, bzw. 3.2.1) nur bei geraden Codelängen auftritt – oder noch genauer – nur dann, wenn der äußere Kranz durch $\mathfrak{S}_2$ gebildet wird, d.h., wenn in den CompositionFactors von **Magma** am Ende Glieder der folgenden Form auftreten:

```
.........
    *
    |  Cyclic(2)
    *
    |  Cyclic(2)
    *
    |  Cyclic(2)
    *
    |  Cyclic(2)
    1
```

Wir werden jetzt nach der folgenden Definition die Konstruktion des „verminderten Kranzprodukts“ in einem Lemma erläutern.

Definition 5.5 (**G-Modul**)
Sei G eine Permutationsgruppe, welche auf der Menge Ω operiert.
Der Vektorraum

$$M := \mathbb{F}_2[\Omega] \tag{5.2}$$

wird durch die Operation von G auf Ω zu einem G-Modul

Es gilt nun folgendes

Lemma 5.6
G operiere auf Ω und es sei $M := \mathbb{F}_2[\Omega]$ der G-Modul. Dann gilt:

$$\mathfrak{S}_2 \wr G = M \rtimes G = \Gamma. \tag{5.3}$$

Sei $U \leq M$ ein Untermodul, dann ist

$$\hat{U} := \{(u, 1) \in M \rtimes G | u \in U\} \tag{5.4}$$

ein Normalteiler von $M \rtimes G$ (in Zeichen $\hat{U} \trianglelefteq \Gamma$) und wir können den folgenden Quotienten (Faktorgruppe) bilden:

$$\Gamma/\hat{U} = (\mathfrak{S}_2 \wr G)/\hat{U}, \tag{5.5}$$

der aufgrund der Konstruktion als Permutationsgruppe auf der Menge Θ operiert, mit $|\Theta| = 2 \cdot |\Omega|$.

Diesen Quotienten (Faktorgruppe) bezeichnen wir als „vermindertes Kranzprodukt“.

Kapitel 6

Anzahl der zyklischen Codes

In diesem Abschnitt möchte ich auf die Gesetzmäßigkeiten im Zusammenhang mit der Anzahl der zyklischen Codes[1] hinweisen:
Bei der Untersuchung der Automorphismengruppen fiel mir auf, daß bestimmte Anzahlen der Codes trotz unterschiedlicher Codelänge wiederholt auftraten. In der Literatur habe ich nur Aussagen zum Fall $q \nmid N$ gefunden (das heißt in unserem Fall, nur für ungerade Codelängen, da $q = 2$). Wir zitieren daher aus LUETKEBOHMERT [10], Kap. 3.2 und formulieren daraus nach einer Definition den folgenden Satz.

Definition 6.1 (**Bahnenzerlegung)**
Sei N die betrachtete Codelänge. Unter der Zerlegung von $\{1, \ldots, N\}$ in Bahnen *oder zyklotomische Teilmengen (engl. Cyclotomic Cosets) verstehen wir die folgende disjunkte Vereinigung*

$$\{1, \ldots, N\} = Z_1 \dot\cup \ldots \dot\cup Z_t. \tag{6.1}$$

wobei Z_i die minimalen Teilmengen von Resten modulo N bezeichnen, die abgeschlossen bezüglich der Multiplikation mit $q = 2$ sind.

Satz 6.2
Sei N ungerade. Dann gibt es zur Codelänge N genau 2^t zyklische Codes, wobei t die Anzahl der Bahnen von der Multiplikation mit 2 auf $\mathbb{Z}/N\mathbb{Z}$ ist.

Die von mir gefundene Formel (6.3) erlaubt nun die Berechnung der Anzahl der Rohcodes beliebiger Codelängen N und schließt damit den oben zitierten Satz 6.2 mit ein. Wir formulieren daher den folgenden wichtigen Satz:

Satz 6.3 (**1. Hauptsatz zur Anzahl der zyklischen Codes)**
Sei N die betrachtete Codelänge. Dann existiert stets eine eindeutige Faktorzerlegung von N in

$$N = 2^i \cdot a, \tag{6.2}$$

mit a ungerade.

[1] damit meine ich die Anzahl der „Rohcodes“, d.h. triviale und nichttriviale Codes im Sinne dieser Arbeit, s. Def. 0.26

Die Anzahl aller zyklischen Codes (=Rohcodes) der Länge N ist dann

$$A_N = (2^i + 1)^{t_a}, \tag{6.3}$$

wobei t_a die Anzahl der Bahnen von der Multiplikation mit 2 auf $\mathbb{Z}/a\mathbb{Z}$ ist.

Für $i = 0$ (und somit $N = a$) ist der obige Satz 6.2 aus der Literatur mit enthalten.

In der nur spärlich existierenden Literatur über Codes gerader Länge (VAN LINT, CASTAGNOLI, et al. [9], [2]) werden diese Codes als „Repeated-Root Cyclic Codes“ bezeichnet. Dort wird hauptsächlich das asymptotische Verhalten der relativen Minimaldistanz $\delta = d/N$ für große i abgeschätzt.

Beweis. Wir betrachten hier den Spezialfall $q = 2$.
Wie dem Begriff „Repeated-Root Cyclic Codes“ zu entnehmen ist, besitzt das Kreisteilungspolynom $x^{2^i \cdot a} - 1$ genau dieselben Wurzeln, wie das Kreisteilungspolynom $x^a - 1$, wobei jede Wurzel wiederholt auftritt, und zwar jeweils genau 2^i-mal. Jede Wurzel ist ein irreduzibles Polynom im Polynomring $\mathbb{F}_2[x]$. Zu jeder Wurzel gehört genau eine Bahn der Multiplikation mit 2 auf $\mathbb{Z}/a\mathbb{Z}$, wobei die Länge der Bahn gleich dem Grad des irreduziblen Polynoms ist.
Um nun für sämtliche zyklischen Codes der Länge $2^i \cdot a$ das jeweilige Generierungspolynom zu erzeugen, werden alle t_a Wurzeln multiplikativ miteinander verknüpft mit allen $2^i + 1$ möglichen Vielfachheiten als Exponent, von 0 bis 2^i, d.h. also

$$g(x) := \prod_{\nu=1}^{t_a} w_\nu(x)^{\mu_\nu}, \mu_\nu = 0, \ldots, 2^i. \tag{6.4}$$

Die $w_\nu(x)$ sind die t_a verschiedenen Wurzeln des Kreisteilungspolynoms. □

Da es ohne Computer oft einfacher ist, die Bahnen zu errechnen, als die irreduziblen Faktoren des zugehörigen Kreisteilungspolynoms zu bestimmen, ist der Satz entsprechend formuliert worden.
Mit dem Computeralgebrasystem **Magma** ist das jedoch elegant zu bestimmen:

```
> Z2:= IntegerRing(2);
> P<x> := PolynomialRing(Z2);
> Factorization(x^40+1);
[
    <x + 1, 8>,
    <x^4 + x^3 + x^2 + x + 1, 8>
]
```

Die Formel des Beweises wurde als Algorithmus in **Magma** zur Erzeugung aller zyklischer Codes programmiert, besonders für größere Codelängen ($N \geq 66$).

Eine Folgerung aus diesem Satz ist das folgende nützliche Korollar, das man auch im Zusammenhang mit der Vererbung von zyklischen Codes (s. Kapitel 2) betrachten kann:

Korollar 6.4
Sei $M = 2 \cdot N$ die doppelte Codelänge einer bereits untersuchten Codelänge N und die Anzahl aller zyklischen Codes der Länge N ist $A_N = (2^i + 1)^{t_a}$ nach Satz 6.3.
Dann ist die Anzahl aller zyklischen Codes der Länge M gegeben mit $A_M = (2^{i+1} + 1)^{t_a}$.

Beweis. Der Beweis folgt unmittelbar aus dem obigen Satz. □

Das folgende Beispiel ist mit den Tabellen aus dem Anhang leicht nachvollziehbar ($t_7 = 3$).

Beispiel 6.5
$A_7 = (2^0 + 1)^{t_7} = 2^3 = 8$
$A_{14} = (2^1 + 1)^{t_7} = 3^3 = 27$
$A_{28} = (2^2 + 1)^{t_7} = 5^3 = 125$
$A_{56} = (2^3 + 1)^{t_7} = 9^3 = 729.$

Eine weitere Folgerung aus dem obigen Hauptsatz ist mit dem Spezialfall $a = 1$ u.a. für technische Realisierungen interessant:

Folgerung 6.6
Sei $N = 2^i$. Dann gilt nach dem obigen Hauptsatz

$$A_N = A_{2^i} = 2^i + 1, \tag{6.5}$$

da $t_1 = 1$. Somit gilt für 2-er Potenzen als Codelänge der zyklischen Codes

$$A_N = N + 1. \tag{6.6}$$

In diesem Zusammenhang habe ich noch eine weitere Gesetzmäßigkeit gefunden, die wir in dem folgenden nützlichen Hilfssatz formulieren:

Hilfssatz 6.7
Sei a (die ungerade Zahl aus dem obigen Hauptsatz 6.3) selbst die Potenz einer ungeraden Zahl b, d.h., ist also $a = b^j$, so gilt für die Anzahl der Bahnen von a:

$$t_a = j \cdot t_b - (j - 1), \tag{6.7}$$

wobei t_b die Anzahl der Bahnen von der Multiplikation mit q auf $\mathbb{Z}/b\mathbb{Z}$ ist.

Beweis. Der Beweis kann geometrisch anschaulich durch fortlaufende Unterteilung (j-mal) der b Sektoren des geteilten Einheitskreises geführt werden.
Da es nicht zum Kernthema gehört, wurde auf die detaillierte Ausführung des Beweises hier verzichtet. □

Das folgende Beispiel ist mit den Tabellen aus dem Anhang leicht nachvollziehbar ($N = 54 = 2 \cdot 27 = 2 \cdot 3^3, t_3 = 2$).

Beispiel 6.8
$A_{54} = (2^1 + 1)^{t_{27}} = 3^{3 \cdot t_3 - 2} = 3^4 = 81.$

Bemerkung 6.9
Noch eine Anmerkung zur Anwendbarkeit dieser hier gemachten Aussagen:
Mit dem Computeralgebrasystem **Magma** lassen sich die Bahnen und deren Anzahl auch für größere Zahlen leicht berechnen. So habe ich auf einem PC mit 2 GB Hauptspeicher für die Zahl $N = 54321$ einen Wert von $t_N = 131$ Bahnen errechnet.
Ende der Bemerkung

Später werden wir sehen, daß zyklische Codes der Länge N genau die Untermoduln des $\mathfrak{Z}_N$-Moduls $\mathbb{F}_2[\{1, 2, \ldots, N\}]$ sind. Dadurch haben wir noch eine weitere elegante Methode, um die Anzahl der zyklischen Codes der Länge N zu bestimmen:

Satz 6.10 (2. Hauptsatz zur Anzahl der zyklischen Codes)
Sei M der $\mathfrak{Z}_N$-Modul $\mathbb{F}_2[\{1, 2, \ldots, N\}]$. Dann gilt:

$$A_N = |\{U \mid U \subseteq M\}|. \tag{6.8}$$

Beweis. Der Beweis ergibt sich unmittelbar aus den Ausführungen im Kapitel 9, Satz 9.2. □

Das folgende Beispiel für $N = 10$ liefert die im Tabellenwerk des Anhangs dokumentierte Anzahl von 9 Rohcodes. Die in dieser Arbeit weiter oben diskutierten 5 nichttrivialen Codes finden wir hier als die Untermodule Nr. 3 bis 7 mit ihren Code-Dimensionen k angegeben:

Beispiel 6.11 (Zyklische Codes als Untermoduln des $\mathfrak{Z}_{10}$-Moduls $\mathbb{F}_2[\Omega]$)

```
> G:=CyclicGroup(10);
> GM:=GModule(G,GF(2));
> Submodules(GM);
[
    GModule of dimension 0 over GF(2),
    GModule of dimension 1 over GF(2),
    GModule of dimension 2 over GF(2),
    GModule of dimension 4 over GF(2),
    GModule of dimension 5 over GF(2),
    GModule of dimension 6 over GF(2),
    GModule of dimension 8 over GF(2),
    GModule of dimension 9 over GF(2),
    GModule GM of dimension 10 over GF(2)
]
> LGM:=Submodules(GM);
> #LGM; // das ist die Anzahl der Codes:
9
>
```

Kapitel 7

Statistik

Im Zuge der Untersuchungen der zyklischen Codes und deren Auswertung habe ich neben den üblichen Attributen – wie Anzahl der Codes zu einer bestimmten Codelänge – auch Daten gefunden, die hier erwähnt werden sollen (dabei werden die Gesetzmäßigkeiten bezüglich der Anzahl Rohcodes in einem gesonderten Kapitel 6 behandelt).
Es fiel mir auf, daß bei manchen Codelängen nur einige, bei anderen Codelängen aber praktisch alle Rohcodes unseren Anforderungen der nichttrivialen Codes erfüllte.
Ich habe daher in die Tabelle der zyklischen Gruppencodes zu Beginn des Anhangs eine Spalte aufgenommen, die dieses Verhältnis von nichttrivialen zu Rohcodes mit dem Begriff „Dichte“ bezeichtet.

Definition 7.1

$$\textbf{Dichte}[\%] := \frac{\textbf{Anzahl nichttriviale Codes}}{\textbf{Anzahl Rohcodes} - \textbf{4}} \cdot \textbf{100}. \tag{7.1}$$

Folgende Beobachtungen wurden gemacht:

1. Codelängen N, die ein Vielfaches von 6 sind, erreichen keine 100%, d.h., es gibt dort auflösbare Automorphismengruppen.

2. Codelängen N, die ein Vielfaches von 9 sind, erreichen keine 100%, d.h., es gibt dort auflösbare Automorphismengruppen.

3. allgemein: Codelängen N, die ein Vielfaches von $3z$ sind, wobei z eine Zahl ungleich 5 oder 7 ist, erreichen keine 100%, d.h., es gibt dort auflösbare Automorphismengruppen.

4. Codelängen N, die eine Potenz von 2 sind, erreichen keine 100%, d.h., es gibt dort auflösbare Automorphismengruppen.

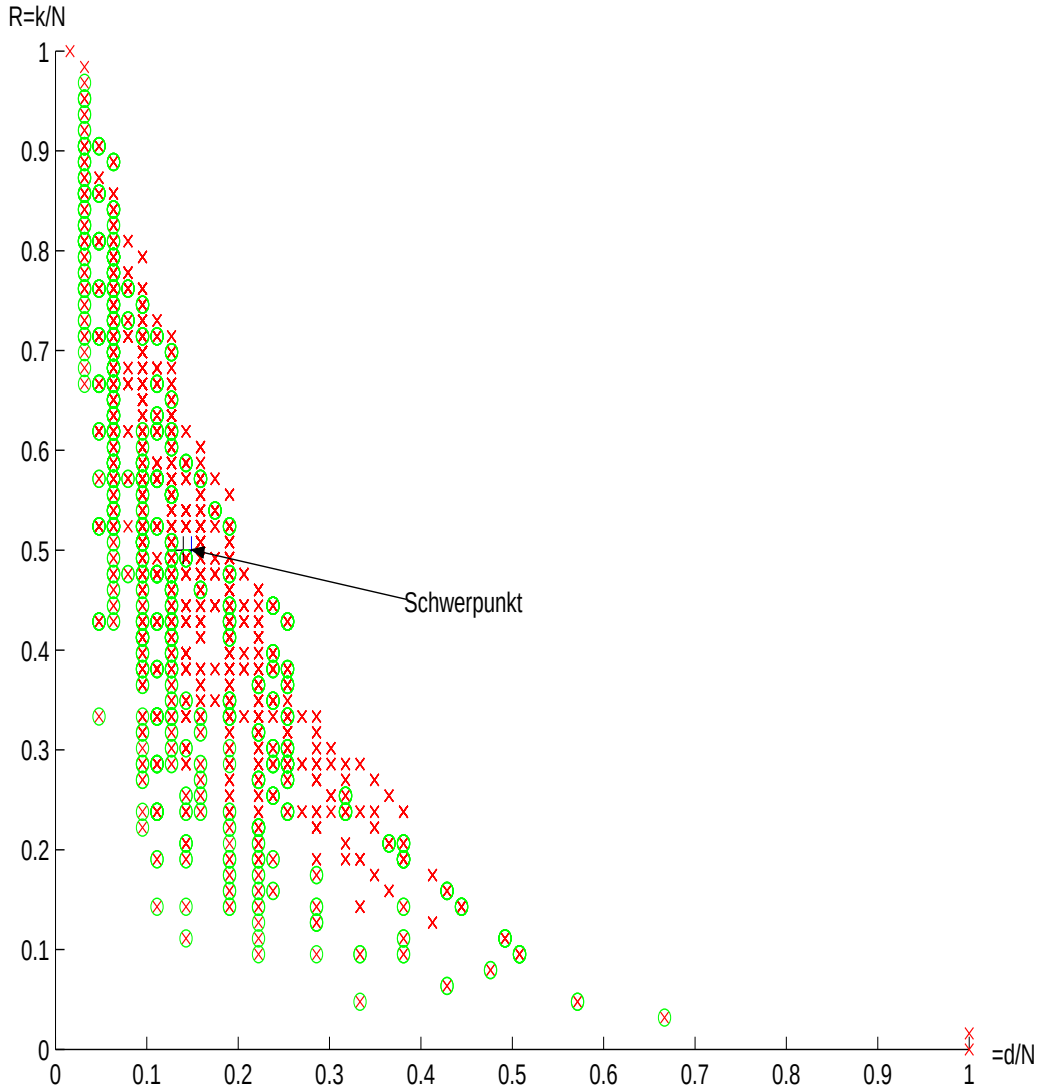
5. die meisten übrigen Codelängen N haben eine Dichte von 100% (Ausnahmen: $N =$ 31, 34, 55, 62, 65).

Bei der großen Menge von errechneten zyklischen Codes lag es nahe, die Verhältnisse $R = k/N$, bzw. $\delta = d/N$ für jeden Code einer bestimmten Codelänge zu berechnen und in einem Diagramm graphisch darzustellen.

Definition 7.2 (Effizienz)
$R(C) = k/N$ *heißt* Effizienz *oder Rate des Codes* C

Definition 7.3 (Zuverlässigkeit)
$\delta(C) = d/N$ *heißt* Zuverlässigkeit *des Codes* C

In der folgenden Grafik am Beispiel $N = 63$ mit 8192 Rohcodes ist eine asymptotische Hüllkurve erkennbar, wie sie z.B in der Literatur MacWilliams [16] Ch17, §7, oder Lütkebohmert [10], Kap. 5.2 als Schranke dargestellt wird.



Dabei sind die Kreuze die δ-R-Werte für alle 8192 zyklischen Codes der Länge 63, während die Kreise um eine Teilmenge von ihnen für die 1052 nichttrivialen Codes (im Sinne dieser Arbeit) stehen.

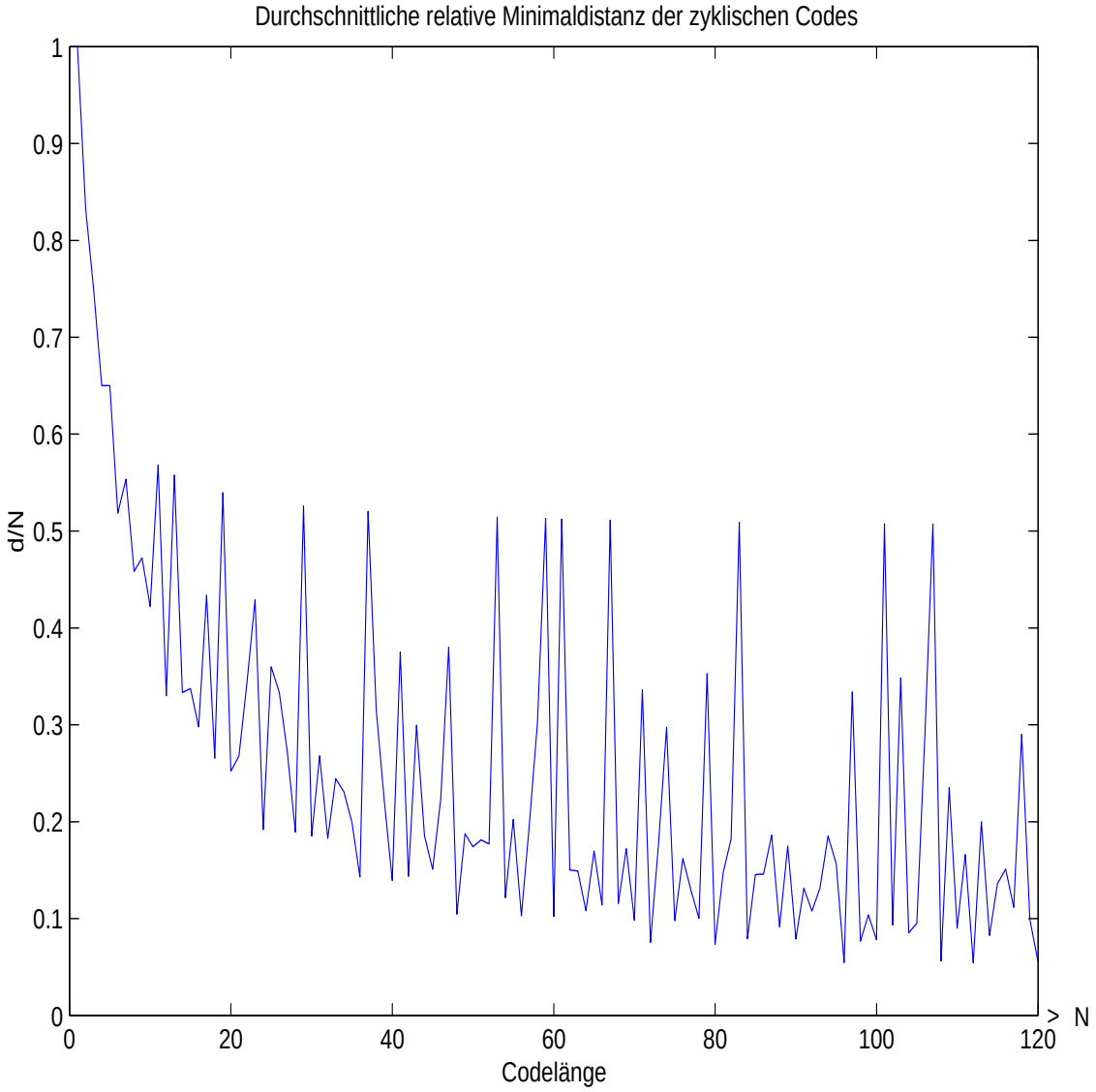
Es ist offensichtlich, daß einige δ-R-Werte mehrfach angenommen werden. Die Abszissen- und Ordinatenwerte eines jeden Punktes sind rationale Zahlen zwischen 0 und 1.
Interessant ist die Lage des Schwerpunktes aller Codes bzw. aller nichttrivialen Codes: Seine Ordinate ist stets 0,5 (beide Schwerpunkte sind in der obigen Grafik eingezeichnet – sie liegen dicht beieinander). Wir wollen diese Erkenntnis in einem Lemma festhalten:

Lemma 7.4
Zu jeder festen Codelänge N gilt:
Die Ordinate des Schwerpunktes aller zyklischen Codes bzw. aller nichttrivialen zyklischen Codes ist stets $0,5$.

Beweis. Der R-Wert eines jeden Codes ist definiert als k/N. Da bei den hier betrachteten Codemengen auch stets der zu einem Code zugehörige duale Code dazugehört, ist dessen R-Wert $(N-k)/N$. Somit ist der Mittelwert der R-Werte eines jeden Paares stets genau $1/2$.
Falls N gerade, so gibt es stets eine ungerade Zahl von selbstdualen zyklischen Codes mit $k = N/2$, d.h. $R = 1/2$. □

Folgerung 7.5
Damit haben wir gezeigt, daß die Ordinate des Schwerpunkts aller zyklischen Codes nicht von der Codelänge abhängig ist. Für weitere statistische Untersuchungen auf dieser Ebene braucht also nur noch die durchschnittliche relative Minimaldistanz (das ist der Abszissenwert des Schwerpunkts) in Abhängigkeit von der Codelänge untersucht zu werden.

Dabei sieht man trotz der Oszillationen, daß mit zunehmender Codelänge die durchschnittliche relative Minimaldistanz immer kleiner wird (man denke sich in der Grafik eine obere und untere Hüllkurve).
Wir wollen dazu eine Grafik und eine Liste beifügen, um diesen Effekt zu verdeutlichen (aus Gründen der Deutlichkeit wurden die Punkte in der Grafik durch eine Linie verbunden). Danach folgt eine Diskussion.



Relative Minimaldistanz der zyklischen Codes bis zu der Laenge N = 120

N	Anz	Sum(d)	Avg(d)	N	Anz	Sum(d)	Avg(d)
1	2	2	1.00000	61	4	125	0.51229
2	3	5	0.83333	62	2187	20367	0.15020
3	4	9	0.75000	63	8192	76873	0.14895
4	5	13	0.65000	64	65	449	0.10793
5	4	13	0.65000	65	128	1412	0.16971
6	9	28	0.51851	66	243	1829	0.11404
7	8	31	0.55357	67	4	137	0.51119
8	9	33	0.45833	68	125	982	0.11552
9	8	34	0.47222	69	64	760	0.17210
10	9	38	0.42222	70	729	5009	0.09816
11	4	25	0.56818	71	8	191	0.33626
12	25	99	0.33000	72	729	3962	0.07548
13	4	29	0.55769	73	512	6679	0.17869
14	27	126	0.33333	74	9	198	0.29729
15	32	162	0.33750	75	256	1881	0.09797
16	17	81	0.29779	76	25	308	0.16210

N	Anz	Sum(d)	Avg(d)	N	Anz	Sum(d)	Avg(d)
17	8	59	0.43382	77	64	640	0.12987
18	27	129	0.26543	78	243	1901	0.10029
19	4	41	0.53947	79	8	223	0.35284
20	25	126	0.25200	80	289	1701	0.07357
21	64	360	0.26785	81	32	382	0.14737
22	9	68	0.34343	82	27	404	0.18247
23	8	79	0.42934	83	4	169	0.50903
24	81	373	0.19187	84	15625	103910	0.07917
25	8	72	0.36000	85	4096	50628	0.14541
26	9	78	0.33333	86	81	1017	0.14599
27	16	117	0.27083	87	32	518	0.18606
28	125	662	0.18914	88	81	652	0.09147
29	4	61	0.52586	89	512	7967	0.17483
30	243	1350	0.18518	90	6561	46639	0.07898
31	128	1064	0.26814	91	1024	12228	0.13122
32	33	193	0.18276	92	125	1240	0.10782
33	32	258	0.24431	93	16384	199977	0.13124
34	27	212	0.23093	94	27	470	0.18518
35	64	446	0.19910	95	32	476	0.15657
36	125	643	0.14288	96	1089	5713	0.05465
37	4	77	0.52027	97	8	259	0.33376
38	9	108	0.31579	98	243	1825	0.07664
39	32	278	0.22275	99	256	2629	0.10373
40	81	451	0.13919	100	125	979	0.07832
41	8	123	0.37500	101	4	205	0.50742
42	729	4395	0.14354	102	6561	62431	0.09329
43	16	206	0.29941	103	8	287	0.34830
44	25	204	0.18545	104	81	718	0.08523
45	256	1738	0.15086	105	32768	326756	0.09497
46	27	278	0.22383	106	9	278	0.29140
47	8	143	0.38031	107	4	217	0.50701
48	289	1449	0.10445	108	625	3795	0.05622
49	32	294	0.18750	109	16	410	0.23509
50	27	235	0.17407	110	243	2410	0.09016
51	256	2366	0.18121	111	32	590	0.16610
52	25	230	0.17692	112	4913	29905	0.05435
53	4	109	0.51415	113	32	723	0.19994
54	81	532	0.12162	114	243	2285	0.08249
55	32	356	0.20227	115	64	1000	0.13586
56	729	4197	0.10280	116	25	438	0.15103
57	32	364	0.19956	117	4096	53506	0.11164
58	9	158	0.30268	118	9	308	0.29001
59	4	121	0.51271	119	512	6048	0.09926
60	3125	19131	0.10203	120	59049	393626	0.05555

Bemerkung 7.6

Die hier dargestellten durchschnittlichen relativen Minimaldistanzen in Abhängigkeit zur Codelänge deuten eine oszillierende Konvergenz nach Null an. Die Oszillationen sind ausgeprägt mit relativ großen Werten für Primzahlen als Codelängen, bei denen nur triviale Codes (i.S.d.A.) existieren. Aber auch diese Werte werden mit zunehmendem N kleiner, wenn wir z.B. die Werte für $N = 13, 19, 29, 37, 53, 59$ vergleichen.

Die Werte bei den Codelängen mit nichttrivialen Codes gehen in dem hier beobachteten Bereich mit einigen Schwankungen immer weiter bis unterhalb 0,1 zurück.
Woran liegt das?
Wir hatten in dem Abschnitt Zusammenfassung, wie auch im Kapitel 4 „Test“ gesehen, daß – im Gegensatz zur Dimension der Codes, wo bei den dualen Codes mit $\dim(C^{\perp}) = N - k$ eine direkte Abhängigkeit zur Codelänge gegeben ist (s. auch obiges Lemma dazu) – bei den Minimaldistanzen der dualen Codes diese Abhängigkeit fehlt. Wir hatten hier stets konstante Werte angeben können: z.B.: 2, 3, 4, etc.
Durch diese in der Natur der zyklischen Codes begründete Eigenschaft verstehen wir nun, daß deshalb der Durchschnitt der relativen Minimaldistanzen bei großen N immer kleiner werden muß.

Kapitel 8

Hamming-Codes und ihre Automorphismengruppen

Eine interessante Teilmenge der zyklischen Codes bilden die Hamming Codes.
Im Zuge meiner Untersuchungen habe ich Gesetzmäßigkeiten im Zusammenhang mit den Automorphismengruppen entdeckt, die nach der Definition erläutert und in Sätzen formuliert werden soll.

Definition 8.1 (**Hamming-Code**)
Es sei $r \in \mathbb{N}$ *und* $N{=}2^r - 1$. *Ein linearer* $[N, N-r, 3]_{\mathbb{F}_2}$*-Code heißt* Hamming-Code $\mathcal{CH}_r$*, falls die n Spalten der Kontollmatrix paarweise linear unabhängig sind.*

Die Kontrollmatrix H_r läßt sich einfach erstellen, indem man sämtliche Vektoren des $\mathbb{F}_2^r$ außer dem Nullvektor als Spaltenvektoren einträgt.
Hamming-Codes sind perfekt[1].

Bezüglich der Werte $R = k/N$ („Rate“ oder „Effizienz“) und $\delta = d/N$ („Zuverlässigkeit“) der Hamming-Codes erwarten wir für große N ein asymptotisches Verhalten gegen (0,1) im Koordinatensystem (δ, R).

Da immer nur 1 Fehler korrigiert werden kann, bedeutet dies, daß die relative Zuverlässigkeit für große N immer schlechter wird. Bei Signaltransmissionen in einem Medium mit extrem wenig Störeinflüssen, wie z.B. Glasfaser, kann die Verwendung von Hamming-Codes wegen der hohen Effizienz dennoch interessant sein.
Bevor wir dazu eine Grafik erstellen, berechnen wir mit **Magma** die Hamming-Codes bis zur 11-ten Ordnung und deren jeweilige Automorphismengruppe und stellen daraus die Tabelle 8.1 zusammen:
Außer der erwarteten Entwicklung der Werte für R und δ fällt auf, daß ab $r = 5$ als Automorphismengruppe die Spezialgruppe $PSL(r, 2)$ ausgewiesen wird.

[1] d.h., die Vereinigung aller abgeschlossenen Kugelumgebungen vom Radius $\lfloor /d - 1)/2 \rfloor$ um alle Codewörter überdeckt den gesamten Vektorraum $\mathbb{F}_2^N$.

Name	r	N	k	d	$R = k/N$	$\delta = d/N$	Automorphismengruppe
$\mathcal{CH}_2$	2	3	1	3	0,33333	1,00000	$PSL(2,2) \cong \mathfrak{S}_3$
$\mathcal{CH}_3$	3	7	4	3	0,57142	0,42857	$PSL(3,2) \cong PSL(2,7)$
$\mathcal{CH}_4$	4	15	11	3	0,73333	0,20000	$PSL(4,2) \cong \mathfrak{A}^8$
$\mathcal{CH}_5$	5	31	26	3	0,83871	0,096774	$PSL(5,2)$
$\mathcal{CH}_6$	6	63	57	3	0,90476	0,047619	$PSL(6,2)$
$\mathcal{CH}_7$	7	127	120	3	0,94488	0,023622	$PSL(7,2)$
$\mathcal{CH}_8$	8	255	247	3	0,96862	0,011764	$PSL(8,2)$
$\mathcal{CH}_9$	9	511	502	3	0,98238	0,0058708	$PSL(9,2)$
$\mathcal{CH}_{10}$	10	1023	1013	3	0,99022	0,0029325	$PSL(10,2)$
$\mathcal{CH}_{11}$	11	2047	2036	3	0,99462	0,0014655	$PSL(11,2)$

Tabelle 8.1: Tabelle der Hamming-Codes

Weiter stellen wir folgende wichtige Isomorphien fest[2]:

$$PSL(2,2) \cong \mathfrak{S}_3 \tag{8.1}$$

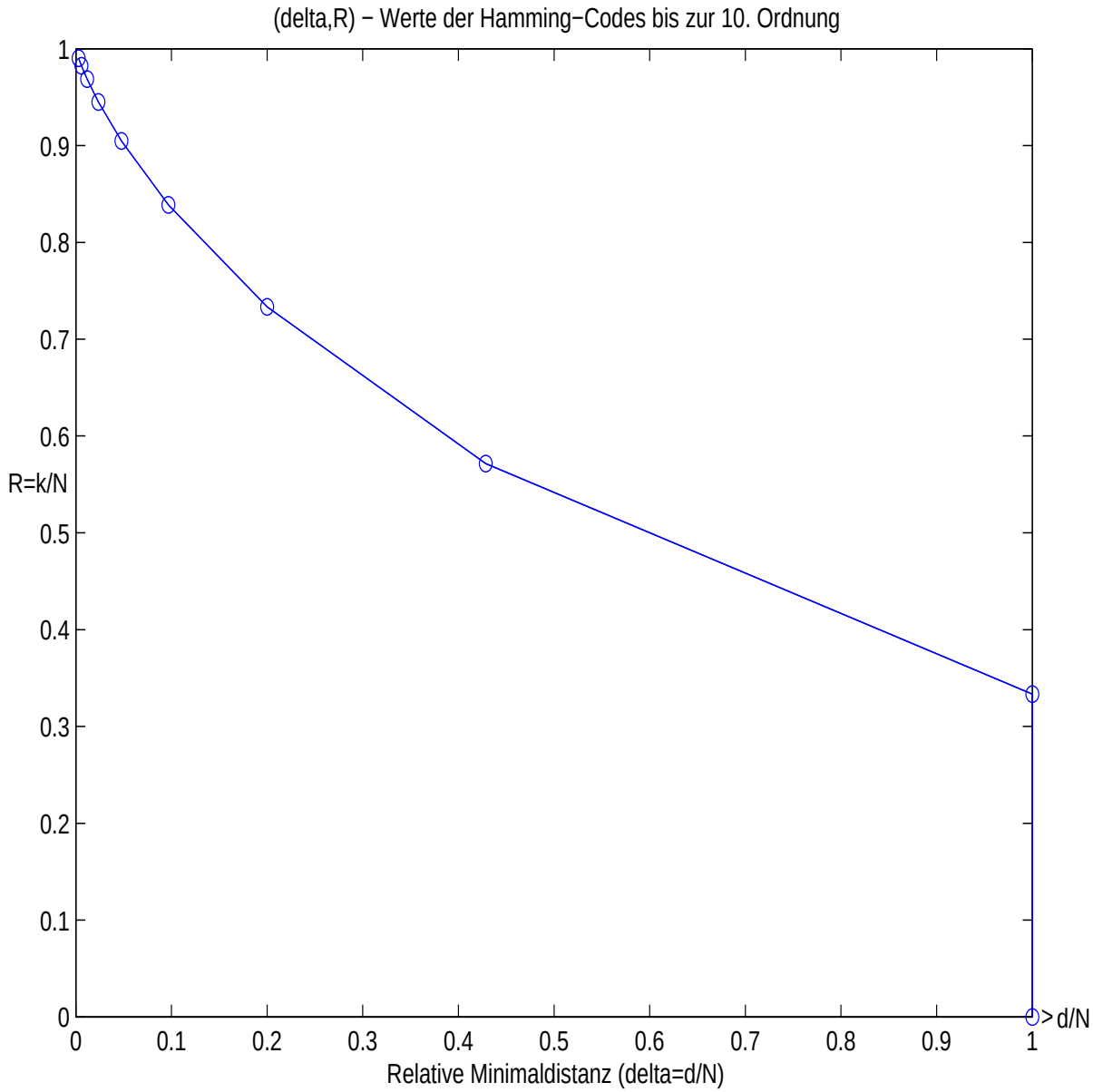
$$PSL(3,2) \cong PSL(2,7) \tag{8.2}$$

$$PSL(4,2) \cong \mathfrak{A}_8 \tag{8.3}$$

Nach der Grafik auf der nächsten Seite werden wir dazu einen Satz formulieren und beweisen.

[2]siehe dazu auch B. Huppert [4], S. 183, Satz 6.14

Die folgende Grafik zeigt nun die erwartete asymptotische Entwicklung der (δ, R) - Werte der Hamming-Codes (mit zunehmender Ordnung) gegen (0,1):



Wir formulieren nun den folgenden Satz[3]:

Satz 8.2

Für den binären Hamming-Code $\mathcal{CH}_r$ der Ordnung $r \geq 2$ ist die Automorphismengruppe Aut($\mathcal{CH}_r$) die Spezialgruppe $PSL(r, 2)$.

[3]Dieser Satz wurde später doch noch in der Literatur gefunden [14], Handbook of Coding Theory, Volume II, S.1408, Theorem 7.2 – mit einer anderen Beweisführung.

Beweis. Wir betrachten hier den Spezialfall $q = 2$.
Die Codelänge des Hamming-Codes $\mathcal{CH}_r$ der Ordnung r ist:

$$N = 2^r - 1, \quad r = 2, 3, \ldots$$

Dies ist gleich der Anzahl der Vektoren im $\mathbb{F}_2^r$, vermindert um den Nullvektor.
Außerdem gilt: $\dim(\mathcal{CH}_r) = 2^r - 1 - r, \quad r = 2, 3, \ldots,$
sowie $d \equiv 3$ für alle r.
Sei ferner H_r die Kontrollmatrix des Hamming-Codes $\mathcal{CH}_r$ der Ordnung r.
Wir betrachten zunächst den Fall $r = 2$:

$$\mathbb{F}_2^2 \setminus \{0\} = \left(\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right) = H_2.$$

$$\mathcal{CH}_r = Ker(H_r) \subseteq \mathbb{F}_2^N, N = 3$$

im Fall $r = 2$. Allgemein gilt:

$$Aut(\mathcal{CH}_r) = \{\sigma \in \mathfrak{S}_N \mid \hat{\sigma}(\mathcal{CH}_r) = \mathcal{CH}_r\}.$$

Außerdem ist:

$$\mathbb{F}_2^N = \{ \begin{pmatrix} a_1 \\ \vdots \\ a_N \end{pmatrix} \mid a_i \in \mathbb{F}_2 \}$$

und es ist:

$$\hat{\sigma} \left(\begin{pmatrix} a_1 \\ \vdots \\ a_N \end{pmatrix} \right) = \begin{pmatrix} a_{\sigma(1)} \\ \vdots \\ a_{\sigma(N)} \end{pmatrix}.$$

Grundsätzlich gilt:

$$Aut(\mathcal{CH}_r) \leq \mathfrak{S}_N.$$

Definition 8.3
Sei

$$\alpha_1 := \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ldots, \alpha_N := \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}$$

eine feste Numerierung von $\mathbb{F}_2^r \setminus \{0\}$.
Dann ist

$$H_r := (\alpha_1, \ldots, \alpha_N).$$

$SL(r, \mathbb{F}_2)$ operiert auf $\mathbb{F}_2^r \setminus \{0\}$, mit $\gamma \in SL(r, \mathbb{F}_2)$.
σ_γ sei die zugehörige Permutation der $\{\alpha_1, \ldots, \alpha_N\}$.
$\gamma \longmapsto \sigma_\gamma$ ist ein Homomorphismus:

$$\lambda : SL(r, \mathbb{F}_2) \longrightarrow \mathfrak{S}_N, \quad \lambda(\gamma) = \sigma_\gamma.$$

Zu zeigen ist:
(i) λ ist injektiv.
(ii) Im $\lambda \subseteq Aut(\mathcal{CH}_r)$.
Teil (i):

Sei u ein Codevektor, $u \in \mathcal{CH}_r$ und $u \in ker(H_r)$ mit $u = \begin{pmatrix} u_1 \\ \vdots \\ u_N \end{pmatrix}$.

Es gilt

$$\gamma \cdot H_r = (\alpha_{\lambda(\gamma)(1)}, \ldots, \alpha_{\lambda(\gamma)(N)}) =: L.$$

$$\widehat{\lambda(\gamma)}(u) = \begin{pmatrix} u_{\lambda(\gamma)(1)} \\ \vdots \\ u_{\lambda(\gamma)(N)} \end{pmatrix}.$$

$$\gamma \cdot H_r \cdot x = 0 \Longleftrightarrow H_r \cdot x = 0$$

$$\widehat{\lambda(\gamma)}(u) \in ker(L) = ker(\gamma H_r) = ker(H_r)$$

wegen $L \cdot \widehat{\lambda(\gamma)}(u) = H_r \cdot u$ und weil γ invertierbar ist. Daraus folgt:

$$\lambda(SL(r, \mathbb{F}_2)) \leq Aut(\mathcal{CH}_r) \leq \mathfrak{S}_N. \tag{8.4}$$

Damit ist Teil (i) bewiesen. □

Es folgt Teil (ii):
Sei $\sigma \in Aut(\mathcal{CH}_r)$. Finde $\gamma \in SL(r, \mathbb{F}_2)$ mit $\lambda(\gamma) = \sigma \in \mathfrak{S}_N$.
σ permutiert die $\alpha_i \, (i = 1, \ldots, N)$ zu $\alpha_{\sigma(i)}$.
Für den weiteren Beweis benötigen wir die beiden folgenden Sätze:

Hilfssatz 8.4
Gilt

$$\alpha_i = \alpha_j + \alpha_k, \tag{8.5}$$

dann folgt:

$$\alpha_{\sigma(i)} = \alpha_{\sigma(j)} + \alpha_{\sigma(k)}.$$

Beweis. Formel 8.5 $\Longleftrightarrow \alpha_i + \alpha_j + \alpha_k = 0$ und bedeutet,
der Vektor u (mit $u_i = u_j = u_k = 1$ und $u_l = 0$ sonst) ist ein Codevektor, also: $u \in \mathcal{CH}_r$.
Sei $\hat{\sigma}(u) = v$ mit $v_{\sigma(i)} = v_{\sigma(j)} = v_{\sigma(k)} = 1$ und $v_l = 0$ sonst.
Es gilt: $v \in \mathcal{CH}_r$, weil $\sigma \in Aut(\mathcal{CH}_r)$. Daraus folgt:

$$\alpha_{\sigma(i)} + \alpha_{\sigma(j)} + \alpha_{\sigma(k)} = 0.$$

Damit ist der Hilfssatz bewiesen. □

Satz 8.5
Die Abbildung

$$\gamma: \quad \mathbb{F}_2^r \longrightarrow \mathbb{F}_2^r$$

$$\gamma: \quad 0 \longmapsto 0$$

$$\gamma: \quad \alpha_i \longmapsto \alpha_{\sigma(i)}$$

ist linear und invertierbar.

Beweis. siehe Hilfssatz.
Das Inverse von γ ist die entsprechende Abbildung zu σ^{-1}. □

Es gilt:

$$\gamma \in GL(r, \mathbb{F}_2) = SL(r, \mathbb{F}_2) = PSL(r, \mathbb{F}_2) = PSL(r, 2). \tag{8.6}$$

Damit ist Teil (ii) und somit der Satz bewiesen. □

Kapitel 9

G-Moduln und lineare Codes

Nomenklatur: In dieser Arbeit bedeutet „$<$“ stets „$\lneq$“ und es bedeutet „$\subset$“ stets „$\subsetneq$“.

Bei der Untersuchung der verminderten Kranzprodukte sind wir bereits auf G-Moduln gestoßen (s. dazu auch Kapitel 10).

Bezeichnung 9.1
Sei Ω die Menge $\{1, 2, \ldots, N\}$ und die Gruppe G operiert auf Ω.
Dann ist $\mathbb{F}_2[\Omega]$ der G-Modul.

Bei der Betrachtung der Untermoduln der $PSL(r, 2)$-Moduln $\mathbb{F}_2[\Omega]$ fiel mir auf, daß die Dimension der Untermoduln identisch sind mit der Dimension derjenigen zyklischen Codes, die diese $PSL(r, 2)$-Gruppe als Automorphismengruppe haben. Daraufhin habe ich ein **Magma**-Programm geschrieben, welches für den jeweiligen Untermodul (als k-dimensionaler Untervektorraum des G-Moduls) eine $k \times N$ Matrix als Basis ermittelt. Der davon erzeugte lineare Code ist tatsächlich der vermutete zyklische Code.
Wir wollen daher jetzt einen wichtigen Satz formulieren und beweisen:

Fakt 9.2
Sei $\mathfrak{Z}_N$ die zyklische Gruppe der Ordnung N und $\Omega = \mathbb{F}_2[\{1, 2, \ldots, N\}]$.
Die Untermoduln des $\mathfrak{Z}_N$-Moduls $\mathbb{F}_2[\Omega]$ sind genau die zyklischen Codes der Länge N.

Beweis. Da der $\mathfrak{Z}_N$-Modul $\mathbb{F}_2[\{1, 2, \ldots, N\}]$ auf Ω (mit $|\Omega| = N$) operiert, können seine Untermoduln als Untervektorräume von $\mathbb{F}_2^N$ aufgefaßt werden, auf denen $\mathfrak{Z}_N$ operiert, d.h. deren Spalten von $\mathfrak{Z}_N$ zyklisch permutiert werden.
Das aber genau ist die Definition eines zyklischen Codes der Länge N ($\mathfrak{Z}_N$ ist die Startgruppe der zyklischen Codes als Gruppencodes). □

Die so gefundenen zyklischen Codes sind natürlich identisch mit den bislang algebraisch oder vektoriell erzeugten zyklischen Codes.

Die Verallgemeinerung des Satzes 9.2 führt uns zum

Satz 9.3 (Hauptsatz für Gruppencodes)
Sei G eine beliebige transitive[1] *Permutationsgruppe $G \leq \mathfrak{S}_N$ und $\Omega = \mathbb{F}_2[\{1, 2, \ldots, N\}]$. Dann sind die Untermoduln des G-Moduls $\mathbb{F}_2[\Omega]$ genau die Gruppencodes C der Länge N mit G als Startgruppe und den Automorphismengruppen $G \leq Aut(C) \leq \mathfrak{S}_N$.*

Der folgende fundamentale Satz stellt einen wichtigen und offensichtlichen Zusammenhang zwischen der Gruppe $\mathfrak{G} \leq \mathfrak{S}_N$ und der Automorphismengruppe $\mathrm{Aut}(C)$ eines von einem Untermodul des $\mathfrak{G}$-Moduls $\mathbb{F}_2[\{1, 2, \ldots, N\}]$ erzeugten linearen Codes C dar:

Satz 9.4
Sei $\mathfrak{G} \leq \mathfrak{S}_N$ und $\Omega = \{1, 2, \ldots, N\}$. Dann gilt:
Die Automorphismengruppen $Aut(C)$ der von den Untermoduln des $\mathfrak{G}$-Moduls $\mathbb{F}_2[\Omega]$ erzeugten linearen Codes C der Länge N genügen der Relation

$$\mathfrak{G} \leq Aut(C) \leq \mathfrak{S}_N. \tag{9.1}$$

Wir führen den Beweis durch Widerspruch:

Beweis. Angenommen, es existiere ein Code $C \subseteq \mathbb{F}_2[\Omega]$ der Länge N mit $Aut(C) < G$, dann gibt es ein Gruppenelement $g \in G$ und ein Codevektor $c \in C$, so daß $g \cdot c \notin C$. Also ist $C \nsubseteq \mathbb{F}_2[\Omega]$. Dies steht im Widerspruch zur Annahme. □

Folgerung 9.5
Zum besseren Verständnis leiten wir jetzt einige Folgerungen aus diesem Satz ab:

1. *Sei GM der $\mathfrak{S}_N$-Modul $\mathbb{F}_2[\Omega]$.*
   Dann existieren zu GM nur die Untermoduln, deren Codes die $\mathfrak{S}_N$ als Automorphismengruppe haben. Das sind genau die 4 primitiven Codes (s. Abschnitt 2.1).

   Beweis. Wir führen den Beweis durch Widerspruch:
   Sei $\Omega := \{1, 2, \ldots, N\}$ und $GM := \mathbb{F}_2[\Omega]$ der $\mathfrak{S}_N$-Modul. Sei ferner $(x_1, \ldots, x_N)$ die Standardbasis von $\mathbb{F}_2[\Omega]$.
   Angenommen, $U \subseteq GM$ ist ein $\mathfrak{S}_N$-Untermodul, der nicht einer der 4 primitiven Codes ist. Dann folgt:
   Es gibt ein Element $\omega \in U$ mit Hamming-Gewicht $\neq$ 0, 1, 2, N, d.h., $\omega = x_I$ ist ein Codevektor.
   Sei nun $I \subsetneq \{1, 2, \ldots, N\}$ eine Index-Menge mit $|I| \neq$ 0, 1, 2, N.
   Dann gibt es $\sigma \in \mathfrak{S}_N$ mit $|\sigma I \cap I| = |I| - 1$, d.h., I und σI stimmen bis auf ein Element überein.
   Aus $x_I \in U$ folgt $x_{\sigma I} \in U$ und $x_{\sigma I} + x_I \in U$.

[1] diese Einschränkung „G transitiv“ war erforderlich, da ansonsten auch lineare Codes unter den Untermoduln sind, die keine Gruppencodes sind (s. dazu auch das Beispiel am Ende von Bemerkung 9.10 weiter unten).

Das Hamming-Gewicht von $x_{\sigma I} + x_I$ ist $= 2$. Das ist ein Widerspruch zur obigen Annahme. □

2. *Gibt es zwischen G und $\mathfrak{S}_N$ keine weiteren Automorphismengruppen, d.h., ist*

$$\{Aut(C) \mid G < Aut(C) < \mathfrak{S}_N\} = \emptyset, \tag{9.2}$$

so existieren neben den primitiven Codes (mit $Aut(C) = \mathfrak{S}_N$) nur diejenigen Codes als Untermoduln von GM, deren vollständige Automorphismengruppe G selbst ist (Beispiel: $N = 31, G = PSL(5, 2)$).

Wie bereits beim Beweis von Satz 1.12 angekündigt, hier nun die knappe Version des zweiten Beweisteils zum Zentralen Satz für zyklische Codes:

Beweis. Sei $N = a \cdot b$. Da $\mathfrak{S}_a \wr \mathfrak{S}_b$ stets maximale Untergruppe unter $\mathfrak{S}_N$ ist[2], kann es keine nichttriviale Obergruppe geben. □

Eine wesentliche Folgerung wollen wir in einem eigenständigen Satz formulieren:

Satz 9.6
Sind $A_1 < A_2$ zwei Automorphismengruppen von Codes der Länge N, so gilt:

$$\{C_i \mid C_i \subseteq A_1\text{-}Modul\ \mathbb{F}_2[\Omega]\} \supset \{C_j \mid C_j \subseteq A_2\text{-}Modul\ \mathbb{F}_2[\Omega]\} \tag{9.3}$$

Wir führen den Beweis ähnlich, wie für Satz 9.4:

Beweis. Da $A_1 < A_2$ nach Voraussetzung, enthält A_1 Gruppenelemente aus A_2, d.h. einzelne Automorphismen[3] der Codes C_j. Daher finden sich die Codes C_j in der Untermodul-Liste des A_1-Moduls $\mathbb{F}_2[\Omega]$ mit aufgenommen. Andererseits sind die Codes C_k (mit $C_i = C_k \cup C_j$), zu denen A_1 die volle Automorphismengruppe ist, nicht in der Untermodul-Liste des A_2-Moduls $\mathbb{F}_2[\Omega]$ enthalten, da A_2 Permutationen enthält, die aus diesen Codes jeweils herausführen. □

Wir schließen daran noch eine wichtige Folgerung an:

Folgerung 9.7
Seien die Voraussetzungen und Bezeichnungen wie in Satz 9.6 gegeben.
Sei darüberhinaus die Menge der Automorphismengruppen A_i von Codes der Länge N mit

$$\{A_i \mid A_1 < A_i < A_2\} = \emptyset.$$

Dann gilt: Die Menge der zu A_1 gehörenden Codes ist genau

$$\{C_i \mid C_i \subseteq A_1\text{-}Modul\ \mathbb{F}_2[\Omega]\} \setminus \{C_j \mid C_j \subseteq A_2\text{-}Modul\ \mathbb{F}_2[\Omega]\} \tag{9.4}$$

[2] die Maximalität von $\mathfrak{S}_a \wr \mathfrak{S}_b$ unter $\mathfrak{S}_N$ wird in Martin W. Liebeck, Cheryl E. Praeger, and Jan Saxl [7],S. 366 gezeigt.

[3] diese Automorphismen bilden natürlich eine Gruppe, aber nicht die **volle** Automorphismengruppe

(s. dazu auch Beispiel 10.12)

Eine weitere wichtige Folgerung sind die folgenden Struktur-Aussagen (die Gruppe G operiert auf der Menge Ω:

- Die Untermoduln des G-Moduls $\mathbb{F}_2[\Omega]$ bilden
  einen modularen Verband[4] mit 0 und 1
- Somit bilden auch die von G erzeugten linearen Codes einen modularen Verband mit 0 und 1. Dabei ist das Nullelement der Nullcode (s. Abschnitt 2.1 „Elementarcodes“) und das Einselement ist der **erste Elementarcode** = `UniverseCode(GF(2),N)`.
- Dann gibt es noch einen weiteren Verband, nämlich den Verband der Automorphismengruppen: Hier ist das Infimum die Gruppe G und das Supremum die Symmetrische Gruppe $\mathfrak{S}_N$ (s. a. Hasse-Diagramm 3.1).

Beobachtung 9.8
Einige interessante Beobachtungen in Bezug auf Code-Isomorphien (s. a. Kapitel 0.1) seien hier noch angefügt:

- Ist A die volle Automorphismengruppe von Code C, so liefert
  $\{U \mid U \subseteq A\text{-Modul } \mathbb{F}_2[\Omega]\}$
  nur genau **einen** Repräsentanten von C (d.h., ohne dazu isomorphe Codes), während
  $\{U \mid U \subseteq \mathfrak{Z}_N\text{-Modul } \mathbb{F}_2[\Omega]\}$
  alle zu C isomorphen Codes enthält.
  Beispiel: $N = 31, A = PSL(5, 2)$.
- Sei A wie oben definiert und aus Gruppenfaktoren zusammengesetzt, von denen mindestens einer einen Isomorphie-Faktor > 1 habe.
  Falls es eine volle Automorphismengruppe D gibt mit $\mathfrak{Z}_N < A < D < \mathfrak{S}_N$ und D hat mindestens einen der Gruppenfaktoren von A mit Isomorphie-Faktor > 1 gemeinsam, so hat $\{U \mid U \subseteq A\text{-Modul } \mathbb{F}_2[\Omega]\}$ auch entsprechend weniger isomorphe Doubletten der Codes, die D als Automorphismengruppe haben – im Vergleich zur Anzahl dieser Codes, wenn sie als $\{U \mid U \subseteq \mathfrak{Z}_N\text{-Modul } \mathbb{F}_2[\Omega]\}$ erzeugt werden.
  Beispiel: $N = 49, A = PSL(3, 2) \wr PSL(3, 2)$, $D = \mathfrak{S}_7 \wr PSL(3, 2)$.
- Ist $A = Aut(C)$ wie oben definiert und aus Gruppenfaktoren zusammengesetzt, die **je** einen **eigenen** Isomorphie-Faktor > 1 haben, so gibt es eine Gruppe B[5] mit $\mathfrak{Z}_N < B < A$, so daß $\{U \mid U \subseteq B\text{-Modul } \mathbb{F}_2[\Omega]\}$ eine echte Teilmenge aller zu C isomorphen Codes liefert.
  Beispiel: $N = 49, A = PSL(3, 2) \wr PSL(3, 2)$, $B = \mathfrak{Z}_7 \wr PSL(3, 2)$.

Die Spezialisierung des Satzes 9.4 führt uns zum

[4] zur Definition eines modularen Verbandes siehe Definition 0.35
[5] B muß nicht notwendig eine volle Automorphismengruppe sein

Satz 9.9 (**Hauptsatz für lineare Codes**)
Sei G die triviale Permutationsgruppe $\langle 1\rangle_N$ und $\Omega = \mathbb{F}_2[\{1, 2, \ldots, N\}]$.
Dann sind die Untermoduln des G-Moduls $\mathbb{F}_2[\Omega]$ genau die sämtlichen linearen Codes C der Länge N.

Beweis. Der Beweis ergit sich als unmittelbare Folgerung aus Satz 9.4. □

Bemerkung 9.10
Wie bereits in der Einleitung bemerkt, gilt die folgende Inklusionskette (für eine bestimmte Codelänge N):

$$\{Zyklische\ Codes\} \subsetneqq \{Gruppencodes\} \subsetneqq \{Lineare\ Codes\} \subsetneqq \{Codes\} \tag{9.5}$$

Dabei ist die erste und die letzte Inklusion offensichtlich.
Die mittlere, nichttriviale Inklusion $\{Gruppencodes\} \subsetneqq \{Lineare\ Codes\}$ konnte nach Satz 9.9 mit **Magma** nachgewiesen werden:
Es wurden mit der Untermodul-Technik lineare Codes gefunden, die nicht als Gruppencodes erzeugt werden konnten. Ein einfaches Beispiel sei hier angefügt:

Beispiel 9.11 (**ein linearer Code, der kein Gruppencode ist)**

```
>C7;
[4, 2, 1] Linear Code over GF(2)
Generator Matrix:
[1 0 0 1]
[0 1 0 0]
>PG:=PermutationGroup(C7); PG;
Permutation group G acting on a set of cardinality 4
Order = 2
    (1, 4)
>
```

Nach **Magma** hat die kleinste Automorphismengruppe aller Gruppencodes der Länge 4 die Ordnung 4. Ein Gruppencode mit der Länge 4, dessen Automorphismengruppe die Ordnung 2 hat, existiert also nicht !

Mit einer letzten Aussage wollen wir dieses Kapitel beschließen:

Fakt 9.12
Sei G eine Gruppe, die auf $\Omega = \{1, 2, \ldots, N\}$ transitiv operiert. Dann gilt: Ein Untermodul des G-Moduls $\mathbb{F}_2[\Omega]$ ist durch seine Dimension **nicht** *eindeutig bestimmt.*

Beweis. Wir zeigen ein Gegenbeispiel auf: Sei $N = 21$ und $G = \mathfrak{S}_3 \times PSL(3, 2)$. Dann existieren 2 Untermoduln des G-Moduls $\mathbb{F}_2[\Omega]$ mit derselben Dimension $k = 15$. Da beide jedoch unterschiedliche Minimaldistanzen haben ($d = 3$, bzw. $d = 4$), können sie nicht gleich sein. □

9.1 Anwendungsbeispiel zum Nachweis der Existenz einer bestimmten Automorphismengruppe

Da sich die Berechnung der nichttrivialen Codes und ihrer Automorphismengruppen der Codelänge $N = 84$ aus den 15625 Rohcodes als äußerst schwierig darstellte und trotz eines Opteron-Rechners mit 16GB Arbeitsspeicher eine geschlossene Auswertung nicht mehr möglich war, habe ich die Erkenntnisse dieser Arbeit angewandt, um die Existenz der Automorphismengruppe des Satzes 3.14 auch für diese Codelänge nachzuweisen.
Zwar war die Automorphismengruppe $G = \mathfrak{S}_4 \times \mathfrak{S}_{21}$ nach (nur) 4084 von 15625 gerechneten Rohcodes als 203. Gruppe von 214 Automorphismengruppen gefunden worden, aber die gesuchte minimale Obergruppe $H = (\mathfrak{K}_4 \wr \mathfrak{S}_{21}) \rtimes \mathfrak{S}_3$ war noch nicht dabei.
Da wir nach Satz 3.14 und dem Beweis zu Satz 3.3 diese Gruppe auch hier als Obergruppe von $G = \mathfrak{S}_4 \times \mathfrak{S}_{21}$ erwarten, habe ich nach Satz 9.4 den G-Modul $\mathbb{F}_2[\Omega]$ gebildet und die Codes (als Untermoduln) mit ihren Automorphismengruppen berechnet. Tatsächlich finden wir hier die in den Sätzen 3.3 und 3.14 angegebenen $[84, k, d]$-Codes in der entsprechenden Anzahl und mit der zugehörigen Automorphismengruppe.
Wir wollen das nun im Detail diskutieren:

- wir bekommen alle Codes, die $G = \mathfrak{S}_4 \times \mathfrak{S}_{21}$ als Automorphismengruppe haben; das sind nach Satz 3.3 ein $[84, 24, 4]$-Code und sein dualer $[84, 60, 4]$-Code (Nr. 8, 9 in der Code-Liste auf der nächsten Seite).

- wir bekommen alle Codes, die $H = (\mathfrak{K}_4 \wr \mathfrak{S}_{21}) \rtimes \mathfrak{S}_3$ als Automorphismengruppe haben; das sind nach Satz 3.14 ein $[84, 23, 4]$-Code und sein dualer $[84, 61, 4]$-Code (Nr. 7, 10 in der Code-Liste auf der nächsten Seite).
  Damit haben wir die Existenz dieser Automorphismengruppe und ihrer zwei Codes auch für $N = 84$ nachgewiesen. Aufgrund der Konstruktion nach Satz 9.4 und wegen $ord(G) < ord(H)$ ist H eine echte Obergruppe von G.

- wir bekommen alle 4 Codes, die $\mathfrak{S}_4 \wr \mathfrak{S}_{21}$ als Automorphismengruppe haben, da dies wegen $\mathfrak{S}_4 \times \mathfrak{S}_{21} = \mathfrak{S}_4 \wr \mathfrak{S}_{21} \cap \mathfrak{S}_{21} \wr \mathfrak{S}_4$ eine Obergruppe von G ist;
  (Nr. 5, 6, 11, 12 in der Code-Liste auf der nächsten Seite).

- wir bekommen alle 4 Codes, die $\mathfrak{S}_{21} \wr \mathfrak{S}_4$ als Automorphismengruppe haben, da dies wegen $\mathfrak{S}_4 \times \mathfrak{S}_{21} = \mathfrak{S}_4 \wr \mathfrak{S}_{21} \cap \mathfrak{S}_{21} \wr \mathfrak{S}_4$ eine Obergruppe von G ist;
  (Nr. 3, 4, 13, 14 in der Code-Liste auf der nächsten Seite).

- wir bekommen alle 4 primitiven Codes, die $\mathfrak{S}_{84}$ als Automorphismengruppe haben;
  (Nr. 1, 2, 15, 16 in der Code-Liste auf der nächsten Seite).

Im Anschluß an die folgende Liste der Codes mit ihren Automorphismengruppen finden wir die nach Satz 9.4 betroffenen Automorphismengruppen

$$G = \mathfrak{S}_4 \times \mathfrak{S}_{21} \leq Aut(C) \leq \mathfrak{S}_{84} \tag{9.6}$$

in dem Hasse-Diagramm ihres Untergruppen-Verbandes dargestellt.

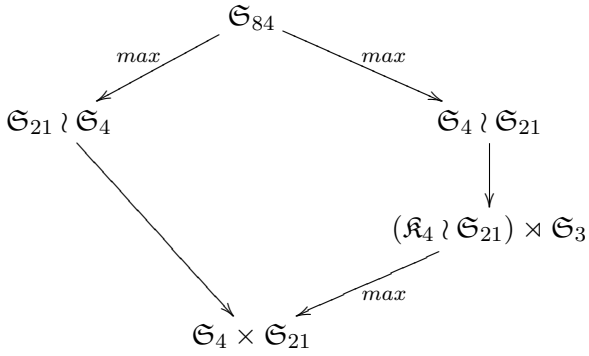
Beispiel 9.13 ($N = 84$**: Untermoduln des** $(\mathfrak{S}_4 \times \mathfrak{S}_{21})$**-Moduls** $\mathbb{F}_2[\Omega]$)

```
Erzeugungsungsprogramm der zyklischen Codes aus Untermoduln. Codelaenge 84
[
    GModule of dimension 0 over GF(2),
    GModule of dimension 1 over GF(2),
    GModule of dimension 3 over GF(2),
    GModule of dimension 4 over GF(2),
    GModule of dimension 20 over GF(2),
    GModule of dimension 21 over GF(2),
    GModule of dimension 23 over GF(2),
    GModule of dimension 24 over GF(2),
    GModule of dimension 60 over GF(2),
    GModule of dimension 61 over GF(2),
    GModule of dimension 63 over GF(2),
    GModule of dimension 64 over GF(2),
    GModule of dimension 80 over GF(2),
    GModule of dimension 81 over GF(2),
    GModule of dimension 83 over GF(2),
    GModule GMG of dimension 84 over GF(2)
]
16 Untermoduln erzeugt

Lineare Codes der Laenge n = 84 zu den obigen Untermoduln

Lfd.Nr.  k   d                          #AutoGroup

   1     0  84 331424013456535326699938757913013128800066628624204948711884603\2
38305913129171686412988572296871675315617792000000000000000000000
   2     1  84 331424013456535326699938757913013128800066628624204948711884603\2
38305913129171686412988572296871675315617792000000000000000000000
   3     3  42 163526028064096121024438564324550976808430710428330173085557719\0
40000000000000000
   4     4  21 163526028064096121024438564324550976808430710428330173085557719\0
40000000000000000
   5    20   8 492924026673884781804658957844169725791174656000\0
   6    21   4 492924026673884781804658957844169725791174656000\0
   7    23   4  13482020398038175409017297305600\00
   8    24   4              1226182612121026560000
   9    60   4              1226182612121026560000
  10    61   4  13482020398038175409017297305600\00
  11    63   2 492924026673884781804658957844169725791174656000\0
  12    64   2 492924026673884781804658957844169725791174656000\0
  13    80   2 163526028064096121024438564324550976808430710428330173085557719\0
40000000000000000
  14    81   2 163526028064096121024438564324550976808430710428330173085557719\0
40000000000000000
  15    83   2 331424013456535326699938757913013128800066628624204948711884603\2
38305913129171686412988572296871675315617792000000000000000000000
  16    84   1 331424013456535326699938757913013128800066628624204948711884603\2
38305913129171686412988572296871675315617792000000000000000000000
16 verschiedene Codes gefunden
```



Die 5 Automorphismengruppen zu den Untermoduln des $(\mathfrak{S}_4 \times \mathfrak{S}_{21})$-Moduls $\mathbb{F}_2[\Omega]$ im Untergruppenverband von $\mathfrak{S}_{84}$

Man beachte:
$(\mathfrak{K}_4 \wr \mathfrak{S}_{21}) \rtimes \mathfrak{S}_3 \cong (\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_{21}))/\mathfrak{S}_2^{21}$
$\mathfrak{S}_4 \times \mathfrak{S}_{21} = \mathfrak{S}_4 \wr \mathfrak{S}_{21} \cap \mathfrak{S}_{21} \wr \mathfrak{S}_4$

Legende: *max* an einer Verbandslinie bedeutet:
Die jeweils untere Gruppe ist maximale Untergruppe der oberen Gruppe.
$G_i \longleftarrow G_j$ bedeutet: $G_i < G_j$

Kapitel 10

Das Magische Dreieck

10.1 Die Automorphismengruppen $PSL(r, 2)$ und ihre Codes

Im Kapitel 8 haben wir die Hamming-Codes diskutiert und gesehen, daß die zugehörige Automorphismengruppe zum Hamming-Code $\mathcal{CH}_r$ die Gruppe $PSL(r, 2)$ ist.
Weiterhin ist bei der Untersuchung zutage getreten, daß mit zunehmendem Index r ($r \geq 3$) die Gruppe $PSL(r, 2)$ nicht nur vom Hamming-Code $\mathcal{CH}_r$ (und natürlich dem zugehörigen dualen Code $\mathcal{CH}_r^{\perp}$) angenommen wird, sondern daß jeweils ein weiteres Paar von Codes hinzukommt:

1. $r = 3$: die Gruppe $PSL(3, 2)$ wird von folgenden Codes angenommen:
   (a) vom $[7, 4, 3]$-Code (das ist der Hamming-Code $\mathcal{CH}_3$) und
   (b) vom dazu dualen $[7, 3, 4]$-Code.

   Zu beiden Codes existieren jeweils isomorphe Codes
2. $r = 4$: die Gruppe $PSL(4, 2)$ wird von folgenden Codes angenommen:
   (a) vom $[15, 11, 3]$-Code (das ist der Hamming-Code $\mathcal{CH}_4$) und
   (b) vom dazu dualen $[15, 4, 8]$-Code; aber zusätzlich noch
   (c) von einem $[15, 10, 4]$-Code und
   (d) dem dazu dualen $[15, 5, 7]$-Code.

   Zu diesen 4 Codes existieren jeweils isomorphe Codes
3. $r = 5$: die Gruppe $PSL(5, 2)$ wird von folgenden Codes angenommen:
   (a) vom $[31, 26, 3]$-Code (das ist der Hamming-Code $\mathcal{CH}_5$) und
   (b) vom dazu dualen $[31, 5, 16]$-Code; aber zusätzlich noch
   (c) von einem $[31, 25, 4]$-Code und
   (d) dem dazu dualen $[15, 6, 15]$-Code, sowie zusätzlich noch
   (e) von einem $[31, 16, 7]$-Code und
   (f) dem dazu dualen $[15, 15, 8]$-Code.

Zu diesen 6 Codes existieren jeweils 5 isomorphe Codes

usw.
Hierbei zeigten sich (außer der Zunahme der Codeanzahl) weitere interessante Phänomene:

1. Die sprunghafte Erhöhung (Quantensprung) des „Isomorphie-Faktors“ setzt sich weiter fort und wird im Kapitel 0.1 näher untersucht.

2. die Dimensionen der oben aufgeführten Codes sind genau die Dimensionen k der Untermoduln[1] zum $PSL(r,2)$-Modul $\mathbb{F}_2[\{1,2,\ldots,N\}]$
(mit $k \neq 0,1$ und $k \neq N, N-1$, wobei hier $N = 2^r - 1$ gilt). Dazu geben wir nach dieser Aufzählung ein Beispiel.

3. die Minimaldistanzen der oben aufgeführten Codes unterliegen der folgenden Gesetzmäßigkeit:

   - $d = 3$ $(=2^2-1)$ für den Hamming-Code $\mathcal{CH}_r$
   - $d = 4$ $(=2^2)$ für den Code[2], dessen Dimension um 1 niedriger ist
   - $d = 7$ $(=2^3-1)$ für den Code[3], dessen Dimension niedriger ist, als die des vorigen Codes $(r \geq 4)$
   - $d = 8$ $(=2^3)$ für den Code, dessen Dimension um 1 niedriger ist $(r \geq 4)$
   - $\cdots$, usw., bis
   - $d = 2^{r-1}$ für den Code mit der kleinsten Dimension – das ist der duale Code zum Hamming-Code $\mathcal{CH}_r$

Das bedeutet, daß die eine Hälfte der Codes eine Minimaldistanz mit der Folge $4, 8, 16, \ldots, 2^{r-1}$ hat, während die andere Hälfte der dualen Codes eine Minimaldistanz mit der Folge $3, 7, 15, \ldots, 2^{r-1} - 1$ hat. Diese letzte Folge ist gleichzeitig – um den Wert 1 ergänzt – auch die Folge der Anzahl der fehlerkorrigierten Bits.

Hier nun das angekündigte Beispiel:

Beispiel 10.1 (**Untermoduln des $PSL(5,2)$-Moduls $\mathbb{F}_2[\{1,2,\ldots,N\}]$**)

```
> GMP5:=GModule(PSL(5,2),GF(2)); Submodules(GMP5);
[
    GModule of dimension 0 over GF(2),
    GModule of dimension 1 over GF(2),
    GModule of dimension 5 over GF(2),
    GModule of dimension 6 over GF(2),
    GModule of dimension 15 over GF(2),
    GModule of dimension 16 over GF(2),
    GModule of dimension 25 over GF(2),
    GModule of dimension 26 over GF(2),
    GModule of dimension 30 over GF(2),
    GModule GMP5 of dimension 31 over GF(2)
]
```

[1] im Kapitel 9 sehen wir, daß diese Codes mit den Untermoduln identisch sind !
[2] wir wollen diesen Code $\mathcal{HB}4_r$ nennen
[3] wir wollen diesen Code $\mathcal{HB}7_r$ nennen

r	N		$[k,d]$					
3	7		[3,4]					
3	7	dual	**[4,3]**					
4	15		[4,8]	[10,4]				
4	15	dual	**[11,3]**	[5,7]				
5	31		[5,16]	[15,8]	[25,4]			
5	31	dual	**[26,3]**	[16,7]	[6,15]			
6	63		[6,32]	[21,16]	[41,8]	[56,4]		
6	63	dual	**[57,3]**	[42,7]	[22,15]	[7,31]		
7	127		[7,64]	[28,32]	[63,16]	[98,8]	[119,4]	
7	127	dual	**[120,3]**	[99,7]	[64,15]	[29,31]	[8,63]	
8	255		[8,128]	[36,64]	[92,32]	[162,16]	[218,8]	[246,4]
8	255	dual	**[247,3]**	[219,7]	[163,15]	[93,31]	[37,63]	[9,127]

Tabelle 10.1: Dimensionen k und Minimaldistanzen d der Codes zu den Automorphismengruppen $PSL(r,2)$. Darunter befinden sich die Angaben zu den dualen Codes; die Werte zu den **Hamming**-Codes sind fett gedruckt $(N = 2^r - 1)$.

Dabei gehören die ersten beiden, sowie die letzten beiden Untermoduln zu den 4 primitiven Codes mit $\mathfrak{S}_N$ als Automorphismengruppe.
Die Untermoduln dazwischen sind alle Codes (ohne Isomorphien, s. dazu auch Kapitel 0.1), die $PSL(5,2)$ als Automorphismengruppe haben.
Ende des Beispiels

Wir wollen diese beobachteten Phänomene nun allgemein beweisen. Dazu benötigen wir zunächst eine Bezeichnung und einen Hilfssatz.

Bezeichnung 10.2
Sei $\Omega = \{1, 2, \ldots, \mathbb{N}\}$, $(N = 2^r - 1)$ die Menge, auf der $PSL(r,2)$ transitiv operiert.
Der zugehörige $PSL(r,2)$-Modul ist dann $\mathbb{F}_2[\Omega]$.

Hilfssatz 10.3
Die zyklische Permutation der Ordnung $|\Omega|$ auf Ω ist in $PSL(r,2)$ enthalten.

Beweis. Da der Hamming-Code $\mathcal{CH}_r$ zyklisch ist und $PSL(r,2)$ als Automorphismengruppe hat, folgt daraus die Behauptung. □

Folgerung 10.4
Sei $U \subseteq \mathbb{F}_2[\Omega]$ ein $PSL(r,2)$-Untermodul.
Dann ist U ein zyklischer Code (weil die zyklische Permutation in $PSL(r,2)$ enthalten ist).

Es gilt:

Satz 10.5
$Aut(U) = PSL(r,2)$.

Beweis. Nach Satz 9.4 gilt: $Aut(U) \geq PSL(r,2)$.
Nach Folgerung 9.5 gilt $Aut(U) \lneqq \mathfrak{S}_N$, mit $N = 2^r - 1$.
Da zwischen $PSL(r,2)$ und $\mathfrak{S}_N$ im Untergruppenverband von $\mathfrak{S}_N$ keine weitere Automorphismengruppe eines zyklischen Codes der Länge N existiert[4], folgt daraus die Behauptung. □

Nun wollen wir noch abschließend Aussagen zur Anzahl und Dimension der Codes U machen.

Satz 10.6
Die Anzahl der Codes U mit $PSL(r,2)$ als Automorphismengruppe ist

$$|\{U\}| \ = 2 \cdot (r-2). \tag{10.1}$$

Beweis. In einem Aufsatz hat Abdukhalikov [1] die Existenz und Beschaffenheit einer Inklusionskette von Untermoduln des $PSL(r,2)$-Moduls $\mathbb{F}_2[\Omega]$ bewiesen:

$$0 = M_0 \subset M_1 \subset M_2 \subset \cdots \subset M_{r-2} \subset M_{r-1} = \mathcal{F}_0 \subset M_r = \mathcal{F} = \mathbb{F}_2[\Omega]. \tag{10.2}$$

Dabei ist in der Konstruktion von Abdukhalikov $\mathcal{F}_0$ derjenige Untermodul mit der Dimension $k = N - 1$, bzw. $k = 2^r - 2$. Dieser Untermodul ist einer der 4 primitiven Codes der Länge N (es ist der „zweite Elementarcode“, s. Abschnitt 2.1) mit $\mathfrak{S}_N$ als Automorphismengruppe. Ebenso ist der Untermodul M_0 einer der 4 primitiven Codes der Länge N (es ist der „Nullcode“, s. Abschnitt 2.1) mit $\mathfrak{S}_N$ als Automorphismengruppe.
Es bleiben in dieser Inklusionskette also nur die Untermoduln M_1 bis M_{r-2} als nichttriviale Codes übrig. Das sind genau $r-2$ Codes.
Durch die Konstruktion von Abdukhalikov, nämlich die Untermoduln von $\mathcal{F}_0$ zu bilden, anstatt von $\mathcal{F} = \mathbb{F}_2[\Omega]$, wird nur die Hälfte aller Codes ermittelt: es fehlen noch die dazu dualen Codes. Damit sind es dann endlich $2 \cdot (r-2)$ Codes mit $PSL(r,2)$ als Automorphismengruppe. □

Die Dimension der einzelnen Untermoduln M_i ist in einem Aufsatz von Zalesskii [17] bewiesen worden und hier in einer Tabelle 10.2 zusammengestellt, die wir später noch für ein weiteres Phänomen benötigen.
Die Dimension der $r-2$ dualen Codes läßt sich anhand der Tabelle 10.2 nach der Formel

$$k = 2^r - 1 - \dim(M_i) \tag{10.3}$$

leicht errechnen, ist aber bereits in die Tabelle 10.1 eingetragen worden – ebenso, wie die zugehörigen Minimaldistanzen.

[4] s. [6]: $PSL(r,2)$ ist maximal unterhalb von $\mathfrak{A}_N$ und die Gruppe $\mathfrak{A}_N$ tritt bei zyklischen Codes nicht als Automorphismengruppe auf

Für die Minimaldistanzen d gelten die folgenden Formeln:

$$md(M_{r-i}) = 2^i, \quad (i = 2, \ldots, r-1), \tag{10.4}$$

bzw. für die dualen Codes

$$md(M_j^{\perp}) = 2^{j+1} - 1, \quad (j = 1, \ldots, r-2). \tag{10.5}$$

(Für den praktischen Einsatz kann man natürlich sämtliche $2 \cdot (r-2)$ Codes direkt aus den Untermoduln von $\mathbb{F}_2[\Omega]$ gewinnen – so, wie im Beispiel 10.1 oben gezeigt.)

Bemerkung 10.7
Die Hamming-Codes sind nach der Konstruktion von Abdukhalikov jeweils die dualen Codes zu M_1: Sie haben von allen nicht-primitiven Untermoduln die höchste Dimension ($k = 2^r - 1 - r$) und die geringste Minimaldistanz ($d = 3$).

Interessant ist in diesem Zusammenhang die von mir so benannte Code-Familie der $\mathcal{HB}4_r$-Codes. Sie sind in der Tabelle 10.1 auf dem rechten Zweig gut zu erkennen: Sie gehören jeweils zum Untermodul M_{r-2} und haben mit
$k = 2^r - 2 - r$ eine geringfügig kleinere Effizienz ($R = k/N$), aber mit $d \equiv 4$ eine bessere Zuverlässigkeit ($\delta = d/N$) als die Hamming-Codes. Sie können daher 2-Bit-Fehler erkennen (s. dazu auch Abschnitt 10.4).

Interessant ist in diesem Zusammenhang besonders die von mir so benannte Code-Familie der $\mathcal{HB}7_r$-Codes. Sie sind in der Tabelle 10.1 gut zu erkennen, nämlich in der Diagonal-Spalte rechts von den Hamming-Codes: Sie sind nach der Konstruktion von Abdukhalikov jeweils die dualen Codes zu M_2: Sie haben zwar eine kleinere Effizienz ($R = k/N$), aber mit $d \equiv 7$ eine deutlich bessere Zuverlässigkeit ($\delta = d/N$) als die Hamming-Codes. Sie können daher 3-Bit-Fehler korrigieren (s. dazu auch Abschnitt 10.4).

10.2 Die Automorphismengruppen $Aut(\mathcal{C}) \cong (\mathfrak{S}_2 \wr PSL(r,2))/\mathfrak{S}_2^y$ und ihre Codes

Bei den Codelängen $N = 2 \cdot (2^r - 1)$ treten – zusätzlich zu den im Kap. 1 beschriebenen Automorphismengruppen mit ihren zugehörigen Codes – nicht nur die im Kapitel „Vererbung“ beschriebenen Mehrfachcodes mit der Automorphismengruppe $\mathfrak{S}_2 \wr PSL(r,2)$ und ebenfalls dort beschriebene weitere Codes[5] mit der Automorphismengruppe $PSL(r,2) \wr \mathfrak{S}_2$ auf (siehe separaten Abschnitt 10.3), sondern auch noch eine zunehmende Anzahl von Codes, welche zu einer zunehmenden Anzahl von Automorphismengruppen gehören, die zu verminderten Kranzprodukten $(\mathfrak{S}_2 \wr PSL(r,2))/\mathfrak{S}_2^y$ isomorph sind.
Das soll später in zwei Tabellen veranschaulicht werden.
Für das Verständnis und auch für die Gewinnung dieser zahlreichen Codes bedienen wir uns der folgeden Erkenntnisse und Techniken:

1. Lineare Codes sind Untermoduln eines G-Moduls über $\mathbb{F}_2$ (s. Kap. 9)
2. diese Untermoduln bilden einen Verband (siehe Grafik im Beispiel 10.11)
3. die Plotkin-Summe (s. Abschnitt 2.2) verknüpft zwei Codes der Länge l zu einem neuen Code der Länge $N = 2 \cdot l$.

Nomenklatur: Um einerseits die Konsistenz mit der Literatur[1] zu erhalten und andererseits Information über die Dimension der Untermoduln zu vermitteln, haben wir zwei Bezeichnungen für unsere Untermoduln gewählt:

1. M_i, wie in $0 = M_0 \subset M_1 \subset M_2 \subset \cdots \subset M_{r-2} \subset M_{r-1} = \mathcal{F}_0$: Hier gibt der Index die Position des Untermoduls in der Inklusionskette an.
2. U_k oder $\mathcal{U}_k$: Hier gibt der Index die Dimension des Untermoduls an, also $k = \dim(U_k)$.

Aus den Beobachtungen der Codelängen $N = 14$, 30 und 62 formulieren wir den folgenden

Satz 10.8
Für Codelängen $N = 2 \cdot l$ mit $l = 2^r - 1$, $r \geq 3$ existieren jeweils $r - 2$ Automorphismengruppen in der Form eines „verminderten[6]“ Kranzprodukts

$$(\mathfrak{S}_2 \wr PSL(r,2))/\mathfrak{S}_2^y, \tag{10.6}$$

wobei y die Werte nach einem Rekursionsgesetz annimmt (siehe dazu auch Tabelle 10.2 und Rekursionsformel unten).

Bemerkung 10.9
Diese ausdividierten Normalteiler $\mathfrak{S}_2^y$ sind gleichzeitig Untermoduln der $PSL(r,2)$-Moduln $\mathbb{F}_2[\Omega]$ und repräsentieren selbst zyklische Codes der Länge $2^n - 1$ mit $PSL(r,2)$ als Automorphismengruppe. Dabei sind dann die y-Werte die Dimensionen dieser Codes (s. a. Abschnitt 10.1).

[5] wir hatten dort von „Rückwärtsvererbung“ gesprochen und die Plotkin-Summe eingeführt.
[6] Diese Konstruktion basiert auf einem von der $PSL(r,2)$-Gruppe induzierten G-Modul über $\mathbb{F}_2$

r	l	N	y
3	7	14	**3**
4	15	30	4 10
5	31	62	5 **15** 25
6	63	126	6 21 41 56
7	127	254	7 28 **63** 98 119
8	255	510	8 36 92 162 218 246
9	511	1022	9 45 129 **255** 381 465 501
10	1023	2046	10 55 175 385 637 847 967 1012
11	2047	4094	11 66 231 561 **1023** 1485 1815 1980 2035

Tabelle 10.2: Exponenten y der Automorphismengruppen $Aut(\mathcal{C}) \cong (\mathfrak{S}_2 \wr PSL(r,2))/\mathfrak{S}_2^y$, $l = 2^r - 1$, $N = 2 \cdot l$

In jeder Zeile der Tabelle 10.2 erkennt man hierbei einen „Mittelpunkt“ (fettgedruckt für r ungerade) $mp = (l-1)/2 = 2^{r-1} - 1$, um den herum die Werte von y symmetrisch angeordnet sind; außerdem erkennt man eine **Rekursion**, die sich ähnlich dem Pascal'schen Dreieck darstellen läßt:

Rekursionsformel (die Angaben gelten pro Zeile):

- Erster Wert:= r.
- Letzter Wert:= $r + 2\cdot$(letzter Wert der Vorzeile) oder $2^r - 2 - r$.
- Zwischenwert:= 1+ Summe der beiden benachbarten Werte oberhalb in der Vorzeile.

Ende der Rekursionsformel

Beweis. Für $r = 3$, 4 und 5 ergibt sich der Beweis aus den durchgeführten Untersuchungen[7] (siehe Tabellenwerk $N = 14$, 30, 62).
Den allgemeinen Beweis für beliebiges $r \geq 3$ führen wir anhand eines Aufsatzes von Abdukhalikov [1] (s.a. Abschnitt 10.1): Dort hat Abdukhalikov die Existenz und Beschaffenheit einer jeweiligen Inklusionskette von Untermoduln des $PSL(r,2)$-Moduls $\mathbb{F}_2[\Omega]$ bewiesen:

$$0 = M_0 \subset M_1 \subset M_2 \subset \cdots \subset M_{r-2} \subset M_{r-1} = \mathcal{F}_0 \tag{10.7}$$

Dabei gilt obendrein:

$$M_{r-1} = \mathcal{F}_0 \subset M_r = \mathbb{F}_2[\Omega] \quad \text{mit} \quad \mathcal{F}_0 \oplus \langle 1 \rangle = \mathbb{F}_2[\Omega]. \tag{10.8}$$

[7] Gerne hätte ich diese Aussagen für $r = 6$ durch entsprechende Automorphismengruppen weiter abgesichert, doch die Anzahl von über 1,5 Millionen Rohcodes für $N = 126$ läßt dies z.Zt. nicht vollständig zu. Ich habe aber zumindest die Automorphismengruppen $\mathfrak{S}_2 \wr PSL(6,2)$, sowie $(\mathfrak{S}_2 \wr PSL(6,2))/\mathfrak{S}_2^{56}$ in der vorhergesagten Anzahl nachweisen können.

Verbandsraster-Abstand $\mathcal{VRA}_{ba} = r-$				2	3	4	5	...	*1*
r	l	N	z	↙	↙	↙	↙		M
3	7	14	*2*	↙	↙	↙			*4*
4	15	30	*2*	*5*	↙	↙			*8*
5	31	62	*2*	*5*	*8*	↙			*12*
6	63	126	*2*	*5*	*8*	*12*			*16*
7	127	254	*2*	*5*	*8*	*12*	*16*		*20*
8	255	510	*2*	*5*	*8*	*12*	*16*	*20*	*24*
9	511	1022	*2*	*5*	*8*	*12*	*16*	*20*	*24*	*28*
10	1023	2046	*2*	*5*	*8*	*12*	*16*	*20*	*24*	*28*	*32*
11	2047	4094	*2*	*5*	*8*	*12*	*16*	*20*	*24*	*28*	*32*	*36*

Tabelle 10.3: Anzahl z der Codes (ohne Isomorphien) zu den Automorphismengruppen $Aut(\mathcal{C}) \cong (\mathfrak{S}_2 \wr PSL(r,2))/\mathfrak{S}_2^y$, $l = 2^r - 1$, $N = 2 \cdot l$ (s. Tabelle 10.2);
M:=Anzahl der Codes (ohne Isomorphien) zu den Automorphismengruppen $\mathfrak{S}_2 \wr PSL(r,2)$.

Die Dimension der einzelnen Untermoduln ist in einem Aufsatz von Zalesskii [17] bewiesen worden. □

Wir wollen das hier mit **Magma** für $r = 6$ einmal beispielhaft durchrechnen:

Beispiel 10.10 (Untermoduln des $PSL(6,2)$-Moduls $\mathbb{F}_2[\Omega]$)

```
>> GMP6:=GModule(PSL(6,2),GF(2));  Submodules(GMP6);
[
    GModule of dimension 0 over GF(2),
    GModule of dimension 1 over GF(2),
    GModule of dimension 6 over GF(2),
    GModule of dimension 7 over GF(2),
    GModule of dimension 21 over GF(2),
    GModule of dimension 22 over GF(2),
    GModule of dimension 41 over GF(2),
    GModule of dimension 42 over GF(2),
    GModule of dimension 56 over GF(2),
    GModule of dimension 57 over GF(2),
    GModule of dimension 62 over GF(2),
    GModule GMP6 of dimension 63 over GF(2)
]
> LGMP6:=Submodules(GMP6);
> Submodules(LGMP6[#LGMP6-1]);
[
    GModule of dimension 0 over GF(2),
    GModule of dimension 6 over GF(2),
    GModule of dimension 21 over GF(2),
    GModule of dimension 41 over GF(2),
    GModule of dimension 56 over GF(2),
    GModule of dimension 62 over GF(2)
]
```

Den Untermodul $\mathcal{F}_0$ gewinnen wir nach ABDUKHALIKOV [1] aus der ersten Untermodul-Liste mit der Dimension $k = N - 1$ (=62).
In der danach erzeugten zweiten Liste finden wir, daß die Dimensionen der Untermoduln M_1 bis M_4 mit den im Magischen Dreieck angegebenen Exponenten übereinstimmen, so daß wir die folgende Inklusionskette der Untermoduln M_i, bzw. U_k bekommen:

$$0 = M_0 \subset M_1 \subset M_2 \subset M_3 \subset M_4 \subset M_5 = \mathcal{F}_0 \tag{10.9}$$

$$0 = U_0 \subset U_6 \subset U_{21} \subset U_{41} \subset U_{56} \subset U_{62} = \mathcal{F}_0 \tag{10.10}$$

Da diese Untermoduln auch als Normalteiler von $\mathfrak{S}_2 \wr PSL(6,2)$ auftreten, kann man die entsprechenden Automorphismengruppen durch Ausdividieren bekommen:

$$(\mathfrak{S}_2 \wr PSL(6,2))/\mathfrak{S}_2^{|M_i|}, i = 1, \cdots, 4 \tag{10.11}$$

Dabei gilt noch insbesondere:

$$\mathfrak{S}_2 \wr PSL(r,2) = (\mathfrak{S}_2 \wr PSL(r,2))/\mathfrak{S}_2^{|M_0|}. \tag{10.12}$$

10.2.1 Beispiel für $(\mathfrak{S}_2 \wr PSL(4,2))/\mathfrak{S}_2^y$ und ihre Codes

Um diesen durchgängigen Beispiel-Abschnitt noch überschaubar zu halten, benötigen wir ein kleineres Ausgangsbeispiel. Daher wurde die zweite Zeile der Tabellen zum Magischen Dreieck gewählt (s. Tabellen 10.2 und 10.3).
Bevor wir jedoch die zugehörige Codelänge $N = 30$ mit den zugehörigen Automorphismengruppen $(\mathfrak{S}_2 \wr PSL(4,2))/\mathfrak{S}_2^y$ und deren Codes diskutieren, müssen wir zunächst die Untermoduln des $PSL(4,2)$-Moduls $\mathbb{F}_2[\Omega]$ ermitteln (Codelänge $l = 15$):

Beispiel 10.11 (**Untermoduln des** $PSL(4,2)$**-Moduls** $\mathbb{F}_2[\Omega]$)

```
> GMP4:=GModule(PSL(4,2),GF(2)); Submodules(GMP4);
[
    GModule of dimension 0 over GF(2),
    GModule of dimension 1 over GF(2),
    GModule of dimension 4 over GF(2),
    GModule of dimension 5 over GF(2),
    GModule of dimension 10 over GF(2),
    GModule of dimension 11 over GF(2),
    GModule of dimension 14 over GF(2),
    GModule GMP4 of dimension 15 over GF(2)
]
> LGMP4:=Submodules(GMP4);
> Submodules(LGMP4[7]);
[
    GModule of dimension 0 over GF(2),
    GModule of dimension 4 over GF(2),
    GModule of dimension 10 over GF(2),
    GModule of dimension 14 over GF(2)
]
>
```

Den Untermodul $\mathcal{F}_0$ gewinnen wir nach ABDUKHALIKOV [1] aus der ersten Untermodul-Liste mit der Dimension $k = l - 1$ (=14).
In der danach erzeugten zweiten Liste finden wir, daß die Dimensionen der Untermoduln M_1 bis M_2 mit den im Magischen Dreieck angegebenen Exponenten (4 und 10) übereinstimmen.
Für die spätere Diskussion und Verständnis der Codes ist es wichtig, neben der Inklusionskette nach ABDUKHALIKOV

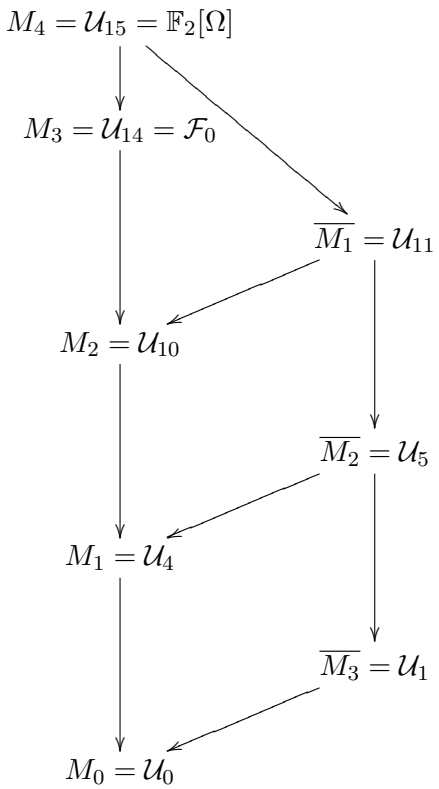
$$0 = M_0 \subset M_1 \subset M_2 \subset M_3 = \mathcal{F}_0 \tag{10.13}$$

$$0 = U_0 \subset U_4 \subset U_{10} \subset U_{14} = \mathcal{F}_0 \tag{10.14}$$

auch den gesamten Untermodulverband zu bestimmen. Auch hier hilft **Magma**.
Wir greifen stellvertretend 2 Prüfungen heraus:

```
> M_3_quer:=LGMP4[2]; M_1:=LGMP4[3]; M_3_quer subset M_1;
false
> M_2_quer:=LGMP4[4]; M_1 subset M_2_quer;
true
```

und konstruieren damit den Untermodulverband des $PSL(4,2)$-Moduls $\mathbb{F}_2[\Omega]$:



Untermodulverband des $PSL(4,2)$-Moduls $\mathbb{F}_2[\Omega]$

Legende: M_i gibt den Untermodul mit seiner Position i in der ABDUKHALIKOV-Kette an.
$\mathcal{U}_k$ gibt den Untermodul mit seiner Dimension k an.
$\mathcal{U}_i \longleftarrow \mathcal{U}_j$ bedeutet: $\mathcal{U}_i \subset \mathcal{U}_j$

Beispiel 10.12 (**Anzahl der Codes aus Untermoduln zum Magischen Dreieck)**

```
> G10:=AutoGroups[10];G:=G10;#G10;
645120
Erzeugungsungsprogramm der linearen Codes aus Untermoduln.
Codelaenge 30
[
    GModule of dimension 0 over GF(2),
    GModule of dimension 1 over GF(2),
    GModule of dimension 4 over GF(2),
    GModule of dimension 5 over GF(2),
    GModule of dimension 6 over GF(2),
    GModule of dimension 10 over GF(2),
    GModule of dimension 11 over GF(2),
    GModule of dimension 12 over GF(2),
    GModule of dimension 14 over GF(2),
    GModule of dimension 14 over GF(2),
    GModule of dimension 15 over GF(2),
    GModule of dimension 15 over GF(2),
    GModule of dimension 16 over GF(2),
    GModule of dimension 16 over GF(2),
    GModule of dimension 18 over GF(2),
    GModule of dimension 19 over GF(2),
    GModule of dimension 20 over GF(2),
    GModule of dimension 24 over GF(2),
    GModule of dimension 25 over GF(2),
    GModule of dimension 26 over GF(2),
    GModule of dimension 29 over GF(2),
    GModule GMG of dimension 30 over GF(2)
]
22 Untermoduln. Lineare Codes zu den obigen Untermoduln:

Lfd.Nr.  k   d                            #AutoGroup

   1     0  30   265252859812191058636308480000000
   2     1  30   265252859812191058636308480000000
   3     4  16                             660602880
   4     5  14                             660602880
   5     6  14                                645120
   6    10   8                             660602880
   7    11   6                             660602880
   8    12   6                              41287680
   9    14   8                                645120
  10    14   4                    42849873690624000
  11    15   6                                645120
  12    15   2                    42849873690624000
  13    16   6                                645120
  14    16   2                    42849873690624000
  15    18   4                              41287680
  16    19   2                             660602880
  17    20   2                             660602880
  18    24   4                                645120
  19    25   2                             660602880
  20    26   2                             660602880
  21    29   2   265252859812191058636308480000000
  22    30   1   265252859812191058636308480000000
22 verschiedene Codes gefunden
```

```
> G27:=AutoGroups[27]; G:=G27; #G27;
41287680
Erzeugungsungsprogramm der linearen Codes aus Untermoduln.
Codelaenge 30
[
    GModule of dimension 0 over GF(2),
    GModule of dimension 1 over GF(2),
    GModule of dimension 4 over GF(2),
    GModule of dimension 5 over GF(2),
    GModule of dimension 10 over GF(2),
    GModule of dimension 11 over GF(2),
    GModule of dimension 12 over GF(2),
    GModule of dimension 14 over GF(2),
    GModule of dimension 15 over GF(2),
    GModule of dimension 16 over GF(2),
    GModule of dimension 18 over GF(2),
    GModule of dimension 19 over GF(2),
    GModule of dimension 20 over GF(2),
    GModule of dimension 25 over GF(2),
    GModule of dimension 26 over GF(2),
    GModule of dimension 29 over GF(2),
    GModule GMG of dimension 30 over GF(2)
]
17 Untermoduln. Lineare Codes zu den obigen Untermoduln:

Lfd.Nr.  k   d                          #AutoGroup

   1     0  30   265252859812191058636308480000000
   2     1  30   265252859812191058636308480000000
   3     4  16                            660602880
   4     5  14                            660602880
   5    10   8                            660602880
   6    11   6                            660602880
   7    12   6                             41287680
   8    14   4                   42849873690624000
   9    15   2                   42849873690624000
  10    16   2                   42849873690624000
  11    18   4                             41287680
  12    19   2                            660602880
  13    20   2                            660602880
  14    25   2                            660602880
  15    26   2                            660602880
  16    29   2   265252859812191058636308480000000
  17    30   1   265252859812191058636308480000000
17 verschiedene Codes gefunden

Code-Nr. aus obiger Liste ?
7
Code-Nr. der Vergleichscodes aus Codefilezyk30 ?
122, 134

Lfd.Nr.  k   d

 122    12   6  Code Nr.7 aus Untermodul ist identisch
 134    12   6  Code Nr.7 aus Untermodul ist isomorph
```

Erklärungen zum obigen Beispiel:
Die zugehörige Codelänge ist $N = 30$ und die zugehörigen Automorphismengruppen sind demnach:
G3=$\mathfrak{S}_2 \wr PSL(4,2)$ mit der Ordnung 660602880, sowie insbesondere
G10=$(\mathfrak{S}_2 \wr PSL(4,2))/\mathfrak{S}_2^{10}$ mit der Ordnung 645120 und
G27=$(\mathfrak{S}_2 \wr PSL(4,2))/\mathfrak{S}_2^{4}$ mit der Ordnung 41287680.
In der Tabelle der Automorphismengruppen im Anhang E haben diese 3 Gruppen die Nummern 3, 10 und 27.

- Da die Untermoduln (und somit auch die Codes) nach Dimension aufsteigend sortiert sind, ist durch die Angabe der Ordnung der zugehörigen Automorphismengruppen die Dualität der Codes und ihrer Unterräume (=Untermoduln) in Spiegelsymmetrie gut erkennbar. Selbstduale Codes sind bei dieser Liste daher in der Mitte zu finden.

- Wie bereits an anderer Stelle bemerkt, treten bei dieser Konstruktion die Codes ohne isomorphe Doubletten auf (s. Bsp. oben für Code-Nr. 7).

- In der ersten obigen Auswertung haben wir den G-Modul zur Gruppe G10 über $\mathbb{F}_2$ gebildet. Da dies die kleinste Gruppe im Teilverband ist, bekommen wir daraus auch die meisten Codes, nämlich 22.
  Die in der Tabelle 10.3 vorhergesagte Anzahl der Codes (8 Codes für G3, 5 Codes für G10, 2 Codes für G27) ist gut überprüfbar.
  Das sind in der Summe 15 Codes. Welches sind die restlichen 7 Codes ?
  Nach Folgerung 9.5 sind stets die 4 primitiven Codes in der Untermodul-Liste enthalten – fehlen uns also nur noch drei:
  Da folgende Relation gilt:
  $(\mathfrak{S}_2 \wr PSL(4,2))/\mathfrak{S}_2^4 < \mathfrak{S}_2 \wr PSL(4,2) < \mathfrak{S}_2 \wr \mathfrak{S}_{15} < \mathfrak{S}_{30}$,
  sind dies nach Satz 9.4 genau die typischen 3 Codes (s. Kapitel 1.2) zur Automorphismengruppe $\mathfrak{S}_2 \wr \mathfrak{S}_{15}$ mit der Ordnung 42849873690624000.

- In der zweiten obigen Auswertung haben wir den G-Modul zur Gruppe G27 über $\mathbb{F}_2$ gebildet. Da folgende Relation gilt:
  $(\mathfrak{S}_2 \wr PSL(4,2))/\mathfrak{S}_2^{10} < (\mathfrak{S}_2 \wr PSL(4,2))/\mathfrak{S}_2^{4}$, d. h. also: G10 < G27,
  bekommen wir nach Satz 9.6 und Folgerung 9.7 in dieser Auswertung genau die 5 Codes nicht mehr, die G10 als Automorphismengruppe haben.

10.2.2 Die Codes zu $(\mathfrak{S}_2 \wr PSL(r,2))/\mathfrak{S}_2^y$

Zum besseren Verständnis der zahlreichen zyklischen Codes, deren Automorphismengruppen isomorph zu $(\mathfrak{S}_2 \wr PSL(r,2))/\mathfrak{S}_2^y$ sind, benötigen wir die PLOTKIN-Summe (s. a. 2.2). Daher wollen wir die Definition hier noch einmal wiederholen:

Definition 10.13 (PLOTKIN-Summe)
Seien $\mathcal{C}_1$ und $\mathcal{C}_2$ zwei Codes über demselben Alphabet (hier: über $\mathbb{F}_2$).
Dann ist $\mathcal{P}(\mathcal{C}_1,\mathcal{C}_2) := \{(u, u+v) \mid u \in \mathcal{C}_1, v \in \mathcal{C}_2\}$ die PLOTKIN-Summe der beiden Codes.
Das Ergebnis ist ein $[N_1 + max(N_1,N_2), k_1 + k_2, min(2 \cdot d_1, d_2)]$-Code.

Im Folgenden sei $\mathcal{U}_k$ ein zyklischer Code der Länge $l = 2^r - 1$ und Dimension k $(0 < k < l)$, der ein Untermodul des $PSL(r,2)$-Moduls $\mathbb{F}_2[\Omega]$ ist. Die Menge dieser $\mathcal{U}_k$ ist genau die Menge der Untermoduln $M_1 \ldots M_{r-1} = \mathcal{F}_0$ aus der ABDUKHALIKOV-Kette und ihrer dualen Untermoduln, also:

$$\mathcal{U}_k \in \{M_1, \ldots, M_{r-1} = \mathcal{F}_0\} \cup \{\overline{M_1}, \ldots, \overline{M_{r-1}} = \overline{\mathcal{F}_0}\} \tag{10.15}$$

Um nun den Bildungsprozeß mit der PLOTKIN-Summe $\mathcal{P}(\mathcal{U}_b,\mathcal{U}_a)$ für unsere Codes (in diesem Abschnitt) zu verstehen, wollen wir einige Regeln[8] aufstellen:

1. $\mathcal{U}_a \subset \mathcal{U}_b$ (s. dazu den Untermodulverband im Bsp. zu $PSL(4,2)$ oben)
2. $\dim(\mathcal{U}_b) - \dim(\mathcal{U}_a) > 1$

Wir wollen diese Regeln auf das obige Beispiel mit $PSL(4,2)$ anwenden.
Da wir das Bildungsgesetz für die Untermoduln der $PSL(r,2)$-Moduln $\mathbb{F}_2[\Omega]$ – wie auch das Bildungsgesetz für die Minimaldistanzen der Untermoduln gefunden, und in der Tabelle 10.1 zusammengefaßt haben, können wir – entsprechend der Definition der PLOTKIN-Summe – jetzt diese 7 Codes mit ihren Attributen k und d angeben:

Beispiel 10.14
Wir können folgende Codes bilden:

1. $\mathcal{P}(\mathcal{U}_5,\mathcal{U}_1)$ ist ein $[30,6,14]$-Code, $Aut(C_1) \cong (\mathfrak{S}_2 \wr PSL(r,2))/\mathfrak{S}_2^{10}$
2. $\mathcal{P}(\mathcal{U}_{14},\mathcal{U}_{10})$ ist der duale $[30,24,4]$-Code, $Aut(C_2) \cong (\mathfrak{S}_2 \wr PSL(r,2))/\mathfrak{S}_2^{10}$
3. $\mathcal{P}(\mathcal{U}_{10},\mathcal{U}_4)$ ist ein $[30,14,8]$-Code, $Aut(C_3) \cong (\mathfrak{S}_2 \wr PSL(r,2))/\mathfrak{S}_2^{10}$
4. $\mathcal{P}(\mathcal{U}_{11},\mathcal{U}_5)$ ist der duale $[30,16,6]$-Code, $Aut(C_4) \cong (\mathfrak{S}_2 \wr PSL(r,2))/\mathfrak{S}_2^{10}$
5. $\mathcal{P}(\mathcal{U}_{11},\mathcal{U}_4)$ ist ein selbstdualer $[30,15,6]$-Code, $Aut(C_5) \cong (\mathfrak{S}_2 \wr PSL(r,2))/\mathfrak{S}_2^{10}$
6. $\mathcal{P}(\mathcal{U}_{11},\mathcal{U}_1)$ ist ein $[30,12,6]$-Code, $Aut(C_6) \cong (\mathfrak{S}_2 \wr PSL(r,2))/\mathfrak{S}_2^{4}$
7. $\mathcal{P}(\mathcal{U}_{14},\mathcal{U}_4)$ ist der duale $[30,18,4]$-Code, $Aut(C_7) \cong (\mathfrak{S}_2 \wr PSL(r,2))/\mathfrak{S}_2^{4}$

[8] im Abschnitt 10.3 werden wir von diesen Regeln abweichen

Wie erwartet, stimmt die Anzahl der Codes $(2+5)$, sowie ihre zugehörige Automorphismengruppen mit Angaben in den Tabellen 10.3, bzw. 10.2 überein. Die auf diese Weise mit der PLOTKIN-Summe konstruierten Codes sind zu den entsprechenden zyklischen Codes der Länge $N = 30$ isomorph.
Wir leiten 2 Folgerungen daraus ab:

Folgerung 10.15
Aus Regel 1 ($\mathcal{U}_a \subset \mathcal{U}_b$) folgt unmittelbar:

$$\mathcal{U}_b \in \{M_1, \ldots, M_{r-1} = \mathcal{F}_0\} \Longrightarrow \mathcal{U}_a \in \{M_1, \ldots, M_{r-1} = \mathcal{F}_0\}$$

$$\mathcal{U}_b \in \{\overline{M_1}, \ldots, \overline{M_{r-1}} = \overline{\mathcal{F}_0}\} \Longrightarrow \mathcal{U}_a \in \{M_1, \ldots, M_{r-1} = \mathcal{F}_0\} \cup \{\overline{M_1}, \ldots, \overline{M_{r-1}} = \overline{\mathcal{F}_0}\}$$

Folgerung 10.16
Es gilt: Der duale Code zur PLOTKIN*-Summe ist die* PLOTKIN*-Summe der dualen Codes (man achte auf die Reihenfolge der Summanden !).*

$$\overline{\mathcal{P}(\mathcal{C}_1, \mathcal{C}_2)} = \mathcal{P}(\overline{\mathcal{C}_2}, \overline{\mathcal{C}_1}) \tag{10.16}$$

Bemerkung 10.17
Die Größe (Ordnung) der Automorphismengruppe hängt offenbar vom Abstand der beteiligten Codes im Untermodulverband ab:
Je größer diese Abstand, desto größer ist auch die zugehörige Automorphismengruppe. Das müssen wir noch präzisieren und werden deshalb unten mit der Definition des Verbandsraster-Abstands $\mathcal{VRA}_{ba}$ ein Maß einführen. Dabei müssen wir erreichen, daß diejenigen Untermoduln $\mathcal{U}_{k+1} \supset \mathcal{U}_k$ aus den beiden Hauptketten des Verbandes auf derselben Rasterstufe stehen, d.h., daß sie den Verbandsraster-Abstand $= 0$ haben. Diese Besonderheit wird uns im Abschnitt 10.3 wieder begegnen.

Ende der Bemerkung

Die zu unseren Codes zugehörigen Automorphismengruppen sind

$$U_x \rtimes PSL(r,2) \cong (\mathfrak{S}_2 \wr PSL(r,2))/U_y \cong (\mathfrak{S}_2 \wr PSL(r,2))/\mathfrak{S}_2^y, \quad U_y = \overline{U_x} \tag{10.17}$$

Dabei ist das jeweilige y ein Wert aus der Tabelle 10.2 und es gilt:

$$\mathcal{U}_y \in \{M_1 \subset M_2 \subset \ldots \subset M_{r-2}\} \tag{10.18}$$

$$\mathcal{U}_x \in \{\overline{M_1} \supset \overline{M_2} \supset \ldots \supset \overline{M_{r-2}}\} \tag{10.19}$$

Definition 10.18 (**Verbandsraster-Abstand)**
Im Zusammenhang mit der PLOTKIN*-Summe* $\mathcal{P}(\mathcal{U}_b,\mathcal{U}_a)$ *bezeichnen wir den Abstand der beteiligten Codes* $\mathcal{U}_b, \mathcal{U}_a$ *im Untermodulverband des G-Moduls* $\mathbb{F}_2[\Omega]$ *als*
Verbandsraster-Abstand $\mathcal{VRA}_{ba}$ *mit der Differenz* $j-i$*, je nachdem, ob:*

1. $\mathcal{U}_b = M_j, \mathcal{U}_a = M_i$*, d.h.,*
   falls die beiden beteiligten Codes $\mathcal{U}_b, \mathcal{U}_a$ *beide aus der* ABDUKHALIKOV*-Kette der* M_s*,* $(s = 1, \ldots, r-1)$ *stammen, bzw.*

2. $\mathcal{U}_b = \overline{M_i}, \mathcal{U}_a = \overline{M_j}$*, d.h.,*
   falls die beiden beteiligten Codes $\mathcal{U}_b, \mathcal{U}_a$ *beide aus der dazu dualen Kette der* $\overline{M_s}$*,* $(s = 1, \ldots, r-1)$ *stammen, bzw.*

3. $\mathcal{U}_b = \overline{M_i}, \mathcal{U}_a = M_m$*,* $j = r-1-m$*, d.h.,*
   falls $\mathcal{U}_b \in \{\overline{M_1} \ldots \overline{M_{r-1}} = \overline{\mathcal{F}_0}\}$ *und* $\mathcal{U}_a \in \{M_1 \ldots M_{r-1} = \mathcal{F}_0\}$.

Ein Beispiel dazu sehen wir 3 Seiten weiter unten.

Wir formulieren jetzt die Zuordnung der Automorphismengruppen zu den hier besprochenen Codes in dem folgenden wichtigen

Fakt 10.19
Sei C:= $\mathcal{P}(\mathcal{U}_b,\mathcal{U}_a)$ *ein Code, wie oben definiert.*
Dann gilt:

$$Aut(C) \cong U_x \rtimes PSL(r,2) \cong (\mathfrak{S}_2 \wr PSL(r,2))/U_y \cong (\mathfrak{S}_2 \wr PSL(r,2))/\mathfrak{S}_2^y, \text{ mit}$$

$$\mathcal{U}_x = \overline{M_{r-1-\mathcal{VRA}_{ba}}}, \text{ bzw.} \tag{10.20}$$

$$\mathcal{U}_y = M_{r-1-\mathcal{VRA}_{ba}} \text{ und } \mathcal{U}_y = \overline{\mathcal{U}_x}. \tag{10.21}$$

Bemerkung 10.20
In dem obigen Beispiel 10.14 wurden Codes mit Verbandsraster-Abstand $\mathcal{VRA}_{ba} = 1$ demnach dem Untermodul

$$\mathcal{U}_x = \overline{M_{r-1-\mathcal{VRA}_{ba}}} = \overline{M_2} = \mathcal{U}_5, \text{ bzw.} \tag{10.22}$$

$$\mathcal{U}_y = M_{r-1-\mathcal{VRA}_{ba}} = M_2 = \mathcal{U}_{10} \tag{10.23}$$

zugeordnet, so daß die Automorphismengruppe für die ersten fünf Codes lautet:

$$\mathcal{U}_5 \rtimes PSL(4,2) \cong (\mathfrak{S}_2 \wr PSL(4,2))/\mathcal{U}_{10} \cong (\mathfrak{S}_2 \wr PSL(4,2))/\mathfrak{S}_2^{10}. \tag{10.24}$$

Ende der Bemerkung

Abschließend wollen wir die zu Beginn des Abschnitts erwähnten – und im Kapitel 2 „Vererbung“ beschriebenen – Mehrfachcodes mit der Automorphismengruppe $\mathfrak{S}_2 \wr PSL(r,2)$ hier mit einbinden:
Dazu müssen wir die beiden Endpunkte unseres Untermodulverbands M_0 und M_r mit einbeziehen. Die Codes haben dann mit der PLOTKIN-Summe eine recht einfache Darstellung:

$$\mathcal{C}_{[k,2d]} = \mathcal{P}(\mathcal{U}_k, M_0), \quad \mathcal{U}_k \in \{M_1, \ldots, M_{r-2}\} \cup \{\overline{M_1}, \ldots, \overline{M_{r-2}}\} \tag{10.25}$$

und nach Folgerung 10.16 können wir auch die dazu dualen Codes angeben:

$$\mathcal{C}_{[N-(l-k),2d]} = \mathcal{P}(M_r, \overline{\mathcal{U}_k}), \quad \overline{\mathcal{U}_k} \in \{M_1, \ldots, M_{r-2}\} \cup \{\overline{M_1}, \ldots, \overline{M_{r-2}}\} \tag{10.26}$$

Bei dieser Gelegenheit haben wir nebenbei gezeigt, daß die Anzahl dieser Codes $4 \cdot (r-2)$ ist, wie in Tabelle 10.3, rechte Spalte angegeben:

1. Im ersten Fall (10.25) halten wir M_0 fest und $\mathcal{U}_k$ durchläuft sowohl die $r-2$ Untermoduln der ABDUKHALIKOV-Kette, als auch die $r-2$ Untermoduln der dazu dualen Kette.

2. Im zweiten Fall (10.26) halten wir M_r fest und $\overline{\mathcal{U}_k}$ durchläuft sowohl die $r-2$ Untermoduln der ABDUKHALIKOV-Kette, als auch die $r-2$ Untermoduln der dazu dualen Kette.

Um nun allen diesen $4 \cdot (r-2)$ Codes stets dieselbe Automorphismengruppe $\mathfrak{S}_2 \wr PSL(r,2)$ nach obigem Schema zuordnen zu können, benötigen wir eine Erweiterung unserer obigen Definition des Verbandsraster-Abstands mit einem konstanten Wert für den Fall, daß einer der beiden Endpunkte des Verbands an der PLOTKIN-Summe beteiligt ist:

$$4. \quad \mathcal{VRA}_{b0} :\equiv r-1, \quad 1 < b < 2^r - 2 \tag{10.27}$$

$$5. \quad \mathcal{VRA}_{la} :\equiv r-1, \quad 1 < a < 2^r - 2; \ (l = 2^r - 1) \tag{10.28}$$

Dann gilt nach Satz 10.19:

$$\mathcal{U}_x = \overline{M_{r-1-\mathcal{VRA}_{b0}}} = \overline{M_{r-1-(r-1)}} = \overline{M_0} = M_r = \mathbb{F}_2[\Omega] \tag{10.29}$$

$$\mathcal{U}_y = M_{r-1-\mathcal{VRA}_{b0}} = M_{r-1-(r-1)} = M_0. \tag{10.30}$$

Dann gilt nach obiger Formel 10.17 für alle diese $4 \cdot (r-2)$ Codes $\mathcal{C}$:

$$\begin{aligned} Aut(\mathcal{C}) &= \mathbb{F}_2[\Omega] \rtimes PSL(r,2) \\ &\cong M_r \rtimes PSL(r,2) \\ &\cong (\mathfrak{S}_2 \wr PSL(r,2))/M_0 \\ &\cong (\mathfrak{S}_2 \wr PSL(r,2))/\mathfrak{S}_2^0 \\ &\cong \mathfrak{S}_2 \wr PSL(r,2) \end{aligned} \tag{10.31}$$

Die Anzahl der Codes zu $(\mathfrak{S}_2 \wr PSL(r,2))/\mathfrak{S}_2^y$

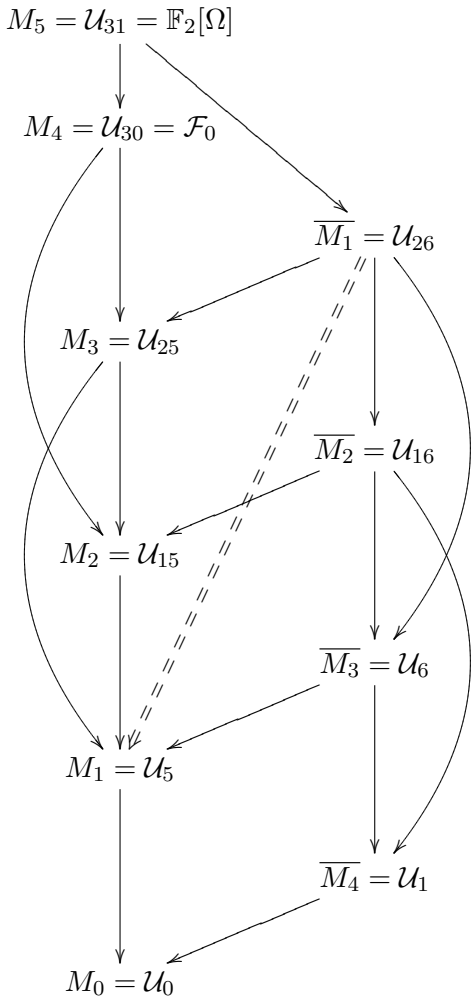
Die Anzahl der Codes zu den Automorphismengruppen $Aut(C) \cong (\mathfrak{S}_2 \wr PSL(r,2))/\mathfrak{S}_2^y$ haben wir bereits oben in der Tabelle 10.3 dargestellt. Dabei fällt auf, daß es für ein bestimmtes r zur Automorphismengruppen $Aut(C) \cong (\mathfrak{S}_2 \wr PSL(r,2))/\mathfrak{S}_2^y$ mit dem kleinsten y-Wert stets 2 Codes gibt (bis auf Isomorphie), für den nächst höheren Wert von y stets 5 Codes, dann 8 Codes, usw.
Dabei findet sich übrigens die Anzahl M der Codes zu $\mathfrak{S}_2 \wr PSL(r,2)$ als Eintrag in der dreieckigen Tabelle wieder, nämlich auf der nächsten Zeile für $r+1$ als Anzahl der Codes, die zu dem höchsten y-Wert gehört.

Woran liegt das? Wir erklären das in mehreren Schritten:

- Wir hatten bereits oben im Satz 10.6 die Anzahl der Codes zur Automorphismengruppe $PSL(r,2)$ mit dem Wert $2 \cdot (r-2)$ angegeben und bewiesen. Wenn wir nun aus jedem dieser Codes der Länge l einen Mehrfachcode der Länge $N = 2 \cdot l$ erzeugen, bekommen wir wieder $2 \cdot (r-2)$ Codes mit den Dimensionen k_i, wie in Tabelle 10.1 angegeben, aber mit der doppelten Minimaldistanz. Zusätzlich bekommen wir jetzt aber noch zu jedem Code den dualen Code mit der Dimension $N - k_i$. Das ergibt dann insgesamt $M = 4 \cdot (r-2)$ Codes zur Automorphismengruppe $\mathfrak{S}_2 \wr PSL(r,2)$, wie in der rechten Spalte der Tabelle 10.3 dargestellt.

- Die übrigen Anzahlen machen wir uns klar anhand der Verbandsstruktur der Untermoduln des $PSL(r,2)$-Moduls $\mathbb{F}_2[\Omega]$, sowie an den oben gemachten Aussagen zur Zuordnung der Codes aus den PLOTKIN-Summen zweier Untermoduln $\mathcal{U}_b, \mathcal{U}_a$ zu den Automorphismengruppen anhand des Verbandsraster-Abstands $\mathcal{VRA}_{ba}$ (s. Satz 10.19):
  So gibt es eben unter Berücksichtigung der Regeln 1 und 2 (im Anschluß an Formel 10.15) stets nur 2 Möglichkeiten, Codes mit einem $\mathcal{VRA}_{ba}$-Wert von $r-2$, aber 5 Möglichkeiten, Codes mit einem $\mathcal{VRA}_{ba}$-Wert von $r-3$ zu bilden, usw.

- Zur besseren Veranschaulichung ist diese Zuordnung der Diagonalspalten in der Tabelle 10.3 zum $\mathcal{VRA}_{ba}$-Wert in die Kopfzeile dieser Tabelle eingetragen worden. Darüberhinaus wollen wir in einem Beispiel die typischen 5 Codes mit einem $\mathcal{VRA}_{ba}$-Wert von $r-3$ mit zusätzlichen 4 Bogenlinien und einer doppelt gestrichelten Linie für den einen selbstdalen Code in die Verbandsstruktur eintragen.



Die typischen 5 Codes $\mathcal{P}(\mathcal{U}_b,\mathcal{U}_a)$ mit
Verbandsraster-Abstand $\mathcal{VRA}_{ba}$ =2= $r-3$
am Beispiel des Untermodulverbands des $PSL(5,2)$-Moduls $\mathbb{F}_2[\Omega]$.
Die zugehörige Automorphismengruppe ist $(\mathfrak{S}_2 \wr PSL(5,2))/\mathfrak{S}_2^{15}$.

Man beachte die Zentralsymmetrie:
$\mathcal{P}(\mathcal{U}_{30},\mathcal{U}_{15}) = \mathcal{P}(\mathcal{M}_4,\mathcal{M}_2)$ ist dual zu $\mathcal{P}(\mathcal{U}_{16},\mathcal{U}_1) = \mathcal{P}(\overline{\mathcal{M}_2},\overline{\mathcal{M}_4})$,
$\mathcal{P}(\mathcal{U}_{25},\mathcal{U}_5) = \mathcal{P}(\mathcal{M}_3,\mathcal{M}_1)$ ist dual zu $\mathcal{P}(\mathcal{U}_{26},\mathcal{U}_6) = \mathcal{P}(\overline{\mathcal{M}_1},\overline{\mathcal{M}_3})$,
$\mathcal{P}(\mathcal{U}_{26},\mathcal{U}_5) = \mathcal{P}(\overline{\mathcal{M}_1},\mathcal{M}_1)$ ist der eine selbstduale Code.

Legende: M_i gibt den Untermodul mit seiner
Position i in der ABDUKHALIKOV-Kette an.
$\mathcal{U}_k$ gibt den Untermodul mit seiner Dimension k an.
$\mathcal{U}_i \longleftarrow \mathcal{U}_j$ bedeutet: $\mathcal{U}_i \subset \mathcal{U}_j$.
$\mathcal{U}_i \curvearrowleft \mathcal{U}_j$ bedeutet: Es wird die PLOTKIN-Summe $\mathcal{P}(\mathcal{U}_j,\mathcal{U}_i)$ gebildet.
$\mathcal{U}_i <= = \cdots = = \mathcal{U}_j$ bedeutet: Es wird die PLOTKIN-Summe $\mathcal{P}(\mathcal{U}_j,\mathcal{U}_i)$
gebildet; diese Summe ergibt einen selbstdualen Code.

10.3 Die Automorphismengruppen $PSL(r,2) \wr \mathfrak{S}_2$ und ihre Codes

Bei den Codelängen $N = 2 \cdot (2^r - 1)$ treten – zusätzlich zu den im Kap. 1, sowie im Abschnitt 10.2 beschriebenen Automorphismengruppen mit ihren zugehörigen Codes – auch noch die im Kapitel „Vererbung“ beschriebenen weiteren Codes[9] mit der Automorphismengruppe $PSL(r,2) \wr \mathfrak{S}_2$ auf.

Für das Verständnis und auch für die Gewinnung dieser Codes bedienen wir uns auch hier der folgeden Erkenntnisse und Techniken:

1. Lineare Codes sind Untermoduln eines G-Moduls über $\mathbb{F}_2$ (s. Kap. 9),
2. diese Untermoduln bilden einen Verband (siehe Grafik im Beispiel 10.11)
3. die PLOTKIN-Summe (s. Abschnitt 2.2) verknüpft zwei Codes der Länge l zu einem neuen Code der Länge $N = 2 \cdot l$.

Nomenklatur: Um einerseits die Konsistenz mit der Literatur[1] zu erhalten und andererseits Information über die Dimension der Untermoduln zu vermitteln, haben wir zwei Bezeichnungen für unsere Untermoduln gewählt:

1. M_i, wie in $0 = M_0 \subset M_1 \subset M_2 \subset \cdots \subset M_{r-2} \subset M_{r-1} = \mathcal{F}_0$: Hier gibt der Index die Position des Untermoduls in der Inklusionskette an.
2. U_k oder $\mathcal{U}_k$: Hier gibt der Index die Dimension des Untermoduls an, also $k = \dim(U_k)$.

Aus den Beobachtungen der Codelängen $N = 14$, 30 und 62 formulieren wir den folgenden Satz:

Satz 10.21
Für Codelängen $N = 2 \cdot l$ mit $l = 2^r - 1$, $r \geq 3$ existiert jeweils eine Automorphismengruppe mit folgendem Kranzprodukt

$$PSL(r,2) \wr \mathfrak{S}_2 \tag{10.32}$$

Dazu gehören (bis auf Isomorphie) $3 \cdot (r-2)$ zyklische Codes.
Ist r ungerade, so ist einer der Codes selbstdual.

Dabei können die Attribute $[N, k, d]$ zu jedem Code angegeben werden (s. dazu Beispiel 10.23).
Zunächst wollen wir auf der nächsten Seite das weitere Vorgehen zusammenfassen:

[9] wir hatten dort von „Rückwärtsvererbung“ gesprochen und die PLOTKIN-Summe eingeführt.

Anmerkungen zur Beweisführung und der weiteren Vorgehensweise:

- in der folgenden Bemerkung wird die Codebildung erläutert und im anschließenden Beispiel 10.23 verdeutlicht.
- Danach folgt die Konstruktion des Codes $\mathcal{C}$ als Bestandteil des Beweises.
- Anschließend überlegen wir, wie $Aut(\mathcal{C})$ auf $\mathcal{C}$ operiert. Dazu werden einige Sätze, sowie Hilfssätze formuliert und bewiesen.
- Zum Abschluß beweisen wir noch die Aussage zur Anzahl der Codes, sowie zur Selbstdualität eines Codes.

Bemerkung 10.22
Grundlage der Codebildung sind auch hier wieder die Untermoduln des $PSL(r,2)$-Moduls $\mathbb{F}_2[\Omega]$. Sie sind zyklische Codes der Länge l, wie im Abschnitt 10.1 gezeigt.
Im Abschnitt 10.2 hatten wir weiter gezeigt, wie durch Anwendung der PLOTKIN-Summe $\mathcal{P}(\mathcal{C}_1,\mathcal{C}_2)$ unter bestimmten Regeln[10] weitere Codes der Länge $2 \cdot l$ erzeugt werden, die (nach Satz 2.17) zu zyklischen Codes isomorph sind. Bei diesen Regeln waren folgende Kombinationen ausgenommen:

- $\dim(\mathcal{C}_1) - \dim(\mathcal{C}_2) \leq 1$. Dies führt nun zu folgenden PLOTKIN-Summen:
  1. $\mathcal{P}(\mathcal{C},\mathcal{C})$; dieser Fall wurde bereits im Abschnitt 2.2 behandelt, sowie
  2. $\mathcal{P}(\mathcal{C}_1,\mathcal{C}_2)$ mit $\mathcal{C}_1 \supseteq \mathcal{C}_2$ und $\dim(\mathcal{C}_1) = \dim(\mathcal{C}_2) + 1$
- $\mathcal{P}(\mathcal{C}_1,\mathcal{C}_2)$ mit $\mathcal{C}_1 \not\supseteq \mathcal{C}_2$. Dies führt aus dem Bereich der zyklischen Codes heraus (nicht-zykl. Gruppencodes) und soll hier nicht weiter untersucht werden.

Wir erweitern daher nun sinngemäß unsere obigen Definition des Verbandsraster-Abstands:

$$6. \quad \mathcal{VRA}_{ba} :\equiv 0, \quad \text{falls } b - a \leq 1 \tag{10.33}$$

und betrachten nun gezielt die Codes mit $\mathcal{VRA}_{ba} = 0$:
Diese Codes haben dann mit der PLOTKIN-Summe eine recht einfache Darstellung:

$$\mathcal{C} = \mathcal{P}(\mathcal{U}_b,\mathcal{U}_a),\ \mathcal{U}_b, \mathcal{U}_a \in \{M_1,\ldots,M_{r-2}\} \cup \{\overline{M_1},\ldots,\overline{M_{r-2}}\} \text{ und } \mathcal{VRA}_{ba} :\equiv 0 \tag{10.34}$$

Auch hier ist für die Bestimmung der $3 \cdot (r-2)$ zyklischen Codes und deren Dimensionen die Tabelle 10.4 hilfreich.

Beispiel 10.23
So finden wir z.B. in der zweiten Zeile ($N = 30$) dieser Tabelle die Werte 4 und 10 aus der ABDUKHALIKOV-Kette. Somit wird es die folgenden 6 Codes (bis auf Isomorphie) zur Automorphismengruppe $PSL(4,2) \wr \mathfrak{S}_2$ geben (siehe dazu auch das Hasse-Diagramm des Untermodulverbands des $PSL(4,2)$-Moduls $\mathbb{F}_2[\Omega]$, 12 Seiten zuvor).

[10] es war $\mathcal{C}_1 \supset \mathcal{C}_2$ vorausgesetzt, sowie $\dim(\mathcal{C}_1) - \dim(\mathcal{C}_2) > 1$

r	l	N	k
3	7	14	**3**
4	15	30	4 10
5	31	62	5 **15** 25
6	63	126	6 21 41 56
7	127	254	7 28 **63** 98 119
8	255	510	8 36 92 162 218 246
9	511	1022	9 45 129 **255** 381 465 501
10	1023	2046	10 55 175 385 637 847 967 1012
11	2047	4094	11 66 231 561 **1023** 1485 1815 1980 2035

Tabelle 10.4: Dimensionen k der Untermoduln des jeweiligen $PSL(r,2)$-Moduls $\mathbb{F}_2[\Omega]$ in seiner ABDUKHALIKOV-Inklusionskette; $l = 2^r - 1$, $N = 2 \cdot l$.

Da wir das Bildungsgesetz für die Untermoduln der $PSL(r,2)$-Moduln $\mathbb{F}_2[\Omega]$ – wie auch das Bildungsgesetz für die Minimaldistanzen der Untermoduln gefunden, und in der Tabelle 10.1 zusammengefaßt haben, können wir – entsprechend der Definition der PLOTKIN-Summe – jetzt diese 6 Codes mit ihren Attributen k und d angeben:

1. $\mathcal{P}(\mathcal{U}_4,\mathcal{U}_4)$, $k = 8$, $d = 8$
2. $\mathcal{P}(\mathcal{U}_{11},\mathcal{U}_{11})$, $k = 22$, $d = 3$ ($\mathcal{U}_{11}$ ist dual zu $\mathcal{U}_4$)
3. $\mathcal{P}(\mathcal{U}_{10},\mathcal{U}_{10})$, $k = 20$, $d = 4$
4. $\mathcal{P}(\mathcal{U}_5,\mathcal{U}_5)$, $k = 10$, $d = 7$ ($\mathcal{U}_5$ ist dual zu $\mathcal{U}_{10}$)
5. $\mathcal{P}(\mathcal{U}_5,\mathcal{U}_4)$, $k = 9$, $d = 8$
6. $\mathcal{P}(\mathcal{U}_{11},\mathcal{U}_{10})$, $k = 21$, $d = 4$

Man sieht an diesem Beispiel, daß es wegen $k \neq 15$ keinen selbstdualen Code unter den obigen 6 Codes geben kann (es war $r = 4$ gerade). Dagegen läßt sich bei ungeradem r stets $l = k = 2^r - 1$ unter obigen Regeln kombinieren.

Wir wollen nun den obigen Satz 10.21 beweisen. Der Beweis ist recht umfangreich. Wir formulieren und beweisen daher eine Reihe von Teilaussagen. Zunächst diskutieren wir die Konstruktion der Codes $\mathcal{C}$:

Beweis. Sei $\Omega = \mathbb{P}^{r-1}(\mathbb{F}_2)$ und $\mathbb{F}_2[\Omega]$ sei unser $PSL(r,2)$-Modul.
$PSL(r,2)$ operiert auf Ω und es sei $L := \mathbb{F}_2[\Omega] \times \mathbb{F}_2[\Omega]$.
Seien ferner U_0, U_1 die Untermoduln von $\mathbb{F}_2[\Omega]$ mit den Dimensionen 0 und 1.

Sei außerdem $U_0 < U_a < \mathcal{F}_0$ ein beliebiger Untermodul aus der ABDUKHALIKOV - Inklusionskette der Untermoduln von $\mathbb{F}_2[\Omega]$ – so, wie im Magischen Dreieck mit seiner Dimension $a = \dim(U_a)$ auf der entsprechenden Zeile angegeben.
Dann gilt:

$$U_1 \subseteq \mathbb{F}_2[\Omega] \supseteq U_a \quad \text{mit} \quad U_a \cap U_1 = U_0. \tag{10.35}$$

Nun sei

$$U_a \subseteq U_b := U_a + U_1 \quad \text{mit} \quad \dim(U_b) = \dim(U_a) + 1 = a + 1 =: b. \tag{10.36}$$

Wir bilden nun die PLOTKIN-Summe:

$$\mathcal{C} := \mathcal{P}(U_b, U_a) = \{(u, u+v) \mid u \in U_b, v \in U_a\} \subseteq L \tag{10.37}$$

und es gilt:

$$Aut(\mathcal{C}) = PSL(r,2) \wr \mathfrak{S}_2 \supseteq PSL(r,2) \times PSL(r,2). \tag{10.38}$$

Wir wollen nun überlegen, wie $Aut(\mathcal{C})$ auf $\mathcal{C}$ operiert.
Sei zunächst $\gamma = (\gamma_1, \gamma_2) \in PSL(r,2) \times PSL(r,2)$. Dann ist

$$(\gamma_1 u, \gamma_2 u + \gamma_2 v) = (\gamma_1 u, \gamma_1 u + \{\gamma_2 u + \gamma_2 v - \gamma_1 u\}) \tag{10.39}$$

Wir zeigen nun, daß $\{\gamma_2 u + \gamma_2 v - \gamma_1 u\} \in U_a$.

Beweis. Wegen $v \in U_a$ folgt $\gamma_2 v \in U_a$ und wegen $u \in U_b$ folgt zunächst: $(\gamma_2 u - \gamma_1 u) \in U_b$.
Nun ist $u = u_1 + u_a$ mit $u_1 \in U_1$ und $u_a \in U_a$.
Es gilt: $\gamma u_1 = u_1, \forall \gamma \in PSL(r,2)$.
Es ist

$$\begin{aligned} \gamma_2 u - \gamma_1 u = & \quad \gamma_2(u_1 + u_a) - \gamma_1(u_1 + u_a) \\ = & \quad \gamma_2 u_1 - \gamma_1 u_1 + \gamma_2 u_a - \gamma_1 u_a \\ = & \quad 0 + \gamma_2 u_a - \gamma_1 u_a \in U_a, \text{ weil } u_a \in U_a. \end{aligned}$$

Daraus folgt die Behauptung. □

Damit haben wir gezeigt, daß $\gamma c \in \mathcal{C}, \forall c \in \mathcal{C}, \forall \gamma \in PSL(r,2) \times PSL(r,2)$.
Nun ist $PSL(r,2) \times PSL(r,2)$ zwar eine Gruppe von Automorphismen für unseren Code $\mathcal{C}$, aber noch nicht die **volle** Automorphismengruppe.
Wir fassen erst einmal zusammen und formulieren den soeben bewiesenen Satz:

Satz 10.24
Sei U_a wie oben definiert. Die Gruppe $PSL(r,2) \times PSL(r,2)$ operiert durch

$$(\gamma_1, \gamma_2) * (u, v) := (\gamma_1 u, \gamma_2 v), \quad (\gamma_1, \gamma_2 \in PSL(r,2); u, v \in \mathbb{F}_2[\Omega]) \tag{10.40}$$

auf L. Diese Operation läßt jede PLOTKIN*-Summe*

$$\mathcal{C} := \mathcal{P}(U_b, U_a) \subseteq L \tag{10.41}$$

invariant, wo $U_a \cap M_x = M_0$ und $U_b = U_a + M_x$.

Folgerung 10.25
Es gilt:

$$M_x \in \{U_0, U_1\} \tag{10.42}$$

Definition 10.26
Sei $\mathfrak{C}_2 := \{1, \sigma\}$ die Gruppe der Ordnung 2.
$\mathfrak{C}_2$ operiert auf L durch $\sigma(w,z) = (z,w)$.

Hilfssatz 10.27
Es gilt:

$$\sigma\mathcal{P}(U_b, U_a) = \mathcal{P}(U_b, U_a). \tag{10.43}$$

Beweis.

$$\sigma(u, u+v) = (u+v, u) \tag{10.44}$$

$$= (u+v, \{u+v\} - v) \tag{10.45}$$

$$u \in U_b, v \in U_a \subseteq U_b \Longrightarrow u+v \in U_b. \tag{10.46}$$

□

Hilfssatz 10.28
Es gilt:

$$\langle PSL(r,2) \times PSL(r,2), \sigma \rangle \cong PSL(r,2) \wr \mathfrak{C}_2 \tag{10.47}$$

Beweis. Die Gruppe von linearen Abbildungen, die von
$PSL(r,2) \times PSL(r,2)$ und $\mathfrak{C}_2$ (nach Satz 10.27 und Satz 10.24) erzeugt wird, ist isomorph zum Kranzprodukt $PSL(r,2) \wr \mathfrak{S}_2$. □

Satz 10.29
Seien $U_a \subseteq U_b$ zwei zyklische Codes der Länge l. Dann gilt: Die Plotkin-*Summe*
$\mathcal{C} := \mathcal{P}(U_b, U_a) := \{(x, x+v) \mid x \in U_b, v \in U_a\}$ ist isomorph zu einem zyklischen Code $\widehat{\mathcal{C}}$ der Länge $N = 2 \cdot l$.

Beweis. Ein Codevektor $z \in \mathcal{C}$ ist eine Aneinanderreihung zweier Codevektoren x und y mit $x, y \in U_b$, da $U_a \subseteq U_b$ nach Voraussetzung und somit $y := x + v$, $v \in U_a$ definiert werden kann.
Durch die folgende Koordinatenpermutation $\sigma \in \mathfrak{S}_N$ mit $\sigma : \mathcal{C} \longrightarrow \widehat{\mathcal{C}}$ wird ein Isomorphismus induziert und wir entsprechen somit der Definition 0.36 von Code-Isomorphie. Die Abbildung $\sigma : z \mapsto \widehat{z} \in \widehat{\mathcal{C}}$ zeigt die Zyklizität von $\widehat{\mathcal{C}}$:

$$z = (x_1, x_2, \ldots, x_l, y_1, y_2, \ldots, y_l),$$

$$\widehat{z} = (x_1, y_1, x_2, y_2, \ldots\ldots, x_l, y_l).$$

□

Noch einmal zurück zum Beispiel 10.23:
Bei den ersten vier Codes ist $M_x = U_0 = M_0$, bei den letzten zwei ist $M_x = U_1$ (s. a. Formel 10.42).

Nun bleibt noch die Aussage zu beweisen:
„Dazu gehören (bis auf Isomorphie) $3 \cdot (r-2)$ zyklische Codes."

Beweis. Die Anzahl der Untermoduln U_a des jeweiligen $PSL(r,2)$-Moduls $\mathbb{F}_2[\Omega]$ in seiner ABDUKHALIKOV-Inklusionskette mit $U_0 < U_a < \mathcal{F}_0$ ist genau $r-2$ (s. Tabelle oben).
Nun können wir folgende Codes $\mathcal{C}$ für alle diese U_a als PLOTKIN-Summe bilden:

1. $\mathcal{P}(\mathcal{U}_a, \mathcal{U}_a)$
2. $\mathcal{P}(\overline{\mathcal{U}_a}, \overline{\mathcal{U}_a})$
3. $\mathcal{P}(\mathcal{U}_a, \{\mathcal{U}_a + \mathcal{U}_1\})$

Das sind genau $3 \cdot (r-2)$ Codes, die zu zyklischen Codes isomorph sind. □

Abschließend bleibt noch die Aussage zu beweisen:
„Ist r ungerade, so ist einer der Codes selbstdual."

Beweis. Das sieht man folgendermaßen:
Ist nun r ungerade, dann ist auch $r-2$ ungerade und es gibt genau einen Untermodul U_a in der Mitte der zugehörigen ABDUKHALIKOV-Inklusionskette mit $a = \dim(U_a)$ (fettgedruckt in der Tabelle), so daß $2a+1 = 2^r - 1$ gilt. Der dritte Code-Typ aus der obigen Varianten-Liste für dieses U_a, also $\mathcal{P}(\mathcal{U}_a, \{\mathcal{U}_a + \mathcal{U}_1\})$ ist dann der eine selbstduale Code. □

Damit ist nun der obige Satz 10.21 bewiesen. □

Ein letztes Beispiel:

Beispiel 10.30
Wenn wir im Tabellenwerk der Automorphismengruppen für $N = 62$ nachsehen (s. Anhang G), so finden wir, daß die Automorphismengruppe $PSL(5,2) \wr \mathfrak{S}_2$ von 54 Codes angenommen wird, davon 6 selbstduale. Diese Zahlenangabe schließt alle isomorphen Codes mit ein.
Im Kapitel 0.1 finden wir in der Tabelle der Isomorphie-Faktoren für $PSL(5,2)$ den Iso-Faktor 6, so daß wir – bis auf Isomorphie – $54/6 = 9$ verschiedene zyklische Codes (davon einer selbstdual) mit der Automorphismengruppe $PSL(5,2) \wr \mathfrak{S}_2$ identifizieren konnten. Somit wurde unsere Aussage mit $9 = 3 \cdot (5-2)$ bestätigt.

10.4 Zwei neue Code-Familien

10.4.1 Die $\mathcal{B}4$-Codes

Unter den zyklischen Codes, die zu diesen oben diskutierten Automorphismengruppen mit verminderten Kranzprodukten

$$(\mathfrak{S}_2 \wr PSL(r,2))/\mathfrak{S}_2^y,$$

gehören, fällt eine Code-Familie durch hohe Effizienz ($R = k/N$) auf: Es ist dies der

$$[N, 2^{r+1} - r - 4, 4] - Code \quad \text{mit} \quad N = 2 \cdot (2^r - 1) \tag{10.48}$$

mit der Automorphismengruppe als verminderter Kranz mit dem höchsten y-Wert (also der rechte Schenkel des nach unten offenen magischen Dreiecks):

$$(\mathfrak{S}_2 \wr PSL(r,2))/\mathfrak{S}_2^{2^r-r-2} \tag{10.49}$$

Da hier die Minimaldistanz konstant $d \equiv 4$ ist, erhalten wir eine bessere Zuverlässigkeit ($\delta = d/N$), als bei den Hamming-Codes: wir können mit diesen Codes sogar 2 Fehler erkennen[11]

Beispiel: Der $[62, 55, 4]$-Code $\mathcal{B}4_5$ mit $(\mathfrak{S}_2 \wr PSL(5,2))/\mathfrak{S}_2^{25}$ als Automorphismengruppe schneidet im Vergleich zum nächstgelegenen Hamming-Code $\mathcal{H}_6$ mit den Attributen $[63, 57, 3]$ durchaus gut ab.

Aus Gründen der Übersichtlichkeit habe ich die wesentlichen Attribute der Codes $\mathcal{B}4_3$ bis $\mathcal{B}4_{10}$ in der Tabelle 10.4 (s.u.) zusammengestellt.

Für die ersten Codes $\mathcal{B}4_3$ bis $\mathcal{B}4_7$ wollen wir hier die Generatorpolynome angeben. Auf die Angabe der bisweilen umfangreichen Kontrollpolynome wollen wir bewußt verzichten, man kann sie bei Bedarf leicht durch **Magma** erstellen:

```
> P<x>:=PolynomialRing(GF(2));
> GenPol:=x^5 + x^2 + x + 1;
> B4_3:=CyclicCode(14,GenPol);
> CheckPolynomial(B4_3);
x^9 + x^6 + x^5 + x^4 + x^3 + x + 1
>
```

Eine Gesetzmäßigkeit konnte bislang noch nicht gefunden werden. Wegen der Code-Isomorphien (s. Kapitel 0.1) sind die hier angegebenen Generator- und Kontrollpolynome nicht eindeutig, daher sollen in der Auflistung noch einige alternative kürzere Generatorpolynome aufgezeigt werden.

[11] ähnlich, wie die weiter oben im Abschnitt 10.1 definierten $\mathcal{HB}4$-Codes !

Name	r	N	k	d	R=k/N	δ = d/N	Automorphismengruppe
$\mathcal{B}4_3$	3	14	9	4	0,643	0,286	$(\mathfrak{S}_2 \wr PSL(3,2))/\mathfrak{S}_2^3$
$\mathcal{B}4_4$	4	30	24	4	0,800	0,133	$(\mathfrak{S}_2 \wr PSL(4,2))/\mathfrak{S}_2^{10}$
$\mathcal{B}4_5$	5	62	55	4	0,887	0,065	$(\mathfrak{S}_2 \wr PSL(5,2))/\mathfrak{S}_2^{25}$
$\mathcal{B}4_6$	6	126	118	4	0,937	0,037	$(\mathfrak{S}_2 \wr PSL(6,2))/\mathfrak{S}_2^{56}$
$\mathcal{B}4_7$	7	254	245	4	0,965	0,016	$(\mathfrak{S}_2 \wr PSL(7,2))/\mathfrak{S}_2^{119}$
$\mathcal{B}4_8$	8	510	500	4	0,980	0,0078	$(\mathfrak{S}_2 \wr PSL(8,2))/\mathfrak{S}_2^{246}$
$\mathcal{B}4_9$	9	1022	1011	4	0,989	0,0039	$(\mathfrak{S}_2 \wr PSL(9,2))/\mathfrak{S}_2^{501}$
$\mathcal{B}4_{10}$	10	2046	2034	4	0,994	0,00196	$(\mathfrak{S}_2 \wr PSL(10,2))/\mathfrak{S}_2^{1012}$

Tabelle 10.5: Tabelle der $\mathcal{B}4$-Code-Familie

$$
\begin{aligned}
\mathcal{B}4_3: &\quad x^5+x^2+x+1\\
\mathcal{B}4_4: &\quad x^6+x^4+x^3+x^2+x+1\\
\mathcal{B}4_5: &\quad x^7+x^6+x^4+x^2+x+1;\\
&\quad x^7+x^3+x^2+1; \quad x^7+x^4+x+1;\\
&\quad x^7+x^5+x^4+1; \quad x^7+x^6+x^3+1\\
\mathcal{B}4_6: &\quad x^8+x^5+x^4+x^2+x+1\\
\mathcal{B}4_7: &\quad x^9+x^8+x^7+x^6+x^5+x^2+x+1;\\
&\quad x^9+x^2+x+1; \quad x^9+x^6+x+1;\\
&\quad x^9+x^8+x^3+1
\end{aligned}
$$

Wegen der Code-Isomorphien gibt es insgesamt 18 verschiedene Generator-Polynome zu $\mathcal{B}4_7$.

Abschließend noch eine Bemerkung: Diese $\mathcal{B}4$-Codes sind von den Attributen mit den im Abschnitt 10.1 eingeführten $\mathcal{HB}4$-Codes vergleichbar, allerdings sind die Automorphismengruppen der $\mathcal{B}4$-Codes wesentlich kleiner:
Die Werte für N, k und insbesondere r sind bei den $\mathcal{B}4$-Codes stets um 1 niedriger !

10.4.2 Die $\mathcal{HB}7$-Codes

Unter den zyklischen Codes, die zu den oben diskutierten Automorphismengruppen $PSL(r,2)$ gehören, fällt eine weitere Code-Familie durch gute R/δ-Relation auf: Es ist dies der

$$[N, N-x_r, 7]-Code \quad \text{mit } N=2^r-1, \tag{10.50}$$

Name	r	N	k	d	R=k/N	δ = d/N	Automorphismengruppe
$\mathcal{HB}7_4$	4	15	5	7	0,333	0,467	$PSL(4,2)$
$\mathcal{HB}7_5$	5	31	16	7	0,516	0,226	$PSL(5,2)$
$\mathcal{HB}7_6$	6	63	42	7	0,667	0,111	$PSL(6,2)$
$\mathcal{HB}7_7$	7	127	99	7	0,780	0,055	$PSL(7,2)$
$\mathcal{HB}7_8$	8	255	219	7	0,859	0,0275	$PSL(8,2)$
$\mathcal{HB}7_9$	9	511	466	7	0,912	0,0137	$PSL(9,2)$
$\mathcal{HB}7_{10}$	10	1023	968	7	0,946	0,00684	$PSL(10,2)$
$\mathcal{HB}7_{11}$	11	2047	1981	7	0,968	0,00342	$PSL(11,2)$

Tabelle 10.6: Tabelle der $\mathcal{HB}7$-Code-Familie

und x_r steht in der zweiten Diagonalspalte von Tabelle 8.2 und genügt folgender Rekursionsformel:

$$x_4 = 10 \tag{10.51}$$

$$x_r = x_{r-1} + r \tag{10.52}$$

mit derselben Automorphismengruppe, wie bei den **Hamming**-Codes:

$$PSL(r,2) \tag{10.53}$$

Da hier die Minimaldistanz konstant $d = 7$ ist, erhalten wir eine deutlich bessere Zuverlässigkeit δ (d/N), als bei den Hamming-Codes: wir können mit diesen Codes sogar 3 Fehler korrigieren !
Diese Codes werden ab Codelängen von 127 interessant (s. Tabelle 10.6).

Anhang A

Magma - Besonderheiten

In diesem Abschnitt möchte ich auf einige Besonderheiten im Zusammenhang mit dem Computeralgebrasystem **Magma** hinweisen:
Bei der Ermittlung der Gruppencodes habe ich die jeweiligen Vektoren von **Magma** in einer Schleife erzeugen lassen, wie in diesem kleinen Beispiel hier:

Beispiel A.1 (**Die 16 Vektoren des Vektorraums** $\mathbb{F}_2^4$**)**

```
> VN:=VectorSpace(GF(2),4);
> for v in VN do; v; end for;
(0 0 0 0)
(1 0 0 0)
(0 1 0 0)
(1 1 0 0)
(0 0 1 0)
(1 0 1 0)
(0 1 1 0)
(1 1 1 0)
(0 0 0 1)
(1 0 0 1)
(0 1 0 1)
(1 1 0 1)
(0 0 1 1)
(1 0 1 1)
(0 1 1 1)
(1 1 1 1)
>
```

Dabei werden mit fortlaufendem impliziten Index die Vektoren von links nach rechts aufgebaut – (und somit also nicht, wie wir es von der arabischen Notation[1] her gewohnt sind, von rechts nach links). Die Vektoren lassen sich auch vergleichen und somit ordnen.
Es gilt allgemein:

$$v[n+1] > v[n], \tag{A.1}$$

wie man leicht nachprüfen kann. Das bedeutet, daß die obigen Vektoren in der Reihenfolge von oben nach unten den Werten von 0 bis 15 zugeordnet sind.

[1] Damit ist die Anordnung der gewichteten Ziffern gemeint: wachsende Potenzen der Basis von rechts nach links.

Im Gegensatz dazu wird das Generatorpolynom eines zyklischen Codes, dessen Koeffizienten direkt mit dem Erzeugungsvektor korrelieren, von **Magma** in der arabischen Anordnung (also in umgekehrter Reihenfolge im Vergleich zum Erzeugungsvektor) dargestellt:

```
Erzeugungs-Vektor ist: (1 1 1 0 1 0 0 0 1 0 0 0 0 0 0)
GeneratorPolynomial:      x^8 + x^4 + x^2 + x + 1
```

Übrigens finden wir die Koeffizienten des Generatorpolynoms auch in der letzten Zeile der Generatormatrix G (mit dem Verschiebungsfaktor $k = \dim(C)$): $1 + x + x^2 + x^4 + x^8$

```
[15, 7, 5] Cyclic Linear Code over GF(2)
Generator matrix:
[1 0 0 0 0 0 0 1 1 1 0 1 0 0 0]
[0 1 0 0 0 0 0 0 1 1 1 0 1 0 0]
[0 0 1 0 0 0 0 0 0 1 1 1 0 1 0]
[0 0 0 1 0 0 0 0 0 0 1 1 1 0 1]
[0 0 0 0 1 0 0 1 1 1 0 0 1 1 0]
[0 0 0 0 0 1 0 0 1 1 1 0 0 1 1]
[0 0 0 0 0 0 1 1 1 0 1 0 0 0 1]
```

Der aus dem jeweiligen Vektor und der zyklischen Gruppe gebildete zyklische Code (dazu gehört stets eine ungerade Laufnummer in den Codelisten und eine Dimension $k > N/2$) ist – mit Ausnahme der letzten Codes[2] bei geraden Codelängen – für die in dieser Arbeit festgestellten Gesetzmäßigkeiten weitgehend uninteressant.
Viel interessanter ist der dazu duale Code mit gerader Laufnummer:
Auf ihn beziehen sich die Aussagen in dieser Arbeit bezüglich k und d in Abhängigkeit von N und dessen Teilern.
Wenn wir dann in einem Nachsatz zu einer solchen Aussage etwa formulieren:
„Zu diesem Code C gehört ein dualer Code mit $d = 2$“, dann ist dieser duale Code in Wirklichkeit unser ursprünglich gefundener Code und seine laufende Nummer ist ungerade und um 1 niedriger als die laufende Nummer des Codes C (siehe dazu das folgende Beispiel und auch Kapitel 4).

Beispiel A.2

```
Lineare Permutations-Gruppencodes der Laenge n = 36
der zyklischen Permutationsgruppe

Lfd.Nr.  k   d              #AutoGrp

   1    34   2         8198077813559456628001996800000
   2     2  18         8198077813559456628001996800000
   3    34   2         6594200419228723445760000
   4     2  24         6594200419228723445760000
   5    33   2         6594200419228723445760000
   6     3  12         6594200419228723445760000
   ..........................
   ..........................
```

[2] ab dem ersten selbstdualen Code

Allgemein ist noch zu erwähnen, daß die meisten Berechnungen mit der **Magma**-Version 2.12-7 (Jahre 2005/2006), sowie 2.13-5 und 2.13-6 (Jahre 2006/2007) durchgeführt wurden. Bei einigen Rohcodes größerer Länge, war aber auch mit diesen Versionen die Berechnung der Automorphismengruppe nicht mehr möglich und das Programm blieb stehen. Hier half oft in Einzelfällen der Einsatz der älteren Version 2.11-2 (daher auch die Zusatzauswertungen), oder aber mitunter tagelange Geduld für einen einzigen Code. Der Lohn ist dann die Vollständigkeit der Auswertungen.

Bei der Überprüfung der identifizierten Automorphismengruppen durch Isomorphie – speziell bei den verminderten Kranzprodukten – gab es ebenfalls Grenzen von **Magma**: So waren manche Gruppendivisionen nicht durchführbar und es gab die folgende Fehlermeldung:

```
> H10:=NG74[16]‘subgroup;
> #H10;
1024
> Q:=G74/H10;
>> Q:=G74/H10;
          ^
Runtime error in ’/’: Index of subgroup is too large
>
```

Rechnen in Verbänden

Wir haben es hier in dieser Arbeit mit 2 Typen von Verbänden zu tun:

1. Der Verband der Untermoduln eines G-Moduls ist der Verband der zur Gruppe G gehörenden Codes (s. Kap. 9). Auf die Implementierung in **Magma** sei hier hingewiesen: So ist die Inklusion von Codes über „`subset`“ prüfbar und der Durchschnitt zweier Codes wird über „`meet`“ gebildet. Die Vereinigung zweier Codes geschieht mit “+“.

2. Der Untergruppenverband der Automorphismengruppen. Zwar funktioniert der Durchschnitt mit „`meet`“, nicht jedoch die Vereinigung mit „`join`“ – auch nicht mit “+“.

Anhang B

Tabellen der zyklischen Codes

Die folgende Tabelle stellt eine statistische Zusammenfassung der mehr als 8000 gerechneten zyklischen Codes dar. Zum besseren Verständnis möchte ich auf folgendes hinweisen:

1. es sind sämtliche zyklischen Codes vollständig bis zur Codelänge $N = 70$ berechnet worden.

   Durch diese Vollständigkeit sind wir in der Lage, für einige Sätze in dieser Arbeit, für die noch kein allgemeingültiger Beweis angegeben werden konnte, zumindest einen teilweisen Beweis durch exemplarische Überprüfung bis zu dieser Codelänge zu geben.

2. für einige Codelängen $N > 70$ sind ebenfalls zyklische Codes gerechnet worden, um bestimmte Aussagen weiter abzusichern. Die Tabelle ist daher an dieser Stelle unterteilt. Aus Gründen der Ressourcen enthalten zwei dieser Berechnungen nicht sämtliche Codes (so konnten für $N = 80$ bei 2 Codepärchen (Rohcodes 275/276 und 277/278) die Automorphismengruppen nicht berechnet werden; ebenso für $N = 72$ bei 2 Codepärchen (707/708 und 727/728)). In einer separaten Bemerkungsspalte will ich darauf hinweisen.
   Immerhin wurden aber noch für folgende Codelängen sämtliche zyklischen Codes berechnet: $N = 73$, 74, 75, 76 ,77, 78, 81, 121, 125.
   Erscheint eine Zahl $N \leq 81$ nicht als Codelänge in dieser Tabelle (z.B. 17), so bedeutet dies, daß hierfür keine nicht-trivialen Codes im Sinne dieser Arbeit (s. Einleitung) existieren.

3. die Spalte „Anzahl Rohcodes“ gibt die Anzahl sämtlicher zyklischen Codes zu einer Codelänge an.
   Da diese Anzahl gewissen Gesetzmäßigkeiten unterliegt, ist dies in einem gesonderten Abschnitt dieser Arbeit behandelt (s. Kapitel 6).
   Die Spalte ist daher auch unterteilt worden, um in der zweiten Unterspalte die Po-

tenzdarstellung anzugeben. Dabei wurde auch in der Darstellung dieser Gesetzmäßigkeit Rechnung getragen:
So haben wir sowohl bei $N = 24$ oder $N = 40$, wie auch bei $N = 54$ jeweils 81 Rohcodes, aber aufgrund der unterschiedlichen Faktorenzerlegung
($2^3 \cdot 3$ oder $2^3 \cdot 5$, versus $2 \cdot 27$) schreiben wir zuerst 9^2, im letzteren Fall stattdessen 3^4.

4. die Spalte „Dichte“ gibt das Verhältnis von nicht-trivialen Codes zu Rohcodes an. Dabei sind bei der Berechnung der Dichte von der Anzahl Rohcodes stets die 4 trivialen Codes abgezogen worden, die für jede Codelänge existieren.
   Aussagen im Zusammenhang mit der Dichte finden sich im Abschnitt „Statistik“ 7.

5. die Automorphismengruppen werden im nächsten Kapitel dieses Anhangs näher beleuchtet – ihre Anzahl ist bereits hier eine interessante statistische Größe.

6. wenn bei geraden Codelängen mehr als der eine typische selbstduale Code auftritt (s. 1.16), so ist das in einer separaten Spalte vermerkt worden. Dieses Phänomen wird im Unterabschnitt 3.4 behandelt.

7. wenn bei der Bildung der Automorphismengruppen außer den typischen Permutationsgruppen (z.B die symmetrischen Gruppen) spezielle Permutationsgruppen involviert sind, so ist dies in der letzten Spalte vermerkt worden.

Code-länge	Anzahl Codes	Anzahl Rohcodes		Dichte in %	Anzahl Automorphismen-Gruppen	Anzahl Selbstduale Codes $\neq 1$	Spezialgruppe(n)
7	4	8	2^3	100	1		PSL(2,7) $\cong$ PSL(3,2)
10	5	9	3^2	100	2		
12	5	25	5^2	23,8	2		
14	23	27	3^3	100	5	3	PSL(2,7) $\cong$ PSL(3,2)
15	28	32	2^5	100	5		$\mathfrak{A}_8 \cong$ PSL(4,2)
16	5	17	N+1	38,5	2		
18	13	27	3^3	56,5	4		
20	21	25	5^2	100	8		
21	60	64	2^6	100	7		PSL(2,7) $\cong$ PSL(3,2), PSL(3,4)
22	5	9	3^2	100	2		
23	4	8	2^3	100	1		M23
24	29	81	9^2	37,7	9		
25	4	8	2^3	100	1		
26	5	9	3^2	100	2		
27	8	16	2^4	66,7	2		
28	121	125	5^3	100	21	5	PSL(2,7) $\cong$ PSL(3,2)
30	203	243	3^5	84,9	36	3	$\mathfrak{A}_8 \cong$ PSL(4,2)
31	36	128	2^7	29,0	1		PSL(5,2)
32	17	33	N+1	58,6	6		
33	12	32	2^5	42,9	8		
34	5	27	3^3	21,7	2		
35	60	64	2^6	100	7		PSL(2,7) $\cong$ PSL(3,2), $\mathfrak{MJ}(7,3)$
36	51	125	5^3	42,1	18		
38	5	9	3^2	100	2		
39	12	32	2^5	42,9	3		
40	77	81	9^2	100	27		
42	605	729	3^6	83,4	60	9	PSL(2,7) $\cong$ PSL(3,2), PSL(3,4)
44	21	25	5^2	100	8		
45	156	256	2^8	61,9	16		$\mathfrak{A}_8 \cong$ PSL(4,2)

Tabelle B.1: Tabelle der zyklischen Codes, Teil 1 von 3

Code-länge	Anzahl Codes	Anzahl Rohcodes		Dichte in %	Anzahl Automorphismen-Gruppen	Anzahl Selbstduale Codes $\neq 1$	Spezialgruppe(n)
46	23	27	3^3	100	5	3	M23
48	97	289	17^2	34,0	31		
49	28	32	2^5	100	4		PSL(2,7) $\cong$ PSL(3,2)
50	23	27	3^3	100	8		
51	76	256	2^8	30,2	4		PSL(2,16)
52	21	25	5^2	100	8		
54	53	81	3^4	68,9	17		
55	12	32	2^5	42,9	3		
56	725	729	9^3	100	76	9	PSL(2,7) $\cong$ PSL(3,2)
57	12	32	2^5	42,9	3		
58	5	9	3^2	100	2		
60	2121	3125	5^5	68,0	213	5	$\mathfrak{A}_8 \cong$ PSL(4,2)
62	221	2187	3^7	10,1	7	13	PSL(5,2)
63	1052	8192	2^{13}	12,8	26		PSL(2,7) $\cong$ PSL(3,2), PSL(3,4), PSL(6,2), PSL(2,8), $\mathfrak{MZ}(7,3)$
64	41	65	N+1	67,2	15		
65	12	128	2^7	9,7	3		
66	77	243	3^5	32,2	24		
68	21	125	5^3	17,4	8		
69	52	64	2^6	86,7	6		M23
70	725	729	9^3	100	62	9	PSL(2,7) $\cong$ PSL(3,2), $\mathfrak{MZ}(7,3)$

Tabelle B.2: Tabelle der zyklischen Codes, Teil 2 von 3

Code-länge	Anzahl Codes	Anzahl Rohcodes		Dichte in %	Anzahl Automorphismen-Gruppen	Anzahl Selbstduale Codes $\neq 1$	Bemerkung oder Spezialgruppe(n)
72	$\geq$235	729	9^3	$\geq$32,4	$\geq$70		ohne Rohcodes Nr. 707/708 u. 727/728
73	48	512	2^9	9,4	1		PSL(3,8)
74	5	9	3^2	100	2		
75	252	256	2^8	100	18		
76	21	25	5^2	100	8		
77	60	64	2^6	100	7		PSL(2,7) $\cong$ PSL(3,2), $\mathfrak{MZ}(7,3)$
78	77	243	3^5	32,2	24		
80	$\geq$281	289	17^2	100	$\geq$80		ohne Rohcodes Nr. 275/276 u. 277/278
81	24	32	2^5	85,7	6		
85	256	4096	2^{12}	6,26	8		PSL(4,4), PSL(2,16), $\mathfrak{MZ}(17,8)$
89	0	512	2^9	0	0		$\mathfrak{MZ}(89,11)$ auflösbar
91	60	1024	2^{10}	5,88	7		PSL(2,7) $\cong$ PSL(3,2)
92	121	125	5^3	100	21	5	M23
100	$\geq$ 119	125	5^3	$\geq 98,3$	$\geq$ 37		
110	77	243	3^5	32,2	24		
119	368	512	2^9	72,4	13		PSL(2,7) $\cong$ PSL(3,2), $\mathfrak{MZ}(7,3)$, $\mathfrak{MZ}(17,8)$
121	4	8	2^3	100	1		
125	12	16	2^4	100	3		

Tabelle B.3: Tabelle der zyklischen Codes, Teil 3 von 3

Anhang C

Tabellenwerk der Automorphismengruppen für zyklische Codes, Einführung

Das folgende Tabellenwerk stellt eine Zusammenfassung aller Automorphismengruppen (>1000) der mehr als 8000 gerechneten nichttrivialen (im Sinne dieser Arbeit) zyklischen Codes dar. Zum besseren Verständnis möchte ich auf folgendes hinweisen:

1. es sind sämtliche Automorphismengruppen sämtlicher nichttrivialen (im Sinne dieser Arbeit) zyklischen Codes vollständig bis zur Codelänge $N = 70$ berechnet worden.

2. für einige Codelängen $N > 70$ sind ebenfalls zyklische Codes gerechnet worden, um bestimmte Aussagen weiter abzusichern. Aus Gründen der Ressourcen enthalten zwei dieser Berechnungen nicht sämtliche Codes (so konnten für $N = 80$ bei 2 Codepärchen (Rohcodes 275/276 und 277/278) die Automorphismengruppen nicht berechnet werden; ebenso für $N = 72$ bei 2 Codepärchen (707/708 und 727/728)).
   Immerhin wurden aber noch für folgende Codelängen sämtliche zyklischen Codes und sämtliche Automorphismengruppen berechnet: $N = 73$, 74, 75, 76 ,77, 78, 81, 121, 125.
   Erscheint eine Zahl $N \leq 81$ nicht als Codelänge in dieser Tabelle (z.B. 17), so bedeutet dies, daß hierfür keine nicht-trivialen Codes im Sinne dieser Arbeit (s. Einleitung) existieren.

   Durch diese Vollständigkeit sind wir in der Lage, für einige Sätze in dieser Arbeit, für die noch kein allgemeingültiger Beweis angegeben werden konnte, zumindest einen teilweisen Beweis durch exemplarische Überprüfung bis zu dieser Codelänge zu geben.

3. die Spalten des Tabellenwerk sollten eigentlich selbsterklärend sein, dennoch einige kurze Anmerkungen dazu:
   Nach der Spalte mit der fortlaufenden Nummer und der Spalte mit der Ordnung der Automorphismengruppen folgt die Spalte „Anz.“. Die Eintragung in dieser Spalte gibt die Häufigkeit der jeweiligen Gruppe an, d.h., die Anzahl der zyklischen Codes, die zu dieser Automorphismengruppe gehört.
   Mitunter finden sich bei bestimmten Codelängen ($N = 14, 28, 30, 42, 46, 56, 60, 62$) hier Eintragungen, wie z.B.: „2/6“.
   Das soll heißen: „2 von 6 zyklischen Codes zu dieser Automorphismengruppe sind selbstdual“.
   Bei diesen Tabellen ist die Gesamtzahl der selbstdualen Codes in der Summenzeile der Tabelle eingearbeitet worden.
   Alle übrigen geraden Codelängen (mit $N = 2 \cdot l$) besitzen genau einen selbstdualen Code, der zur Automorphismengruppe $\mathfrak{S}_2 \wr \mathfrak{S}_l$ gehört, welche aus diesem Grund stets mit ungeradem Wert in dieser Spalte erscheint. Auf eine besondere Darstellung dieser allgemeinen Fälle im Tabellenwerk ist daher verzichtet worden.

4. die Spalte „Formeltyp“ gibt die Nummer der allgemeinen Formel der jeweiligen Automorphismengruppe im Textteil dieser Arbeit an. Dort werden ggfs. noch weitere Eigenschaften der zyklischen Codes zu dieser Automorphismengruppe aufgezeigt, wie z.B. Dimension k, Minimaldistanz d und Anzahl der Codes zu dieser Gruppe.

5. die letzte Spalte „Produktformel“ zeigt die Zusammensetzung der Automorphismengruppe aus den einzelnen Faktoren. Dabei werden die unterschiedlichen Gruppenprodukttypen Kranzprodukt, direktes Produkt und semidirektes Produkt, sowie die Quotientenbildung verwendet. Tritt ein Faktor mit Potenz auf, wie z.B.: $\mathfrak{S}_2^3$, so ist dies die Kurzschreibweise für $\mathfrak{S}_2 \times \mathfrak{S}_2 \times \mathfrak{S}_2$.
   Soweit es technisch möglich war, sind diese Angaben mit dem Computeralgebrasystem Magma auf Isomorphie überprüft worden.

   Auf eine Besonderheit möchte ich an dieser Stelle noch beispielhaft hinweisen:
   Bei der Codelänge $N = 56$ ist für die Automorphismengruppen Nr. 37 und Nr. 56 nicht nur die Gruppenordnung gleich, sondern auch die Produktformel – d.h., die Darstellung der Produktformel ist nicht eindeutig! In beiden Fällen ist die Gruppe mit der Nr. 21 die Basisgruppe, deren Normalteiler finden wir in
   `NG21:=NormalSubgroups(G21)`; Im ersten Fall bekommen wir $G37 \cong G21/NG21[69]$, im zweiten Fall $G56 \cong G21/NG21[67]$.

Anhang D

Tabellen der Automorphismengruppen für zyklische Codes, Teil 1 ($7 \leq N \leq 28$)

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	168	4	Gruppe	$PSL(3,2) \cong PSL(2,7)$
	Anzahl Codes:	4		

Tabelle D.1: Tabelle der Automorphismengruppen für N=7

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	28800	2	(1.16)	$\mathfrak{S}_5 \wr \mathfrak{S}_2$
2	3840	3	(1.17)	$\mathfrak{S}_2 \wr \mathfrak{S}_5$
	Anzahl Codes:	5		

Tabelle D.2: Tabelle der Automorphismengruppen für N=10

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	1036800	2	(1.16)	$\mathfrak{S}_6 \wr \mathfrak{S}_2$
2	46080	3	(1.17)	$\mathfrak{S}_2 \wr \mathfrak{S}_6$
	Anzahl Codes:	5		

Tabelle D.3: Tabelle der Automorphismengruppen für N=12

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	50803200	2	(1.16)	$\mathfrak{S}_7 \wr \mathfrak{S}_2$
2	21504	8	(3.135)	$\mathfrak{S}_2 \wr PSL(3,2)$
3	2688	4	(3.138)	$(\mathfrak{S}_2 \wr PSL(3,2))/\mathfrak{S}_2^3$
4	56448	2/6	(3.136)	$PSL(3,2) \wr \mathfrak{S}_2$
5	645120	1/3	(1.17)	$\mathfrak{S}_2 \wr \mathfrak{S}_7$
	Anzahl Codes:	23	davon 3	selbstdual

Tabelle D.4: Tabelle der Automorphismengruppen für N=14

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	10368000	4	(1.74)	$\mathfrak{S}_5 \wr \mathfrak{S}_3$
2	20160	8	Gruppe	$PSL(4,2) \cong \mathfrak{A}_8$
3	933120	4	(1.75)	$\mathfrak{S}_3 \wr \mathfrak{S}_5$
4	360	8		$\mathfrak{Z}_3 \rtimes \mathfrak{S}_5$
5	720	4	(1.72)	$\mathfrak{S}_5 \times \mathfrak{S}_3$
	Anzahl Codes:	28		

Tabelle D.5: Tabelle der Automorphismengruppen für N=15

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	3251404800	2	(1.16)	$\mathfrak{S}_8 \wr \mathfrak{S}_2$
2	10321920	3	(1.17)	$\mathfrak{S}_2 \wr \mathfrak{S}_8$
	Anzahl Codes:	5		

Tabelle D.6: Tabelle der Automorphismengruppen für N=16

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	263363788800	2	(1.16)	$\mathfrak{S}_9 \wr \mathfrak{S}_2$
2	2239488000	4	(1.74)	$\mathfrak{S}_6 \wr \mathfrak{S}_3$
3	33592320	4	(1.75)	$\mathfrak{S}_3 \wr \mathfrak{S}_6$
4	185794560	3	(1.17)	$\mathfrak{S}_2 \wr \mathfrak{S}_9$
	Anzahl Codes:	13		

Tabelle D.7: Tabelle der Automorphismengruppen für N=18

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	26336378880000	2	(1.18)	$\mathfrak{S}_{10} \wr \mathfrak{S}_2$
2	4976640000	4	(1.22)	$\mathfrak{S}_5 \wr \mathfrak{S}_4$
3	955514880	4	(1.23)	$\mathfrak{S}_4 \wr \mathfrak{S}_5$
4	3932160	2	(1.20)	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_5$
5	737280	2	(1.28) (1.29)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_5))/\mathfrak{S}_2^5$ $\cong (\mathfrak{K}_4 \wr \mathfrak{S}_5) \rtimes \mathfrak{S}_3$
6	29491200	2	(1.21)	$\mathfrak{S}_2 \wr \mathfrak{S}_5 \wr \mathfrak{S}_2$
7	2880	2	(1.24)	$\mathfrak{S}_4 \times \mathfrak{S}_5$
8	3715891200	3	(1.19)	$\mathfrak{S}_2 \wr \mathfrak{S}_{10}$
	Anzahl Codes:	21		

Tabelle D.8: Tabelle der Automorphismengruppen für N=20

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	768144384000	4	(1.74)	$\mathfrak{S}_7 \wr \mathfrak{S}_3$
2	47029248	8	(1.114)	$\mathfrak{S}_3 \wr PSL(3,2)$
3	1008	24	(1.116)	$\mathfrak{S}_3 \times PSL(3,2)$
4	1410877440	4	(1.75)	$\mathfrak{S}_3 \wr \mathfrak{S}_7$
5	30240	4	(1.72)	$\mathfrak{S}_7 \times \mathfrak{S}_3$
6	28449792	8	(1.113)	$PSL(3,2) \wr \mathfrak{S}_3$
7	120960	8		$PSL(3,4) \rtimes \mathfrak{S}_3$
	Anzahl Codes:	60		

Tabelle D.9: Tabelle der Automorphismengruppen für N=21

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	3186701844480000	2	(1.16)	$\mathfrak{S}_{11} \wr \mathfrak{S}_2$
2	81749606400	3	(1.17)	$\mathfrak{S}_2 \wr \mathfrak{S}_{11}$
	Anzahl Codes:	5		

Tabelle D.10: Tabelle der Automorphismengruppen für N=22

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	10200960	4	Gruppe	$M23$
	Anzahl Codes:	4		

Tabelle D.11: Tabelle der Automorphismengruppen für N=23

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	458885065605120000	2	(1.18)	$\mathfrak{S}_{12} \wr \mathfrak{S}_2$
2	393289924608000	4	(1.74)	$\mathfrak{S}_8 \wr \mathfrak{S}_3$
3	6449725440000	4	(1.22)	$\mathfrak{S}_6 \wr \mathfrak{S}_4$
4	137594142720	4	(1.23)	$\mathfrak{S}_4 \wr \mathfrak{S}_6$
5	188743680	2	(1.20)	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_6$
6	67722117120	4	(1.75)	$\mathfrak{S}_3 \wr \mathfrak{S}_8$
7	241920	4	(1.72)	$\mathfrak{S}_8 \times \mathfrak{S}_3$
8	4246732800	2	(1.21)	$\mathfrak{S}_2 \wr \mathfrak{S}_6 \wr \mathfrak{S}_2$
9	1961990553600	3	(1.19)	$\mathfrak{S}_2 \wr \mathfrak{S}_{12}$
	Anzahl Codes:	29		

Tabelle D.12: Tabelle der Automorphismengruppen für N=24

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	2985984000000	4	(1.101)	$\mathfrak{S}_5 \wr \mathfrak{S}_5$
	Anzahl Codes:	4		

Tabelle D.13: Tabelle der Automorphismengruppen für N=25

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	775515760872652800000	2	(1.16)	$\mathfrak{S}_{13} \wr \mathfrak{S}_2$
2	51011754393600	3	(1.17)	$\mathfrak{S}_2 \wr \mathfrak{S}_{13}$
	Anzahl Codes:	5		

Tabelle D.14: Tabelle der Automorphismengruppen für N=26

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	286708355039232000	4	(1.74)	$\mathfrak{S}_9 \wr \mathfrak{S}_3$
2	3656994324480	4	(1.75)	$\mathfrak{S}_3 \wr \mathfrak{S}_9$
	Anzahl Codes:	8		

Tabelle D.15: Tabelle der Automorphismengruppen für N=27

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	15200108913103994880000	2	(1.18)	$\mathfrak{S}_{14} \wr \mathfrak{S}_2$
2	770527199232	8	(1.36)	$\mathfrak{S}_4 \wr PSL(3,2)$
3	15485790781440000	4	(1.22)	$\mathfrak{S}_7 \wr \mathfrak{S}_4$
4	44040192	12	(1.42)	$\mathfrak{S}_2 \wr ((\mathfrak{S}_2 \wr PSL(3,2))/\mathfrak{S}_2^3)$
5	924844032	12	(1.34)	$\mathfrak{S}_2 \wr PSL(3,2) \wr \mathfrak{S}_2$
6	258048	8	(1.46)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times PSL(3,2)))/\mathfrak{S}_2^{13}$
			(1.48)	$\cong ((\mathfrak{K}_4 \wr PSL(3,2))/\mathfrak{K}_4^3) \rtimes \mathfrak{S}_3$
7	23115815976960	4	(1.23)	$\mathfrak{S}_4 \wr \mathfrak{S}_7$
8	4032	20	(1.37)	$\mathfrak{S}_4 \times PSL(3,2)$
9	10569646080	2	(1.20)	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_7$
10	495452160	2	(1.28)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_7))/\mathfrak{S}_2^7$
			(1.29)	$\cong (\mathfrak{K}_4 \wr \mathfrak{S}_7) \rtimes \mathfrak{S}_3$
11	14450688	8	(1.43)	$((\mathfrak{S}_2 \wr PSL(3,2))/\mathfrak{S}_2^3) \wr \mathfrak{S}_2$
12	352321536	8	(1.33)	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr PSL(3,2)$
13	120960	2	(1.24)	$\mathfrak{S}_7 \times \mathfrak{S}_4$
14	1344	4	(1.39)	$PSL(3,2) \times (\mathfrak{S}_2 \wr \mathfrak{S}_2)$
15	19118260224	8	(1.35)	$PSL(3,2) \wr \mathfrak{S}_4$
16	832359628800	2	(1.21)	$\mathfrak{S}_2 \wr \mathfrak{S}_7 \wr \mathfrak{S}_2$
17	16515072	4	(1.30)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times PSL(3,2)))/\mathfrak{S}_2^7$
			(1.31)	$\cong (\mathfrak{K}_4 \wr PSL(3,2)) \rtimes \mathfrak{S}_3$
18	86016	4	(1.41)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_2 \times PSL(3,2)))/\mathfrak{S}_2^6$
19	1428329123020800	1/3	(1.19)	$\mathfrak{S}_2 \wr \mathfrak{S}_{14}$
20	6372753408	2/2	(1.38)	$PSL(3,2) \wr \mathfrak{S}_2 \wr \mathfrak{S}_2$
21	5505024	2/2	(1.40)	$\mathfrak{S}_2 \wr (\mathfrak{S}_2 \times PSL(3,2))$
	Anzahl Codes:	121	davon 5	selbstdual

Tabelle D.16: Tabelle der Automorphismengruppen für N=28

Anhang E

Tabellen der Automorphismengruppen für zyklische Codes, Teil 2 ($30 \leq N \leq 49$)

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	342002450544839884800000	2	(1.18)	$\mathfrak{S}_{15} \wr \mathfrak{S}_2$
2	286708355039232000000	4	(1.74)	$\mathfrak{S}_{10} \wr \mathfrak{S}_3$
3	660602880	16	(3.135)	$\mathfrak{S}_2 \wr PSL(4,2)$
4	214990848000000	2	(1.85)	$\mathfrak{S}_5 \wr \mathfrak{S}_3 \wr \mathfrak{S}_2$
5	143327232000000	2	(1.84)	$\mathfrak{S}_5 \wr \mathfrak{S}_2 \wr \mathfrak{S}_3$
6	23219011584000000	4	(1.78)	$\mathfrak{S}_6 \wr \mathfrak{S}_5$
7	2149908480000000	4	(1.79)	$\mathfrak{S}_5 \wr \mathfrak{S}_6$
8	11796480	16	$\mathfrak{S}_2 \wr$ N15Gr4	$\mathfrak{S}_2 \wr (\mathfrak{Z}_3 \rtimes \mathfrak{S}_5)$
9	23592960	8	(3.80)	$\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_5)$
10	645120	2/10	(10.6)	$(\mathfrak{S}_2 \wr PSL(4,2))/\mathfrak{S}_2^{10}$
11	232190115840	2	(1.82)	$\mathfrak{S}_3 \wr \mathfrak{S}_2 \wr \mathfrak{S}_5$
12	812851200	12	(3.136)	$PSL(4,2) \wr \mathfrak{S}_2$
13	92160	4	(3.101) (3.102)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_5 \times \mathfrak{S}_3))/\mathfrak{S}_2^8$ $\cong \mathfrak{S}_4 \times (\mathfrak{S}_2 \wr \mathfrak{S}_5)$
14	1741425868800	2	(1.83)	$\mathfrak{S}_3 \wr \mathfrak{S}_5 \wr \mathfrak{S}_2$
15	46080	4		$\mathfrak{S}_2^7 \rtimes (\mathfrak{Z}_3 \rtimes \mathfrak{S}_5)$
16	8640	2	(3.82)	$(\mathfrak{S}_3 \wr \mathfrak{S}_2) \times \mathfrak{S}_5$
17	86400	4	(1.86)	$\mathfrak{S}_6 \times \mathfrak{S}_5$
18	219419659468800	4	(1.75)	$\mathfrak{S}_3 \wr \mathfrak{S}_{10}$
19	30576476160	4	(1.80)	$\mathfrak{S}_2 \wr \mathfrak{S}_3 \wr \mathfrak{S}_5$
20	184320	4		$(\mathfrak{S}_2 \wr (\mathfrak{Z}_3 \rtimes \mathfrak{S}_5))/\mathfrak{S}_2^6$
21	172800	2	(3.85)	$(\mathfrak{S}_5 \wr \mathfrak{S}_2) \times \mathfrak{S}_3$
22	43200	12		$(\mathfrak{A}_5 \wr \mathfrak{S}_2) \rtimes \mathfrak{S}_3$
23	368640	2	(3.100)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_5))/\mathfrak{S}_2^6$
24	21772800	4	(1.72)	$\mathfrak{S}_3 \times \mathfrak{S}_{10}$
25	259200	12	N15Gr4$\wr\mathfrak{S}_2$	$(\mathfrak{Z}_3 \rtimes \mathfrak{S}_5) \wr \mathfrak{S}_2$
26	1036800	6	(3.81)	$(\mathfrak{S}_3 \times \mathfrak{S}_5) \wr \mathfrak{S}_2$
27	41287680	4	(3.140)	$(\mathfrak{S}_2 \wr PSL(4,2))/\mathfrak{S}_2^4$
28	339738624000	4	(1.81)	$\mathfrak{S}_2 \wr \mathfrak{S}_5 \wr \mathfrak{S}_3$
29	1911029760	2	(3.75)	$(\mathfrak{S}_2 \wr \mathfrak{S}_3 \wr \mathfrak{S}_5)/\mathfrak{S}_2^4$
30	720	8	N15Gr4$\times\mathfrak{S}_2$	$(\mathfrak{Z}_3 \rtimes \mathfrak{S}_5) \times \mathfrak{S}_2$
31	2160	12		$(\mathfrak{Z}_3 \wr \mathfrak{S}_2) \rtimes \mathfrak{S}_5$
32	23040	2	(3.87) (3.86)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_5))/\mathfrak{S}_2^{10}$ $\cong (\mathfrak{S}_2 \wr \mathfrak{S}_5) \times \mathfrak{S}_3$

Tabelle E.1: Tabelle der Automorphismengruppen für N=30, Teil 1 von 2

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
33	11520	16		$(\mathfrak{S}_2 \wr (\mathfrak{Z}_3 \rtimes \mathfrak{S}_5))/\mathfrak{S}_2^{10}$ $\cong \mathfrak{Z}_3 \rtimes (\mathfrak{S}_2 \wr \mathfrak{S}_5)$
34	84934656000	2	(3.76)	$(\mathfrak{S}_2 \wr \mathfrak{S}_5 \wr \mathfrak{S}_3)/\mathfrak{S}_2^2$
35	5760	2	(3.84) (3.83)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_5))/\mathfrak{S}_2^{12}$ $\cong (\mathfrak{S}_2 \wr \mathfrak{S}_3) \times \mathfrak{S}_5$
36	42849873690624000	1/3	(1.19)	$\mathfrak{S}_2 \wr \mathfrak{S}_{15}$
	Anzahl Codes:	203	davon 3	selbstdual

Tabelle E.2: Tabelle der Automorphismengruppen für N=30, Teil 2 von 2

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	9999360	36	Gruppe	$PSL(5,2)$
	Anzahl Codes:	36		

Tabelle E.3: Tabelle der Automorphismengruppen für N=31

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	87552627339479010508800000 0	2	(1.18)	$\mathfrak{S}_{16} \wr \mathfrak{S}_2$
2	63429799040778240000	4	(1.22)	$\mathfrak{S}_8 \wr \mathfrak{S}_4$
3	4438236667576320	4	(1.23)	$\mathfrak{S}_4 \wr \mathfrak{S}_8$
4	676457349120	2	(1.20)	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_8$
5	213084064972800	2	(1.21)	$\mathfrak{S}_2 \wr \mathfrak{S}_8 \wr \mathfrak{S}_2$
6	1371195958099968000	3	(1.19)	$\mathfrak{S}_2 \wr \mathfrak{S}_{16}$
	Anzahl Codes:	17		

Tabelle E.4: Tabelle der Automorphismengruppen für N=32

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	381608820557217792000000	4	(1.74)	$\mathfrak{S}_{11} \wr \mathfrak{S}_3$
2	14481697524940800	4	(1.75)	$\mathfrak{S}_3 \wr \mathfrak{S}_{11}$
3	239500800	4	(1.72)	$\mathfrak{S}_{11} \times \mathfrak{S}_3$
	Anzahl Codes:	12		

Tabelle E.5: Tabelle der Automorphismengruppen für N=33

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	25302709301109434037043200000 0	2	(1.16)	$\mathfrak{S}_{17} \wr \mathfrak{S}_2$
2	46620662575398912000	3	(1.17)	$\mathfrak{S}_2 \wr \mathfrak{S}_{17}$
	Anzahl Codes:	5		

Tabelle E.6: Tabelle der Automorphismengruppen für N=34

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	60197437440000000	8	(1.114)	$\mathfrak{S}_5 \wr PSL(3,2)$
2	390241927692288000000	4	(1.101)	$\mathfrak{S}_7 \wr \mathfrak{S}_5$
3	1805923123200000000	4	(1.102)	$\mathfrak{S}_5 \wr \mathfrak{S}_7$
4	20160	24	(1.116)	$\mathfrak{S}_5 \times PSL(3,2)$
5	604800	4	(1.105)	$\mathfrak{S}_5 \times \mathfrak{S}_7$
6	16059338588160	8	(1.113)	$PSL(3,2) \wr \mathfrak{S}_5$
7	2520	8	(1.118)	$\mathfrak{S}_5 \times \mathfrak{MZ}(7,3)$
	Anzahl Codes:	60		

Tabelle E.7: Tabelle der Automorphismengruppen für N=35;
$\mathfrak{MZ}(7,3) := \mathfrak{Z}_7 \rtimes \mathfrak{Z}_3$ metazyklisch

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	8198077813559456628001996800000	2	(1.18)	$\mathfrak{S}_{18} \wr \mathfrak{S}_2$
2	659420041922872344576000000	4	(1.74)	$\mathfrak{S}_{12} \wr \mathfrak{S}_3$
3	416162911506546032640000	4	(1.22)	$\mathfrak{S}_9 \wr \mathfrak{S}_4$
4	10030613004288000000	2	(1.85)	$\mathfrak{S}_6 \wr \mathfrak{S}_3 \wr \mathfrak{S}_2$
5	6687075336192000000	2	(1.84)	$\mathfrak{S}_6 \wr \mathfrak{S}_2 \wr \mathfrak{S}_3$
6	100306130042880000000	4	(1.78)	$\mathfrak{S}_6 \wr \mathfrak{S}_6$
7	100306130042880	2	(1.82)	$\mathfrak{S}_3 \wr \mathfrak{S}_2 \wr \mathfrak{S}_6$
8	958659120196485120	4	(1.23)	$\mathfrak{S}_4 \wr \mathfrak{S}_9$
9	2256887925964800	2	(1.83)	$\mathfrak{S}_3 \wr \mathfrak{S}_6 \wr \mathfrak{S}_2$
10	48704929136640	2	(1.20)	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_9$
11	570760888320	2	(1.28) (1.29)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_9))/\mathfrak{S}_2^9$ $\cong (\mathfrak{K}_4 \wr \mathfrak{S}_9) \rtimes \mathfrak{S}_3$
12	1042682221795737600	4	(1.75)	$\mathfrak{S}_3 \wr \mathfrak{S}_{12}$
13	8806025134080	4	(1.80)	$\mathfrak{S}_2 \wr \mathfrak{S}_3 \wr \mathfrak{S}_6$
14	8709120	2	(1.24)	$\mathfrak{S}_9 \times \mathfrak{S}_4$
15	587068342272000	4	(1.81)	$\mathfrak{S}_2 \wr \mathfrak{S}_6 \wr \mathfrak{S}_3$
16	69039237051187200	2	(1.21)	$\mathfrak{S}_2 \wr \mathfrak{S}_9 \wr \mathfrak{S}_2$
17	146767085568000	2	(3.76)	$(\mathfrak{S}_2 \wr \mathfrak{S}_6 \wr \mathfrak{S}_3)/\mathfrak{S}_2^2$
18	1678343852714360832000	3	(1.19)	$\mathfrak{S}_2 \wr \mathfrak{S}_{18}$
	Anzahl Codes:	51		

Tabelle E.8: Tabelle der Automorphismengruppen für N=36

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	295950609069496384270872084480000000	2	(1.18)	$\mathfrak{S}_{19} \wr \mathfrak{S}_2$
2	63777066403145711616000	3	(1.19)	$\mathfrak{S}_2 \wr \mathfrak{S}_{19}$
	Anzahl Codes:	5		

Tabelle E.9: Tabelle der Automorphismengruppen für N=38

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	144874583210455054103347200000	4	(1.74)	$\mathfrak{S}_{13} \wr \mathfrak{S}_3$
2	81329213300067532800	4	(1.75)	$\mathfrak{S}_3 \wr \mathfrak{S}_{13}$
3	37362124800	4	(1.72)	$\mathfrak{S}_{13} \times \mathfrak{S}_3$
	Anzahl Codes:	12		

Tabelle E.10: Tabelle der Automorphismengruppen für N=39

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	118380243627798553708348/ 83379200000000	2	(1.18)	$\mathfrak{S}_{20} \wr \mathfrak{S}_2$
2	41616291150654603264000000000	4	(1.22)	$\mathfrak{S}_{10} \wr \mathfrak{S}_4$
3	12787447486620893184000000	4	(1.52)	$\mathfrak{S}_8 \wr \mathfrak{S}_5$
4	16511297126400000000	2	(1.53)	$\mathfrak{S}_5 \wr \mathfrak{S}_2 \wr \mathfrak{S}_4$
5	49533891379200000000	2	(1.54)	$\mathfrak{S}_5 \wr \mathfrak{S}_4 \wr \mathfrak{S}_2$
6	243468982907043840	2	(1.55)	$\mathfrak{S}_4 \wr \mathfrak{S}_2 \wr \mathfrak{S}_5$
7	773094113280	4	$\mathfrak{S}_2 \wr$(1.28)	$\mathfrak{S}_2 \wr (\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_5))/\mathfrak{S}_2^5)$
8	1733686198272000000000	4	(1.51)	$\mathfrak{S}_5 \wr \mathfrak{S}_8$
9	1826017371802828800	2	(1.56)	$\mathfrak{S}_4 \wr \mathfrak{S}_5 \wr \mathfrak{S}_2$
10	3019898880	4	(1.65)	$\mathfrak{S}_2 \wr (\mathfrak{S}_4 \times \mathfrak{S}_5)$
11	737280	4	(3.101)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_4 \times \mathfrak{S}_5))/\mathfrak{S}_2^{12}$
12	230078188847156428800	4	(1.23)	$\mathfrak{S}_4 \wr \mathfrak{S}_{10}$
13	138240	2	(1.61)	$(\mathfrak{S}_4 \wr \mathfrak{S}_2) \times \mathfrak{S}_5$
14	4838400	4	(1.59)	$\mathfrak{S}_8 \times \mathfrak{S}_5$
15	3896394330931200	2	(1.20)	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_{10}$
16	30923764531200	2	(1.49)	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_5 \wr \mathfrak{S}_2$
17	120795955200	2	(1.67)	$\mathfrak{S}_2 \wr (\mathfrak{S}_2 \times \mathfrak{S}_5) \wr \mathfrak{S}_2$
18	1087163596800	2	(1.28)$\wr\mathfrak{S}_2$	$((\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_5))/\mathfrak{S}_2^5) \wr \mathfrak{S}_2$
19	4123168604160	2	(1.50)	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_5$
20	1001929970810880	4	(1.57)	$\mathfrak{S}_2 \wr \mathfrak{S}_4 \wr \mathfrak{S}_5$
21	16588800	4	(1.64)	$(\mathfrak{S}_4 \times \mathfrak{S}_5) \wr \mathfrak{S}_2$
22	5218385264640000	4	(1.58)	$\mathfrak{S}_2 \wr \mathfrak{S}_5 \wr \mathfrak{S}_4$
23	62620623175680	2	(3.75)	$(\mathfrak{S}_2 \wr \mathfrak{S}_4 \wr \mathfrak{S}_5)/\mathfrak{S}_2^4$
24	27615694820474880000	2	(1.21)	$\mathfrak{S}_2 \wr \mathfrak{S}_{10} \wr \mathfrak{S}_2$
25	1006632960	2	(1.66)	$\mathfrak{S}_2 \wr (\mathfrak{S}_5 \times (\mathfrak{S}_2 \wr \mathfrak{S}_2))$
26	2551082656125828464640000	3	(1.19)	$\mathfrak{S}_2 \wr \mathfrak{S}_{20}$
27	46080	2	(3.84) (1.60)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_4 \times \mathfrak{S}_5))/\mathfrak{S}_2^{16}$ $\cong (\mathfrak{S}_2 \wr \mathfrak{S}_4) \times \mathfrak{S}_5$
	Anzahl Codes:	77		

Tabelle E.11: Tabelle der Automorphismengruppen für N=40

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	52205687439859162185381/ 83570227200000000	2	(1.18)	$\mathfrak{S}_{21} \wr \mathfrak{S}_2$
2	39753585632948866845959847168000000	4	(1.74)	$\mathfrak{S}_{14} \wr \mathfrak{S}_3$
3	16851429847203840000000	8	(1.114)	$\mathfrak{S}_6 \wr PSL(3,2)$
4	11800915893414789120000000	2	(1.85)	$\mathfrak{S}_7 \wr \mathfrak{S}_3 \wr \mathfrak{S}_2$
5	786727726227652608000000	2	(1.84)	$\mathfrak{S}_7 \wr \mathfrak{S}_2 \wr \mathfrak{S}_3$
6	2113929216	48	(3.107)	$\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times PSL(3,2))$
7	210642873090048	8	$\mathfrak{S}_3 \wr$(3.138)	$\mathfrak{S}_3 \wr ((\mathfrak{S}_2 \wr PSL(3,2))/\mathfrak{S}_2^3)$
8	11800915893414789120000000	4	(1.111)	$\mathfrak{S}_7 \wr \mathfrak{S}_6$
9	4423500334891008	12	$\mathfrak{S}_3 \wr$(3.136)	$\mathfrak{S}_3 \wr PSL(3,2) \wr \mathfrak{S}_2$
10	505542895416115200000000	4	(1.110)	$\mathfrak{S}_6 \wr \mathfrak{S}_7$
11	12096	28	(3.111)	$(\mathfrak{S}_3 \wr \mathfrak{S}_2) \times PSL(3,2)$
12	64512	24	(3.115)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times PSL(3,2)))/\mathfrak{S}_2^{15}$ $\cong \mathfrak{S}_4 \times ((\mathfrak{S}_2 \wr PSL(3,2))/\mathfrak{S}_2^3)$
13	129024	8	(3.115)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times PSL(3,2)))/\mathfrak{S}_2^{14}$
14	120960	32	(1.116)	$\mathfrak{S}_6 \times PSL(3,2)$
15	63417876480	8	(3.80)	$\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_7)$
16	50554289541611520	2	(1.82)	$\mathfrak{S}_3 \wr \mathfrak{S}_2 \wr \mathfrak{S}_7$
17	338688	24	(3.114)	$(PSL(3,2) \wr \mathfrak{S}_2) \times \mathfrak{S}_3$
18	59663538192384	16	(3.135)$\wr\mathfrak{S}_3$	$\mathfrak{S}_2 \wr PSL(3,2) \wr \mathfrak{S}_3$
19	253671505920	16	$\mathfrak{S}_2 \wr$N21Gr7	$\mathfrak{S}_2 \wr (PSL(3,4) \rtimes \mathfrak{S}_3)$
20	2032128	36	(3.108)	$(\mathfrak{S}_3 \times PSL(3,2)) \wr \mathfrak{S}_2$
21	516096	12	(3.115)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times PSL(3,2)))/\mathfrak{S}_2^{12}$
22	16128	20	(3.115) $\mathfrak{S}_3 \times$(3.138)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times PSL(3,2)))/\mathfrak{S}_2^{17}$ $\cong ((\mathfrak{S}_2 \wr PSL(3,2))/\mathfrak{S}_2^3) \times \mathfrak{S}_3$
23	15482880	4	(3.101) (3.102)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_7))/\mathfrak{S}_2^{12}$ $\cong \mathfrak{S}_4 \times (\mathfrak{S}_2 \wr \mathfrak{S}_7)$
24	1685142984720384	8	$\mathfrak{S}_3 \wr$(3.135)	$\mathfrak{S}_3 \wr \mathfrak{S}_2 \wr PSL(3,2)$
25	362880	2	(3.82)	$(\mathfrak{S}_3 \wr \mathfrak{S}_2) \times \mathfrak{S}_7$
26	29132587008	8	(3.79)	$(((\mathfrak{S}_2 \wr PSL(3,2))/\mathfrak{S}_2^3) \wr \mathfrak{S}_3)/\mathfrak{S}_2^2$
27	3628800	4	(1.112)	$\mathfrak{S}_7 \times \mathfrak{S}_6$
28	123863040	4		$(\mathfrak{S}_2 \wr (PSL(3,4) \rtimes \mathfrak{S}_3))/\mathfrak{S}_2^{11}$
29	129024	28	(3.113) (3.112)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times PSL(3,2)))/\mathfrak{S}_2^{14}$ $\cong (\mathfrak{S}_2 \wr PSL(3,2)) \times \mathfrak{S}_3$
30	8064	2/50	(3.110) (3.109)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times PSL(3,2)))/\mathfrak{S}_2^{18}$ $\cong (\mathfrak{S}_2 \wr \mathfrak{S}_3) \times PSL(3,2)$

Tabelle E.12: Tabelle der Automorphismengruppen für N=42, Teil 1 von 2

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
31	3981150301401907200	2	(1.83)	$\mathfrak{S}_3 \wr \mathfrak{S}_7 \wr \mathfrak{S}_2$
32	495452160	4		$(\mathfrak{S}_2 \wr (PSL(3,4) \rtimes \mathfrak{S}_3))/\mathfrak{S}_2^9$
33	116530348032	12	(3.138)$\wr\mathfrak{S}_3$	$((\mathfrak{S}_2 \wr PSL(3,2))/\mathfrak{S}_2^3) \wr \mathfrak{S}_3$
34	6831653917205672755200	4	(1.75)	$\mathfrak{S}_3 \wr \mathfrak{S}_{14}$
35	2958824445050880	4	(1.80)	$\mathfrak{S}_2 \wr \mathfrak{S}_3 \wr \mathfrak{S}_7$
36	2016	20	(3.115) $\mathfrak{S}_2\times$(1.116)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times PSL(3,2)))/\mathfrak{S}_2^{20}$ $\cong \mathfrak{S}_2 \times \mathfrak{S}_3 \times PSL(3,2)$
37	8257536	8	3.118	$\mathfrak{S}_2^{13} \rtimes (PSL(3,2) \times \mathfrak{S}_3)$
38	304819200	2	(3.85)	$(\mathfrak{S}_7 \wr \mathfrak{S}_2) \times \mathfrak{S}_3$
39	247726080	2	(3.100)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_7))/\mathfrak{S}_2^8$
40	523069747200	4	(1.72)	$\mathfrak{S}_3 \times \mathfrak{S}_{14}$
41	516096	12	(3.115) (3.104)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times PSL(3,2)))/\mathfrak{S}_2^{12}$ $\cong \mathfrak{S}_4 \times (\mathfrak{S}_2 \wr PSL(3,2))$
42	1828915200	6	(3.81)	$(\mathfrak{S}_3 \times \mathfrak{S}_7) \wr \mathfrak{S}_2$
43	1032192	4	(3.115)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times PSL(3,2)))/\mathfrak{S}_2^{11}$
44	46231631953920	2	(3.75)	$(\mathfrak{S}_2 \wr \mathfrak{S}_3 \wr \mathfrak{S}_7)/\mathfrak{S}_2^6$
45	33030144	8	3.118	$\mathfrak{S}_2^{15} \rtimes (PSL(3,2) \times \mathfrak{S}_3)$
46	3870720	2	(3.87) (3.86)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_7))/\mathfrak{S}_2^{14}$ $\cong (\mathfrak{S}_2 \wr \mathfrak{S}_7) \times \mathfrak{S}_3$
47	66060288	4	3.118	$\mathfrak{S}_2^{16} \rtimes (PSL(3,2) \times \mathfrak{S}_3)$
48	4128768	12	3.118	$\mathfrak{S}_2^{12} \rtimes (PSL(3,2) \times \mathfrak{S}_3)$
49	98627481501696	8	$\mathfrak{S}_2\wr$(1.114)	$\mathfrak{S}_2 \wr \mathfrak{S}_3 \wr PSL(3,2)$
50	16187813296865280	8	(1.113)	$PSL(3,2) \wr \mathfrak{S}_6$
51	1610915531194368000	4	(1.81)	$\mathfrak{S}_2 \wr \mathfrak{S}_7 \wr \mathfrak{S}_3$
52	29262643200	12	N21Gr7$\wr\mathfrak{S}_2$	$(PSL(3,4) \rtimes \mathfrak{S}_3) \wr \mathfrak{S}_2$
53	241920	2	(3.84) (3.83)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_7))/\mathfrak{S}_2^{18}$ $\cong (\mathfrak{S}_2 \wr \mathfrak{S}_3) \times \mathfrak{S}_7$
54	12328435187712	4	(3.78)	$(\mathfrak{S}_2 \wr \mathfrak{S}_3 \wr PSL(3,2))/\mathfrak{S}_2^3$
55	1541054398464	2/6	(3.77)	$(\mathfrak{S}_2 \wr \mathfrak{S}_3 \wr PSL(3,2))/\mathfrak{S}_2^6$
56	1618781329686528	4	(1.113)$\wr\mathfrak{S}_2$	$PSL(3,2) \wr \mathfrak{S}_3 \wr \mathfrak{S}_2$
57	402728882798592000	2	(3.76)	$(\mathfrak{S}_2 \wr \mathfrak{S}_7 \wr \mathfrak{S}_3)/\mathfrak{S}_2^2$
58	4877107200	2/6		$(PSL(3,4) \wr \mathfrak{S}_2) \rtimes \mathfrak{S}_3$
59	1079187553124352	2/6	(3.136)$\wr\mathfrak{S}_3$	$PSL(3,2) \wr \mathfrak{S}_2 \wr \mathfrak{S}_3$
60	10714547155728479551488000000	1/3	(1.19)	$\mathfrak{S}_2 \wr \mathfrak{S}_{21}$
	Anzahl Codes:	605	davon 9	selbstdual

Tabelle E.13: Tabelle der Automorphismengruppen für N=42, Teil 2 von 2

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	252675527208918344977248084798 99/ 64800000000	2	(1.18)	$\mathfrak{S}_{22} \wr \mathfrak{S}_2$
2	609304118736734046388224000000 00	4	(1.22)	$\mathfrak{S}_{11} \wr \mathfrak{S}_4$
3	60740641855649297203200	4	(1.23)	$\mathfrak{S}_4 \wr \mathfrak{S}_{11}$
4	342882701121945600	2	(1.20)	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_{11}$
5	1004539163443200	2	(1.28) (1.29)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_{11}))/\mathfrak{S}_2^{11}$ $\cong (\mathfrak{K}_4 \wr \mathfrak{S}_{11}) \rtimes \mathfrak{S}_3$
6	958003200	2	(1.24)	$\mathfrak{S}_4 \times \mathfrak{S}_{11}$
7	13365996293109841920000	2	(1.21)	$\mathfrak{S}_2 \wr \mathfrak{S}_{11} \wr \mathfrak{S}_2$
8	47144007485205310026547200 00	3	(1.19)	$\mathfrak{S}_2 \wr \mathfrak{S}_{22}$
	Anzahl Codes:	21		

Tabelle E.14: Tabelle der Automorphismengruppen für N=44

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	13416835151120242560510984192000000000	4	(1.74)	$\mathfrak{S}_{15} \wr \mathfrak{S}_3$
2	9478929289052160	16	(1.77)	$\mathfrak{S}_3 \wr PSL(4,2)$
3	75508598663747712162201 6000000	4	(1.92)	$\mathfrak{S}_9 \wr \mathfrak{S}_5$
4	6687075336192000000000	4	(1.90)	$\mathfrak{S}_5 \wr \mathfrak{S}_3 \wr \mathfrak{S}_3$
5	169266594447360	16	$\mathfrak{S}_3 \wr$ N15Gr4	$\mathfrak{S}_3 \wr (\mathfrak{Z}_3 \rtimes \mathfrak{S}_5)$
6	338533188894720	8	(1.95)	$\mathfrak{S}_3 \wr (\mathfrak{S}_3 \times \mathfrak{S}_5)$
7	1872381094133760000000000	4	(1.91)	$\mathfrak{S}_5 \wr \mathfrak{S}_9$
8	438739012807557120	4	(1.88)	$\mathfrak{S}_3 \wr \mathfrak{S}_3 \wr \mathfrak{S}_5$
9	155520	12	(1.94)	$(\mathfrak{S}_3 \wr \mathfrak{S}_3) \times \mathfrak{S}_5$
10	49161240576000	16	(1.76)	$PSL(4,2) \wr \mathfrak{S}_3$
11	4874877920083968000	4	(1.89)	$\mathfrak{S}_3 \wr \mathfrak{S}_5 \wr \mathfrak{S}_3$
12	43545600	4	(1.93)	$\mathfrak{S}_9 \times \mathfrak{S}_5$
13	614848852548510547968000	4	(1.75)	$\mathfrak{S}_3 \wr \mathfrak{S}_{15}$
14	19440	32		$(\mathfrak{Z}_3 \wr \mathfrak{S}_3) \rtimes \mathfrak{S}_5$
15	279936000	16	N15Gr4$\wr\mathfrak{S}_3$	$(\mathfrak{Z}_3 \rtimes \mathfrak{S}_5) \wr \mathfrak{S}_3$
16	2239488000	8	(1.96)	$(\mathfrak{S}_5 \times \mathfrak{S}_3) \wr \mathfrak{S}_3$
	Anzahl Codes:	156		

Tabelle E.15: Tabelle der Automorphismengruppen für N=45

Nr	Ordnung	Anz	Formeltyp	Produktformel
1	133665353893517804492964236858669137920000000 0	2	(1.18)	$\mathfrak{S}_{23} \wr \mathfrak{S}_2$
2	85571854663680	8	(3.135)	$\mathfrak{S}_2 \wr M23$
3	41783132160	4	(3.139)	$(\mathfrak{S}_2 \wr M23)/\mathfrak{S}_2^{11}$
4	208119169843200	2/6	(3.136)	$M23 \wr \mathfrak{S}_2$
5	216862434431944426122117120000	1/3	(1.19)	$\mathfrak{S}_2 \wr \mathfrak{S}_{23}$
	Anzahl Codes:	23	davon 3	selbstdual

Tabelle E.16: Tabelle der Automorphismengruppen für N=46

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	769912438426662553879474004305934 23/ 4419200000000	2	(1.18)	$\mathfrak{S}_{24} \wr \mathfrak{S}_2$
2	549553567789885135278529912504320 00000000	4	(1.74)	$\mathfrak{S}_{16} \wr \mathfrak{S}_3$
3	126345302061249171859062128640000 0000	4	(1.22)	$\mathfrak{S}_{12} \wr \mathfrak{S}_4$
4	309353929596332647907328000000	2	(1.85)	$\mathfrak{S}_8 \wr \mathfrak{S}_3 \wr \mathfrak{S}_2$
5	206235953064221765271552000000	2	(1.84)	$\mathfrak{S}_8 \wr \mathfrak{S}_2 \wr \mathfrak{S}_3$
6	277326388342554624000000000	2	(1.53)	$\mathfrak{S}_6 \wr \mathfrak{S}_2 \wr \mathfrak{S}_4$
7	309353929596332647907328000000 0	4	(1.52)	$\mathfrak{S}_8 \wr \mathfrak{S}_6$
8	831979165027663872000000000	2	(1.54)	$\mathfrak{S}_6 \wr \mathfrak{S}_4 \wr \mathfrak{S}_2$
9	16828576098534870220 80	2	(1.55)	$\mathfrak{S}_4 \wr \mathfrak{S}_2 \wr \mathfrak{S}_6$
10	291192707759682355200000000 0	4	(1.51)	$\mathfrak{S}_6 \wr \mathfrak{S}_8$
11	4058744094720	8	(3.80)	$\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_8)$
12	29119270775968235520	2	(1.82)	$\mathfrak{S}_3 \wr \mathfrak{S}_2 \wr \mathfrak{S}_8$
13	37864296221703457996800	2	(1.56)	$\mathfrak{S}_4 \wr \mathfrak{S}_6 \wr \mathfrak{S}_2$
14	247726080	4	(3.101) (3.102)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_8))/\mathfrak{S}_2^{14}$ $\cong \mathfrak{S}_4 \times (\mathfrak{S}_2 \wr \mathfrak{S}_8)$
15	17493304854426997594521600	4	(1.23)	$\mathfrak{S}_4 \wr \mathfrak{S}_{12}$
16	32916739307706777600	2	(1.20)	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_{12}$
17	71248353479884800	2	(1.49)	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_6 \wr \mathfrak{S}_2$
18	9172570294429994188800	2	(1.83)	$\mathfrak{S}_3 \wr \mathfrak{S}_8 \wr \mathfrak{S}_2$
19	59025489844657012604928000	4	(1.75)	$\mathfrak{S}_3 \wr \mathfrak{S}_{16}$
20	1136188586899537920	4	(1.80)	$\mathfrak{S}_2 \wr \mathfrak{S}_3 \wr \mathfrak{S}_8$
21	19508428800	2	(3.85)	$(\mathfrak{S}_8 \wr \mathfrak{S}_2) \times \mathfrak{S}_3$
22	125536739328000	4	(1.72)	$\mathfrak{S}_3 \times \mathfrak{S}_{16}$
23	3166593487994880	2	(1.50)	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_6$
24	2308446652748267520	4	(1.57)	$\mathfrak{S}_2 \wr \mathfrak{S}_4 \wr \mathfrak{S}_6$
25	117050572800	6	(3.81)	$(\mathfrak{S}_3 \times \mathfrak{S}_8) \wr \mathfrak{S}_2$
26	61931520	2	(3.87) (3.86)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_8))/\mathfrak{S}_2^{16}$ $\cong (\mathfrak{S}_2 \wr \mathfrak{S}_8) \times \mathfrak{S}_3$
27	108208436847575040000	4	(1.58)	$\mathfrak{S}_2 \wr \mathfrak{S}_6 \wr \mathfrak{S}_4$
28	6598310015772131328000	4	(1.81)	$\mathfrak{S}_2 \wr \mathfrak{S}_8 \wr \mathfrak{S}_3$
29	7698813864831268945920000	2	(1.21)	$\mathfrak{S}_2 \wr \mathfrak{S}_{12} \wr \mathfrak{S}_2$
30	1649577503943032832000	2	(3.76)	$(\mathfrak{S}_2 \wr \mathfrak{S}_8 \wr \mathfrak{S}_3)/\mathfrak{S}_2^2$
31	10409396852733332453861621760000	3	(1.19)	$\mathfrak{S}_2 \wr \mathfrak{S}_{24}$
	Anzahl Codes:	97		

Tabelle E.17: Tabelle der Automorphismengruppen für N=48

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	13877877090655792005120000000	8	(1.114)	$\mathfrak{S}_7 \wr PSL(3,2)$
2	41633631271967376015360000000	4	(1.110)	$\mathfrak{S}_7 \wr \mathfrak{S}_7$
3	19036868437113569280	8	(1.113)	$PSL(3,2) \wr \mathfrak{S}_7$
4	634562281237118976	8	(1.115)	$PSL(3,2) \wr PSL(3,2)$
	Anzahl Codes:	28		

Tabelle E.18: Tabelle der Automorphismengruppen für N=49

Anhang F

Tabellen der Automorphismengruppen für zyklische Codes, Teil 3 ($50 \leq N \leq 58$)

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	4811952740166640961746712526912088965/ 12000000000000	2	(1.18)	$\mathfrak{S}_{25} \wr \mathfrak{S}_2$
2	7550859866374771216220160000000000	4	(1.101)	$\mathfrak{S}_{10} \wr \mathfrak{S}_5$
3	2377626786201600000000000	2	(3.73)	$\mathfrak{S}_5 \wr \mathfrak{S}_2 \wr \mathfrak{S}_5$
4	1783220089651200000000000	2	(3.72)	$\mathfrak{S}_5 \wr \mathfrak{S}_5 \wr \mathfrak{S}_2$
5	2246857312960512000000000000	4	(1.102)	$\mathfrak{S}_5 \wr \mathfrak{S}_{10}$
6	100192997081088000000	4	(3.71)	$\mathfrak{S}_2 \wr \mathfrak{S}_5 \wr \mathfrak{S}_5$
7	6262062317568000000	2	(3.75)	$(\mathfrak{S}_2 \wr \mathfrak{S}_5 \wr \mathfrak{S}_5)/\mathfrak{S}_2^4$
8	52046984263666662269308108800000 0	3	(1.19)	$\mathfrak{S}_2 \wr \mathfrak{S}_{25}$
	Anzahl Codes:	23		

Tabelle F.1: Tabelle der Automorphismengruppen für N=50

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	269995667855170566962341746013 3/ 72416000000000	4	(1.74)	$\mathfrak{S}_{17} \wr \mathfrak{S}_3$
2	48960	64		$PSL(2,16) \rtimes \mathfrak{Q}_3$
3	60205999641550152857026560000	4	(1.75)	$\mathfrak{S}_3 \wr \mathfrak{S}_{17}$
4	2134124568576000	4	(1.72)	$\mathfrak{S}_3 \times \mathfrak{S}_{17}$
	Anzahl Codes:	76		

Tabelle F.2: Tabelle der Automorphismengruppen für N=51;
$\mathfrak{Q}_3 \cong t12n5 \cong \mathfrak{S}_2 \rtimes \mathfrak{S}_3 \cong \mathfrak{Z}_3 \rtimes \mathfrak{Z}_4$, Quaternionengruppe; in mancher Literatur auch „T“ genannt

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	3252880052352649290140777668192 5/ 7214042112000000000000	2	(1.18)	$\mathfrak{S}_{26} \wr \mathfrak{S}_2$
2	3608548172171337597466673456 08/ 70400000000	4	(1.22)	$\mathfrak{S}_{13} \wr \mathfrak{S}_4$
3	5457911114581223249490739200	4	(1.23)	$\mathfrak{S}_4 \wr \mathfrak{S}_{13}$
4	3423340888001504870400	2	(1.20)	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_{13}$
5	2507329751954227200	2	(1.28) (1.29)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_{13}))/\mathfrak{S}_2^{13}$ $\cong (\mathfrak{K}_4 \wr \mathfrak{S}_{13}) \rtimes \mathfrak{S}_3$
6	149448499200	2	(1.24)	$\mathfrak{S}_{13} \times \mathfrak{S}_4$
7	52043981726259378074419200 00	2	(1.21)	$\mathfrak{S}_2 \wr \mathfrak{S}_{13} \wr \mathfrak{S}_2$
8	27064431817106664380040216576000000	3	(1.19)	$\mathfrak{S}_2 \wr \mathfrak{S}_{26}$
	Anzahl Codes:	21		

Tabelle F.3: Tabelle der Automorphismengruppen für N=52

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	237134955816508133251262692011238509 0/ 36699648000000000000	2	(1.18)	$\mathfrak{S}_{27} \wr \mathfrak{S}_2$
2	157461473493135474652437706274998/ 7930112000000000	4	(1.74)	$\mathfrak{S}_{18} \wr \mathfrak{S}_3$
3	164403361698604618736518299648000000	2	(1.85)	$\mathfrak{S}_9 \wr \mathfrak{S}_3 \wr \mathfrak{S}_2$
4	109602241132403079157678866432000000	2	(1.84)	$\mathfrak{S}_9 \wr \mathfrak{S}_2 \wr \mathfrak{S}_3$
5	1644033616986046187365182996480000000	4	(1.92)	$\mathfrak{S}_9 \wr \mathfrak{S}_6$
6	673903123672407736320000000000	4	(1.90)	$\mathfrak{S}_6 \wr \mathfrak{S}_3 \wr \mathfrak{S}_3$
7	188692874628274166169600000000000	4	(1.91)	$\mathfrak{S}_6 \wr \mathfrak{S}_9$
8	18869287462827416616960	2	(1.82)	$\mathfrak{S}_3 \wr \mathfrak{S}_2 \wr \mathfrak{S}_9$
9	3411634563591564165120	4	(1.88)	$\mathfrak{S}_3 \wr \mathfrak{S}_3 \wr \mathfrak{S}_6$
10	227442304239437611008000	4	(1.89)	$\mathfrak{S}_3 \wr \mathfrak{S}_6 \wr \mathfrak{S}_3$
11	26747214978557863054540800	2	(1.83)	$\mathfrak{S}_3 \wr \mathfrak{S}_9 \wr \mathfrak{S}_2$
12	650224796128741650855886848000	4	(1.75)	$\mathfrak{S}_3 \wr \mathfrak{S}_{18}$
13	490833469540600381440	4	(1.80)	$\mathfrak{S}_2 \wr \mathfrak{S}_3 \wr \mathfrak{S}_9$
14	1917318240392970240	2	(3.75)	$(\mathfrak{S}_2 \wr \mathfrak{S}_3 \wr \mathfrak{S}_9)/\mathfrak{S}_2^8$
15	3848134401198306990489600 0	4	(1.81)	$\mathfrak{S}_2 \wr \mathfrak{S}_9 \wr \mathfrak{S}_3$
16	9620336002995767476224000	2	(3.76)	$(\mathfrak{S}_2 \wr \mathfrak{S}_9 \wr \mathfrak{S}_3)/\mathfrak{S}_2^2$
17	14614793181237598765221716951040000 00	3	(1.19)	$\mathfrak{S}_2 \wr \mathfrak{S}_{27}$
	Anzahl Codes:	53		

Tabelle F.4: Tabelle der Automorphismengruppen für N=54

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	12160735323395232791434729881600000000000	4	(1.101)	$\mathfrak{S}_{11} \wr \mathfrak{S}_5$
2	29658516531078758400000000000000	4	(1.102)	$\mathfrak{S}_5 \wr \mathfrak{S}_{11}$
3	4790016000	4	(1.105)	$\mathfrak{S}_{11} \times \mathfrak{S}_5$
	Anzahl Codes:	12		

Tabelle F.5: Tabelle der Automorphismengruppen für N=55

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	185913805360142376468989950536810/ 991084772524032000000000000	2	(1.18)	$\mathfrak{S}_{28} \wr \mathfrak{S}_2$
2	291040176964229755151214184240000000	8	(1.114)	$\mathfrak{S}_8 \wr PSL(3,2)$
3	13862598658213410514427972748903 9/ 7286400000000	4	(1.22)	$\mathfrak{S}_{14} \wr \mathfrak{S}_4$
4	56544015691077163941888	8	$\mathfrak{S}_4 \wr$(3.138)	$\mathfrak{S}_4 \wr ((\mathfrak{S}_2 \wr PSL(3,2))/\mathfrak{S}_2^3)$
5	15987314408435472389898240000000 0	2	(1.53)	$\mathfrak{S}_7 \wr \mathfrak{S}_2 \wr \mathfrak{S}_4$
6	1187424329512620442779648	12	$\mathfrak{S}_4 \wr$(3.136)	$\mathfrak{S}_4 \wr PSL(3,2) \wr \mathfrak{S}_2$
7	69269232549888	16	$\mathfrak{S}_2 \wr$(1.46)	$\mathfrak{S}_2 \wr ((\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times PSL(3,2)))/\mathfrak{S}_2^{13})$
			$\mathfrak{S}_2 \wr$(1.48)	$\mathfrak{S}_2 \wr ((\mathfrak{K}_4 \wr PSL(3,2))/\mathfrak{K}_4^3) \rtimes \mathfrak{S}_3)$
8	47961943225306417169694720000000 0	2	(1.54)	$\mathfrak{S}_7 \wr \mathfrak{S}_4 \wr \mathfrak{S}_2$
9	87312053089268926545364254720000000 0	4	(1.52)	$\mathfrak{S}_8 \wr \mathfrak{S}_7$
10	1082331758592	40	(3.109)	$\mathfrak{S}_2 \wr (\mathfrak{S}_4 \times PSL(3,2))$
11	16786680128857246009393152000000000 0	4	(1.51)	$\mathfrak{S}_7 \wr \mathfrak{S}_8$
12	516096	24	(3.115)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_4 \times PSL(3,2)))/\mathfrak{S}_2^{21}$
13	13570563765858519346053120	2	(1.55)	$\mathfrak{S}_4 \wr \mathfrak{S}_2 \wr \mathfrak{S}_7$
14	193536	48	(3.111)	$(\mathfrak{S}_4 \wr \mathfrak{S}_2) \times PSL(3,2)$
15	132996926495784960	4	$\mathfrak{S}_2 \wr$(1.28)	$\mathfrak{S}_2 \wr ((\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_7))/\mathfrak{S}_2^7)$
			$\mathfrak{S}_2 \wr$(1.29)	$\cong \mathfrak{S}_2 \wr ((\mathfrak{K}_4 \wr \mathfrak{S}_7) \rtimes \mathfrak{S}_3)$
16	3879077022793728	24	(1.42)$\wr \mathfrak{S}_2$	$(\mathfrak{S}_2 \wr ((\mathfrak{S}_2 \wr PSL(3,2))/\mathfrak{S}_2^3)) \wr \mathfrak{S}_2$
17	6773760	32	(1.116)	$PSL(3,2) \times \mathfrak{S}_8$
18	452352125528617311535104	8	$\mathfrak{S}_4 \wr$(3.135)	$\mathfrak{S}_4 \wr \mathfrak{S}_2 \wr PSL(3,2)$
19	32469952757760	4	(3.80)	$\mathfrak{S}_2 \wr (\mathfrak{S}_4 \times \mathfrak{S}_7)$
20	123863040	4	(3.101)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_4 \times \mathfrak{S}_7))/\mathfrak{S}_2^{18}$
21	360777252864	32	$\mathfrak{S}_2 \wr$(1.39)	$\mathfrak{S}_2 \wr (PSL(3,2) \times (\mathfrak{S}_2 \wr \mathfrak{S}_2))$
22	14797504512	12	(1.41) $\wr \mathfrak{S}_2$	$((\mathfrak{S}_2 \wr (\mathfrak{S}_2 \times PSL(3,2)))/\mathfrak{S}_2^6) \wr \mathfrak{S}_2$
23	5132018901156102144	16	(3.135)$\wr \mathfrak{S}_4$	$\mathfrak{S}_2 \wr PSL(3,2) \wr \mathfrak{S}_4$
24	133177540608	12	(1.46)$\wr \mathfrak{S}_2$	$((\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times PSL(3,2)))/\mathfrak{S}_2^{13}) \wr \mathfrak{S}_2$
			(1.48)$\wr \mathfrak{S}_2$	$((\mathfrak{K}_4 \wr PSL(3,2))/\mathfrak{K}_4^3) \rtimes \mathfrak{S}_3) \wr \mathfrak{S}_2$
25	11821949021847552	8		$(\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_2 \wr PSL(3,2))/\mathfrak{S}_2^3$
26	10686818965613583985016832000	2	(1.56)	$\mathfrak{S}_4 \wr \mathfrak{S}_7 \wr \mathfrak{S}_2$
27	5806080	2	(3.82)	$(\mathfrak{S}_4 \wr \mathfrak{S}_2) \times \mathfrak{S}_7$

Tabelle F.6: Tabelle der Automorphismengruppen für N=56, Teil 1 von 3

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
28	4433230883192832	8	$\mathfrak{S}_2 \wr (1.30)$ $\mathfrak{S}_2 \wr (1.31)$	$\mathfrak{S}_2 \wr ((\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times PSL(3,2)))/\mathfrak{S}_2^7)$ $\cong \mathfrak{S}_2 \wr (\mathfrak{K}_4 \wr PSL(3,2)) \rtimes \mathfrak{S}_3)$
29	23089744183296	12	$\mathfrak{S}_2 \wr (1.41)$	$\mathfrak{S}_2 \wr ((\mathfrak{S}_2 \wr (\mathfrak{S}_2 \times PSL(3,2)))/\mathfrak{S}_2^6)$
30	203212800	4	(1.59)	$\mathfrak{S}_7 \times \mathfrak{S}_8$
31	32514048	32	(3.108)	$(\mathfrak{S}_4 \times PSL(3,2)) \wr \mathfrak{S}_2$
32	1833858134499291011828888371200	4	(1.23)	$\mathfrak{S}_4 \wr \mathfrak{S}_{14}$
33	33030144	8	(3.115)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_4 \times PSL(3,2)))/\mathfrak{S}_2^{15}$
34	1710672967052034048	4	$(1.34) \wr \mathfrak{S}_2$	$\mathfrak{S}_2 \wr PSL(3,2) \wr \mathfrak{S}_2 \wr \mathfrak{S}_2$
35	704643072	8	(3.116)	$(\mathfrak{S}_2 \wr (PSL(3,2) \times (\mathfrak{S}_2 \wr \mathfrak{S}_2)))/\mathfrak{S}_2^9$
36	1477743627730944	4	(3.120)	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr (\mathfrak{S}_2 \times PSL(3,2))$
37	1376256	8	(3.116)	$(\mathfrak{S}_2 \wr (PSL(3,2) \times (\mathfrak{S}_2 \wr \mathfrak{S}_2)))/\mathfrak{S}_2^{18}$
38	64512	2/54	(3.115) (3.109)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_4 \times PSL(3,2)))/\mathfrak{S}_2^{24}$ $\cong (\mathfrak{S}_2 \wr \mathfrak{S}_4) \times PSL(3,2)$
39	792723456	4		$((\mathfrak{S}_2^6 \rtimes \mathfrak{S}_4) \wr \mathfrak{S}_2) \rtimes PSL(3,2)$
40	383414179456168545484800	2	(1.20)	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_{14}$
41	2234348365129187328 00	2	(1.49)	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_7 \wr \mathfrak{S}_2$
42	16911433728	8	(3.115)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_4 \times PSL(3,2)))/\mathfrak{S}_2^6$
43	21504	24	(3.122) (3.116)	$(\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_2) \times PSL(3,2) \cong$ $(\mathfrak{S}_2 \wr (PSL(3,2) \times (\mathfrak{S}_2 \wr \mathfrak{S}_2)))/\mathfrak{S}_2^{24}$
44	94575592174780416	8	$\mathfrak{S}_2 \wr (1.33)$	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_2 \wr PSL(3,2)$
45	1252934302040064	12	$(3.138) \wr \mathfrak{S}_4$	$((\mathfrak{S}_2 \wr PSL(3,2))/\mathfrak{S}_2^3) \wr \mathfrak{S}_4$
46	54549520633036800	2		$\mathfrak{S}_2 \wr (\mathfrak{S}_2 \times \mathfrak{S}_7) \wr \mathfrak{S}_2$
47	490945685697331200	2	$(1.28) \wr \mathfrak{S}_2$ $(1.29) \wr \mathfrak{S}_2$	$((\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_7))/\mathfrak{S}_2^7) \wr \mathfrak{S}_2$ $\cong ((\mathfrak{K}_4 \wr \mathfrak{S}_7) \rtimes \mathfrak{S}_3) \wr \mathfrak{S}_2$
48	417644767346688	4	$(1.43) \wr \mathfrak{S}_2$	$((\mathfrak{S}_2 \wr PSL(3,2))/\mathfrak{S}_2^3) \wr \mathfrak{S}_2 \wr \mathfrak{S}_2$
49	11010048	8	(3.116)	$(\mathfrak{S}_2 \wr (PSL(3,2) \times (\mathfrak{S}_2 \wr \mathfrak{S}_2)))/\mathfrak{S}_2^{15}$
50	4128768	16	(3.115)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_4 \times PSL(3,2)))/\mathfrak{S}_2^{18}$
51	11821949021847552	8	$\mathfrak{S}_2 \wr (1.42)$	$\mathfrak{S}_2 \wr (\mathfrak{S}_2 \wr ((\mathfrak{S}_2 \wr PSL(3,2))/\mathfrak{S}_2^3))$
52	29262643200	4	(3.81)	$(\mathfrak{S}_4 \times \mathfrak{S}_7) \wr \mathfrak{S}_2$
53	248260929458798592	12	$(1.33) \wr \mathfrak{S}_2$	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr PSL(3,2) \wr \mathfrak{S}_2$
54	23089744183296	8		$(\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr (\mathfrak{S}_2 \times PSL(3,2)))/\mathfrak{S}_2^6$
55	2113929216	8	(3.115)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_4 \times PSL(3,2)))/\mathfrak{S}_2^9$
56	1376256	4	(3.116)	$(\mathfrak{S}_2 \wr (PSL(3,2) \times (\mathfrak{S}_2 \wr \mathfrak{S}_2)))/\mathfrak{S}_2^{18}$
57	2837267765243412480	2	(1.50)	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_7$
58	6205104602587343093760	4	(1.57)	$\mathfrak{S}_2 \wr \mathfrak{S}_4 \wr \mathfrak{S}_7$

Tabelle F.7: Tabelle der Automorphismengruppen für N=56, Teil 2 von 3

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
59	88080384	8	(3.116)	$(\mathfrak{S}_2 \wr (PSL(3,2) \times (\mathfrak{S}_2 \wr \mathfrak{S}_2)))/\mathfrak{S}_2^{12}$
60	3612672	12	(3.119)	$((\mathfrak{S}_2 \wr \mathfrak{S}_2) \times (PSL(3,2)) \wr \mathfrak{S}_2$
61	264241152	12	(3.115)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_4 \times PSL(3,2)))/\mathfrak{S}_2^{12}$
62	172032	8	(3.116)	$(\mathfrak{S}_2 \wr (PSL(3,2) \times (\mathfrak{S}_2 \wr \mathfrak{S}_2)))/\mathfrak{S}_2^{21}$
63	96954759415427235840	2	(3.75)	$(\mathfrak{S}_2 \wr \mathfrak{S}_4 \wr \mathfrak{S}_7)/\mathfrak{S}_2^6$
64	25585551179480637112320	8	(1.113)	$PSL(3,2) \wr \mathfrak{S}_8$
65	41569353099364427366400000	4	(1.58)	$\mathfrak{S}_2 \wr \mathfrak{S}_7 \wr \mathfrak{S}_4$
66	206836820086244769792	8	$\mathfrak{S}_2 \wr$(1.36)	$\mathfrak{S}_2 \wr \mathfrak{S}_4 \wr PSL(3,2)$
67	10823317585920	2	(1.66)	$\mathfrak{S}_2 \wr (\mathfrak{S}_7 \times (\mathfrak{S}_2 \wr \mathfrak{S}_2))$
68	545495206330368	4	(1.30)$\wr\mathfrak{S}_2$	$((\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times PSL(3,2)))/\mathfrak{S}_2^7) \wr \mathfrak{S}_2$
69	25854602510780596224	4	(3.78)	$(\mathfrak{S}_2 \wr \mathfrak{S}_4 \wr PSL(3,2))/\mathfrak{S}_2^3$
70	731015747985161060352	4	(1.35)$\wr\mathfrak{S}_2$	$PSL(3,2) \wr \mathfrak{S}_4 \wr \mathfrak{S}_2$
71	408024816733873/ 5241034465280000	2	(1.21)	$\mathfrak{S}_2 \wr \mathfrak{S}_{14} \wr \mathfrak{S}_2$
72	1935360	2	(3.84) (3.83)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_4 \times \mathfrak{S}_7))/\mathfrak{S}_2^{24}$ $\cong (\mathfrak{S}_2 \wr \mathfrak{S}_4) \times \mathfrak{S}_7$
73	3231825313847574528	2/6	(3.77)	$(\mathfrak{S}_2 \wr \mathfrak{S}_4 \wr PSL(3,2))/\mathfrak{S}_2^6$
74	60610578481152	2/6	(3.121)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_2 \times PSL(3,2))) \wr \mathfrak{S}_2$
75	243671915995053686784	2/6	(3.136)$\wr\mathfrak{S}_4$	$PSL(3,2) \wr \mathfrak{S}_2 \wr \mathfrak{S}_4$
76	8184284181493055308/ 5241614925824000000	1/3	(1.19)	$\mathfrak{S}_2 \wr \mathfrak{S}_{28}$
	Anzahl Codes:	725	davon 9	selbstdual

Tabelle F.8: Tabelle der Automorphismengruppen für N=56, Teil 3 von 3

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	10800282466894162206410702273402167212638/ 208000000000	4	(1.74)	$\mathfrak{S}_{19} \wr \mathfrak{S}_3$
2	741256267586765481975711006720000	4	(1.75)	$\mathfrak{S}_3 \wr \mathfrak{S}_{19}$
3	729870602452992000	4	(1.72)	$\mathfrak{S}_{19} \times \mathfrak{S}_3$
	Anzahl Codes:	12		

Tabelle F.9: Tabelle der Automorphismengruppen für N=57

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	1563535103078797386104205484014/ 58043502293692710912000000000000	2	(1.18)	$\mathfrak{S}_{29} \wr \mathfrak{S}_2$
2	4746884825265972078944013665697792000000	3	(1.19)	$\mathfrak{S}_2 \wr \mathfrak{S}_{29}$
	Anzahl Codes:	5		

Tabelle F.10: Tabelle der Automorphismengruppen für N=58

Anhang G

Tabellen der Automorphismengruppen für zyklische Codes, Teil 4 ($60 \leq N \leq 69$)

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	14071815927709176474937849356/ 131223915206432343982080 0$*10^{12}$	2	(1.18)	$\mathfrak{S}_{30} \wr \mathfrak{S}_2$
2	864022597351532976512856 1818/ 7217337701105664$*10^{12}$	4	(1.74)	$\mathfrak{S}_{20} \wr \mathfrak{S}_3$
3	7017940570720539072 92/ 91612041326362624$*10^{12}$	4	(1.22)	$\mathfrak{S}_{15} \wr \mathfrak{S}_4$
4	10177922824393889509539840	16	(2.2)	$\mathfrak{S}_4 \wr PSL(4,2)$
5	16440336169860461873651829964 8$*10^{12}$	2	(1.85)	$\mathfrak{S}_{10} \wr \mathfrak{S}_3 \wr \mathfrak{S}_2$
6	10960224113240307915767886643 2$*10^{12}$	2	(1.84)	$\mathfrak{S}_{10} \wr \mathfrak{S}_2 \wr \mathfrak{S}_3$
7	302598009199108256 59/ 582867058982912$*10^{11}$	4	(1.101)	$\mathfrak{S}_{12} \wr \mathfrak{S}_5$
8	20542695432781824000000000000	4		$(\mathfrak{S}_5 \wr \mathfrak{K}_4 \wr \mathfrak{S}_3) \rtimes \mathfrak{S}_3$
9	16440336169860461873651829964 8$*10^{12}$	4	(1.79)	$\mathfrak{S}_{10} \wr \mathfrak{S}_6$
10	181748621864176598384640	16	$\mathfrak{S}_4 \wr$ N15Gr4	$\mathfrak{S}_4 \wr (\mathfrak{Z}_3 \rtimes \mathfrak{S}_5)$
11	363497243728353196769280	8	(3.88)	$\mathfrak{S}_4 \wr (\mathfrak{S}_3 \times \mathfrak{S}_5)$
12	692692325498880	2/30	$\mathfrak{S}_2 \wr$(10.6)	$\mathfrak{S}_2 \wr ((\mathfrak{S}_2 \wr PSL(4,2))/\mathfrak{S}_2^{10})$
13	14376599971678031708160000000000 0	2	(3.62)	$\mathfrak{S}_6 \wr \mathfrak{S}_2 \wr \mathfrak{S}_5$
14	12839184645488640000000000000	4	(3.94)	$\mathfrak{S}_5 \wr (\mathfrak{S}_3 \times \mathfrak{S}_4)$
15	123863040	24		$((\mathfrak{S}_2 \wr PSL(4,2))/\mathfrak{S}_2^5) \rtimes \mathfrak{S}_3$
16	2695612494689630945280	4	$\mathfrak{S}_3 \wr$(1.28)	$\mathfrak{S}_3 \wr ((\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_5))/\mathfrak{S}_2^5)$
17	41085390865563648000000000000 0	2	(3.59)	$\mathfrak{S}_5 \wr \mathfrak{S}_2 \wr \mathfrak{S}_6$
18	872792330128588800	24	(3.135)$\wr \mathfrak{S}_2$	$\mathfrak{S}_2 \wr PSL(4,2) \wr \mathfrak{S}_2$
19	27732638834255462400000000000 0	4	(3.62)	$\mathfrak{S}_5 \wr \mathfrak{S}_3 \wr \mathfrak{S}_4$
20	483840	56	(1.26)	$PSL(4,2) \times \mathfrak{S}_4$
21	98956046499840	12	$\mathfrak{S}_2 \wr$ (3.102)	$\mathfrak{S}_2 \wr (\mathfrak{S}_4 \times (\mathfrak{S}_2 \wr \mathfrak{S}_5))$
22	41085390865563648000000000000 0	2	(3.124)	$\mathfrak{S}_5 \wr \mathfrak{S}_2 \wr \mathfrak{S}_3 \wr \mathfrak{S}_2$
23	10782449978758523781120000000000 00	2	(3.61)	$\mathfrak{S}_6 \wr \mathfrak{S}_5 \wr \mathfrak{S}_2$
24	49478023249920	12	$\mathfrak{S}_2 \wr$N30Gr15	$\mathfrak{S}_2 \wr (\mathfrak{S}_2^7 \rtimes (\mathfrak{Z}_3 \rtimes \mathfrak{S}_5)$
25	9277129359360	4	$\mathfrak{S}_2 \wr$(3.82)	$\mathfrak{S}_2 \wr ((\mathfrak{S}_3 \wr \mathfrak{S}_2) \times \mathfrak{S}_5)$
26	27390260577042432000000000000	2	(3.125)	$\mathfrak{S}_5 \wr \mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_3$
27	10529736307381370880	4	(3.88)	$\mathfrak{S}_3 \wr (\mathfrak{S}_4 \times \mathfrak{S}_5)$
28	73953703558014566400000000000 0	4	(3.61)	$\mathfrak{S}_5 \wr \mathfrak{S}_4 \wr \mathfrak{S}_3$
29	35389440	8		$\mathfrak{S}_2^{12} \rtimes (\mathfrak{S}_4 \times (\mathfrak{Z}_3 \rtimes \mathfrak{S}_5))$
30	92771293593600	8	(3.80)	$\mathfrak{S}_2 \wr (\mathfrak{S}_5 \times \mathfrak{S}_6)$

Tabelle G.1: Tabelle der Automorphismengruppen für N=60, Teil 1 von 7

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
31	70778880	8		$(\mathfrak{S}_2 \wr ((\mathfrak{S}_3 \wr \mathfrak{S}_2) \times \mathfrak{S}_5))/\mathfrak{S}_2^{17}$
32	$135858869732357399642112{*}10^{12}$	4	(1.78)	$\mathfrak{S}_6 \wr \mathfrak{S}_{10}$
33	47109242787194574301298688O	4	(3.59)	$\mathfrak{S}_4 \wr \mathfrak{S}_3 \wr \mathfrak{S}_5$
34	8640	208	$\mathfrak{S}_4\times$ N15Gr4	$\mathfrak{S}_4 \times (\mathfrak{Z}_3 \rtimes \mathfrak{S}_5)$
35	17280	40		$\mathfrak{S}_3 \times \mathfrak{S}_4 \times \mathfrak{S}_5$
36	197912092999680	12	$\mathfrak{S}_2\wr$N30Gr20	$\mathfrak{S}_2 \wr ((\mathfrak{S}_2 \wr (\mathfrak{Z}_3 \rtimes \mathfrak{S}_5))/\mathfrak{S}_2^6)$
37	$9244212944751820800{*}10^{12}$	2	(3.60)	$\mathfrak{S}_5 \wr \mathfrak{S}_6 \wr \mathfrak{S}_2$
38	185542587187200	4	$\mathfrak{S}_2\wr$ (3.85)	$\mathfrak{S}_2 \wr ((\mathfrak{S}_5 \wr \mathfrak{S}_2) \times \mathfrak{S}_3)$
39	46385646796800	24	$\mathfrak{S}_2\wr$N30Gr22	$\mathfrak{S}_2 \wr (\mathfrak{A}_5 \wr \mathfrak{S}_2) \rtimes \mathfrak{S}_3)$
40	395824185999360	6	$\mathfrak{S}_2\wr$ (3.100)	$\mathfrak{S}_2 \wr ((\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_5))/\mathfrak{S}_2^6)$
41	88473600	4	(3.101)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_5 \times \mathfrak{S}_6))/\mathfrak{S}_2^{20}$
42	1132462080	4		$\mathfrak{S}_2^{16} \rtimes (\mathfrak{S}_3 \times \mathfrak{S}_4 \times \mathfrak{S}_5)$
43	566231040	8		$\mathfrak{S}_2^{16} \rtimes (\mathfrak{S}_4 \times (\mathfrak{Z}_3 \rtimes \mathfrak{S}_5))$
44	23378365985587200	8	(3.80)	$\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_{10})$
45	13585886973235739964211200	2	(3.59)	$\mathfrak{S}_3 \wr \mathfrak{S}_2 \wr \mathfrak{S}_{10}$
46	832359628800	2/18	(10.6)$\wr\mathfrak{S}_2$	$((\mathfrak{S}_2 \wr PSL(4,2))/\mathfrak{S}_2^{10}) \wr \mathfrak{S}_2$
47	276480	8		$\mathfrak{S}_5 \times ((\mathfrak{K}_4 \wr \mathfrak{S}_3) \rtimes \mathfrak{S}_3)$
48	$427082638047534120960{*}10^{12}$	4	(1.102)	$\mathfrak{S}_5 \wr \mathfrak{S}_{12}$
49	278313880780800	24		$(\mathfrak{S}_2 \wr (\mathfrak{Z}_3 \rtimes \mathfrak{S}_5)) \wr \mathfrak{S}_2$
50	1113255523123200	12	(3.80)$\wr\mathfrak{S}_2$	$\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_5) \wr \mathfrak{S}_2$
51	44332308831928320	12	$\mathfrak{S}_2\wr$(3.140)	$\mathfrak{S}_2 \wr ((\mathfrak{S}_2 \wr PSL(4,2))/\mathfrak{S}_2^4)$
52	52343603096882860334776320O0	4	(3.60)	$\mathfrak{S}_4 \wr \mathfrak{S}_5 \wr \mathfrak{S}_3$
53	107824499787585237811200	2	(3.126)	$\mathfrak{S}_3 \wr \mathfrak{S}_2 \wr \mathfrak{S}_5 \wr \mathfrak{S}_2$
54	2051952580220682240	4	$\mathfrak{S}_2\wr$(3.75)	$\mathfrak{S}_2 \wr ((\mathfrak{S}_2 \wr \mathfrak{S}_3 \wr \mathfrak{S}_5)/\mathfrak{S}_2^4)$
55	773094113280	52	$\mathfrak{S}_2\wr$(N15Gr4$\times\mathfrak{S}_2$)	$\mathfrak{S}_2 \wr ((\mathfrak{Z}_3 \rtimes \mathfrak{S}_5) \times \mathfrak{S}_2)$
56	368640	6		$(\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_3) \times \mathfrak{S}_5$
57	552960	2		$(\mathfrak{S}_2 \wr \mathfrak{S}_3 \wr \mathfrak{S}_2) \times \mathfrak{S}_5$
58	2319282339840	24	$\mathfrak{S}_2\wr$ N30Gr31	$\mathfrak{S}_2 \wr ((\mathfrak{Z}_3 \wr \mathfrak{Z}_2) \rtimes \mathfrak{S}_5)$
59	24739011624960	10	$\mathfrak{S}_2\wr$ (3.86)	$\mathfrak{S}_2 \wr ((\mathfrak{S}_2 \wr \mathfrak{S}_5) \times \mathfrak{S}_3)$
60	3732480	12	(3.96)	$(\mathfrak{S}_3 \wr \mathfrak{S}_4) \times \mathfrak{S}_5$
61	12369505812480	48	$\mathfrak{S}_2\wr$ N30Gr33	$\mathfrak{S}_2 \wr (\mathfrak{Z}_3 \rtimes (\mathfrak{S}_2 \wr \mathfrak{S}_5))$
62	89181388800	4	(3.101) (3.102)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_{10}))/\mathfrak{S}_2^{18}$ $\cong \mathfrak{S}_4 \times (\mathfrak{S}_2 \wr \mathfrak{S}_{10})$

Tabelle G.2: Tabelle der Automorphismengruppen für N=60, Teil 2 von 7

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
63	176947200	4		$(\mathfrak{S}_2^{12} \rtimes (\mathfrak{A}_5 \wr \mathfrak{S}_2)) \rtimes \mathfrak{Z}_6$
64	507343011840	8		$\mathfrak{S}_2^{20} \rtimes (\mathfrak{S}_4 \times PSL(4,2))$
65	9953280	12	(3.91)	$\mathfrak{S}_5 \times (\mathfrak{S}_4 \wr \mathfrak{S}_3)$
66	23482733690880	4		$((\mathfrak{K}_4 \rtimes \mathfrak{S}_4) \wr \mathfrak{S}_5) \rtimes \mathfrak{S}_4$
67	22394880	6	(3.98)	$\mathfrak{S}_4 \times (\mathfrak{S}_3 \wr \mathfrak{S}_5)$
68	4423680	8	$\mathfrak{S}_3 \times$(1.28)	$\mathfrak{S}_3 \times ((\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_5))/\mathfrak{S}_2^5)$
69	91197892454252544000	4	$\mathfrak{S}_2 \wr$N30Gr34	$\mathfrak{S}_2 \wr (\mathfrak{S}_2 \wr \mathfrak{S}_5 \wr \mathfrak{S}_3)/\mathfrak{S}_2^2)$
70	161280	12	(1.39)	$(\mathfrak{S}_2 \wr \mathfrak{S}_2) \times PSL(4,2)$
71	124416000	2	(3.85)	$\mathfrak{S}_5 \times (\mathfrak{S}_6 \wr \mathfrak{S}_2)$
72	44236800	4		$((\mathfrak{S}_2^5 \rtimes \mathfrak{A}_5) \wr \mathfrak{S}_2) \rtimes \mathfrak{S}_3$
73	176947200	2		$\mathfrak{S}_3 \times (\mathfrak{S}_2 \wr \mathfrak{S}_5 \wr \mathfrak{S}_2)$
74	6184752906240	10	$\mathfrak{S}_2 \wr$(3.83)	$\mathfrak{S}_2 \wr ((\mathfrak{S}_2 \wr \mathfrak{S}_3) \times \mathfrak{S}_5)$
75	691200	2		$((\mathfrak{S}_2 \times \mathfrak{S}_5) \wr \mathfrak{S}_2) \times \mathfrak{S}_3$
76	14376599971678031708160	2	(3.127)	$\mathfrak{S}_3 \wr \mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_5$
77	660188928419744764258399813632000	4	(1.23)	$\mathfrak{S}_4 \wr \mathfrak{S}_{15}$
78	34935137931177617050828800	4	(3.57)	$\mathfrak{S}_3 \wr \mathfrak{S}_4 \wr \mathfrak{S}_5$
79	35389440	4		$((\mathfrak{S}_2 \times (\mathfrak{K}_4 \rtimes t6n4)) \wr \mathfrak{S}_2) \rtimes (\mathfrak{S}_2 \wr \mathfrak{S}_5)/\mathfrak{S}_2$
80	2764800	2	Formeltyp	$\mathfrak{S}_4 \times ((\mathfrak{S}_2 \times \mathfrak{S}_5) \wr \mathfrak{S}_2)$
81	188743680	8		$(\mathfrak{S}_2 \wr ((\mathfrak{S}_2 \wr \mathfrak{S}_3) \times \mathfrak{S}_5))/\mathfrak{S}_2^{15}$
82	57480192000	4	(1.105)	$\mathfrak{S}_5 \times \mathfrak{S}_{12}$
83	94371840	4		$(\mathfrak{S}_2 \wr ((\mathfrak{S}_2 \wr \mathfrak{S}_3) \times \mathfrak{S}_5))/\mathfrak{S}_2^{16}$
84	4246732800	8	N30Gr15 $\wr \mathfrak{S}_2$	$(\mathfrak{S}_2^7 \rtimes (\mathfrak{Z}_3 \rtimes \mathfrak{S}_5)) \wr \mathfrak{S}_2$
85	4174708211712000	4		$((\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_5)/\mathfrak{S}_2^7) \wr \mathfrak{S}_3) \rtimes \mathfrak{S}_4$
86	16986931200	6	(3.102)$\wr \mathfrak{S}_2$	$(\mathfrak{S}_4 \times (\mathfrak{S}_2 \wr \mathfrak{S}_5)) \wr \mathfrak{S}_2$
87	3964362440048640000	16	(2.8)	$PSL(4,2) \wr \mathfrak{S}_4$
88	5898240	4		$(\mathfrak{S}_2 \wr ((\mathfrak{S}_2 \wr \mathfrak{S}_3) \times \mathfrak{S}_5))/\mathfrak{S}_2^{20}$
89	1819538433915500888064000 0	4	(3.58)	$\mathfrak{S}_3 \wr \mathfrak{S}_5 \wr \mathfrak{S}_4$
90	2880	168		$\mathfrak{A}_5 \rtimes (\mathfrak{D}_6 \rtimes \mathfrak{K}_4)$
91	248832000	6	(3.98)	$\mathfrak{S}_4 \times (\mathfrak{S}_5 \wr \mathfrak{S}_3)$
92	149299200	4	(3.82)$\wr \mathfrak{S}_2$	$((\mathfrak{S}_3 \wr \mathfrak{S}_2) \times \mathfrak{S}_5) \wr \mathfrak{S}_2$
93	23592960	6		$\mathfrak{S}_3 \times (\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_5)$
94	737280	44		$(\mathfrak{S}_2 \wr (\mathfrak{S}_2 \times \mathfrak{A}_5)) \rtimes \mathfrak{S}_3$
95	46009701534740225458176000	2	(1.20)	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_{15}$

Tabelle G.3: Tabelle der Automorphismengruppen für N=60, Teil 3 von 7

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
96	2211840	4		$((\mathfrak{S}_2^5 \rtimes \mathfrak{Z}_3) \wr \mathfrak{S}_2) \rtimes \mathfrak{S}_5$
97	11059200	10		$(\mathfrak{K}_4 \wr \mathfrak{S}_3) \rtimes (\mathfrak{S}_5 \wr \mathfrak{S}_2)$
98	92160	6		$(\mathfrak{S}_2 \wr (\mathfrak{S}_2 \times \mathfrak{S}_3)) \times \mathfrak{S}_5$
99	34560	2		$\mathfrak{S}_5 \times ((\mathfrak{S}_2 \times \mathfrak{S}_3) \wr \mathfrak{S}_2)$
100	47185920	8		$(\mathfrak{S}_2 \wr ((\mathfrak{S}_2 \wr \mathfrak{S}_3) \times \mathfrak{S}_5))/\mathfrak{S}_2^{17}$
101	754974720	8		$(\mathfrak{S}_2 \wr ((\mathfrak{S}_2 \wr \mathfrak{S}_3) \times \mathfrak{S}_5))/\mathfrak{S}_2^{13}$
102	552960	2		$(\mathfrak{S}_2 \wr \mathfrak{S}_5) \times \mathfrak{S}_2 \times t6n13$
103	8424627966566203392000	2	(1.28) (1.29)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_{15}))/\mathfrak{S}_2^{15}$ $\cong (\mathfrak{K}_4 \wr \mathfrak{S}_{15}) \rtimes \mathfrak{S}_3$
104	2211840	24		$(\mathfrak{Z}_3 \times \mathfrak{K}_4) \rtimes (\mathfrak{S}_2^8 \rtimes \mathfrak{S}_3)$
105	42278584320	8	(1.41)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_2 \times PSL(4,2)))/\mathfrak{S}_2^{10}$
106	364791569817010176000	4	(3.128)	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_5 \wr \mathfrak{S}_3$
107	5733089280	12	(3.93)	$(\mathfrak{S}_4 \wr \mathfrak{S}_5) \times \mathfrak{S}_3$
108	14929920000	6	(3.81)	$(\mathfrak{S}_5 \times \mathfrak{S}_6) \wr \mathfrak{S}_2$
109	11796480	24		$(\mathfrak{S}_2 \wr ((\mathfrak{S}_2 \wr \mathfrak{S}_3) \times \mathfrak{S}_5))/\mathfrak{S}_2^{18}$
110	737280	4		$(\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr (\mathfrak{Z}_3 \rtimes \mathfrak{S}_5))/\mathfrak{S}_2^{34}$
111	41287680	32	(1.41)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_2 \times PSL(4,2)))/\mathfrak{S}_2^{20}$
112	1321454146682880000	4	(3.136)$\wr\mathfrak{S}_2$	$PSL(4,2) \wr \mathfrak{S}_2 \wr \mathfrak{S}_2$
113	962899739228083069963468800000	2	(3.60)	$\mathfrak{S}_3 \wr \mathfrak{S}_{10} \wr \mathfrak{S}_2$
114	8847360	10		$(\mathfrak{K}_4 \wr \mathfrak{S}_5) \rtimes (\mathfrak{S}_3 \wr \mathfrak{S}_2)$
115	1866240000	32		$(\mathfrak{A}_5 \wr \mathfrak{S}_4) \rtimes \mathfrak{S}_3$
116	29859840000	12	(3.92)	$\mathfrak{S}_3 \times (\mathfrak{S}_5 \wr \mathfrak{S}_4)$
117	31384184832000	2	(3.5)	$\mathfrak{S}_4 \times \mathfrak{S}_{15}$
118	566231040	4		$\mathfrak{S}_2^{16} \rtimes (\mathfrak{A}_5 \rtimes (\mathfrak{D}_6 \rtimes \mathfrak{D}_6))$
119	709316941310853120	16	$\mathfrak{S}_2\wr$(3.135)	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr PSL(4,2)$
120	2866544640	32		$\mathfrak{Z}_3 \rtimes (\mathfrak{S}_4 \wr \mathfrak{S}_5)$
121	66795331387392000	2		$(\mathfrak{K}_4 \wr \mathfrak{S}_5 \wr \mathfrak{S}_3) \rtimes \mathfrak{S}_3$
122	188743680	8		$(\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_5))/\mathfrak{S}_2^{27}$
123	6039797760	4		$(\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_5))/\mathfrak{S}_2^{22}$
124	67947724800	8	N30Gr20$\wr\mathfrak{S}_2$	$((\mathfrak{S}_2 \wr (\mathfrak{Z}_3 \rtimes \mathfrak{S}_5))/\mathfrak{S}_2^6) \wr \mathfrak{S}_2$
125	271790899200	4	(3.100)$\wr\mathfrak{S}_2$	$((\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_5))/\mathfrak{S}_2^6) \wr \mathfrak{S}_2$
126	89060441849856000	4		$\mathfrak{S}_2 \wr (\mathfrak{S}_2 \times \mathfrak{S}_5) \wr \mathfrak{S}_3$
127	32831241283530915840	4	(3.129)	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_3 \wr \mathfrak{S}_5$
128	889507521104118578370853208064000 0	4	(1.75)	$\mathfrak{S}_3 \wr \mathfrak{S}_{20}$

Tabelle G.4: Tabelle der Automorphismengruppen für N=60, Teil 4 von 7

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
129	235600065379488183091200	4	(3.57)	$\mathfrak{S}_2 \wr \mathfrak{S}_3 \wr \mathfrak{S}_{10}$
130	46080	40		$\mathfrak{K}_4 \times ((\mathfrak{S}_2^5 \rtimes \mathfrak{A}_5) \rtimes \mathfrak{S}_3)$
131	46080	16		$(\mathfrak{S}_2 \wr \mathfrak{A}_5) \rtimes (\mathfrak{K}_4 \times \mathfrak{S}_3)$
132	11796480	8		$(\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr (\mathfrak{Z}_3 \rtimes \mathfrak{S}_5))/\mathfrak{S}_2^{30}$
133	5760	12		$\mathfrak{S}_3 \times \mathfrak{S}_5 \times (\mathfrak{S}_2 \wr \mathfrak{S}_2)$
134	59719680000	4		$(\mathfrak{S}_3 \times (\mathfrak{S}_5 \wr \mathfrak{S}_2)) \wr \mathfrak{S}_2$
135	3732480000	20	N30Gr22$\wr\mathfrak{S}_2$	$((\mathfrak{A}_5 \wr \mathfrak{S}_2) \rtimes \mathfrak{S}_3) \wr \mathfrak{S}_2$
136	1327104000	4		$(((\mathfrak{S}_2 \wr \mathfrak{S}_2) \times \mathfrak{S}_5) \wr \mathfrak{S}_3)/\mathfrak{S}_2^2$
137	35389440	4		$((\mathfrak{S}_2^7 \rtimes \mathfrak{Z}_3) \wr \mathfrak{S}_2) \rtimes \mathfrak{S}_5$
138	8640	28		$\mathfrak{A}_5 \rtimes (\mathfrak{D}_6 \rtimes \mathfrak{D}_6)$
139	158018273280000	2	(3.85)	$\mathfrak{S}_3 \times (\mathfrak{S}_{10} \wr \mathfrak{S}_2)$
140	622080000	8		$(\mathfrak{A}_5 \wr \mathfrak{K}_4) \rtimes \mathfrak{D}_6$
141	1474560	6		$(\mathfrak{S}_2 \wr (\mathfrak{S}_2 \times \mathfrak{S}_5)) \times \mathfrak{S}_3$
142	233280	32		$(\mathfrak{Z}_3 \wr \mathfrak{S}_4) \rtimes \mathfrak{S}_5$
143	2404631929946112000	2	(1.28) $\wr\mathfrak{S}_3$	$((\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_5))/\mathfrak{S}_2^5) \wr \mathfrak{S}_3$
144	138240	8		$\mathfrak{D}_6 \times (\mathfrak{Z}_3 \rtimes (\mathfrak{S}_2 \wr \mathfrak{S}_5))$
145	45298483200	4		$(((\mathfrak{S}_2^8 \rtimes (\mathfrak{S}_2 \times \mathfrak{A}_5)) \wr \mathfrak{S}_2) \rtimes \mathfrak{S}_4$
146	181193932800	2		$(((\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_5)/\mathfrak{S}_2^6) \wr \mathfrak{S}_2) \rtimes \mathfrak{S}_4$
147	12666373951979520	16	$\mathfrak{S}_2\wr$N30Gr8	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr (\mathfrak{Z}_3 \rtimes \mathfrak{S}_5)$
148	25332747903959040	8	$\mathfrak{S}_2\wr$(3.80)	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_5)$
149	14597412049059840000	4	(1.75)	$\mathfrak{S}_3 \times \mathfrak{S}_{20}$
150	32061759065948160	4		$\mathfrak{S}_2 \wr (\mathfrak{S}_2 \times \mathfrak{S}_3) \wr \mathfrak{S}_5$
151	948109639680000	6	(3.81)	$(\mathfrak{S}_3 \times \mathfrak{S}_{10}) \wr \mathfrak{S}_2$
152	6039797760	2		$(\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_5))/\mathfrak{S}_2^{22}$
153	94371840	4		$\mathfrak{S}_4 \times (\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_5)$
154	1869841788726096691200	2	(3.130)	$\mathfrak{S}_2 \wr \mathfrak{S}_3 \wr \mathfrak{S}_5 \wr \mathfrak{S}_2$
155	1911029760	4		$(\mathfrak{S}_2 \wr \mathfrak{S}_3 \wr \mathfrak{S}_5)/\mathfrak{S}_2^4$
156	143327232000	6	(3.97)	$(\mathfrak{S}_4 \times \mathfrak{S}_5) \wr \mathfrak{S}_3$
157	77760	8		$\mathfrak{S}_5 \times (\mathfrak{Z}_3 \rtimes \mathfrak{S}_3) \wr \mathfrak{S}_2$
158	2211840	24		$(\mathfrak{S}_2 \wr ((\mathfrak{S}_3 \wr \mathfrak{S}_2) \times \mathfrak{S}_5))/\mathfrak{S}_2^{22}$
159	45298483200	2		$(((\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_5)/\mathfrak{S}_2^6) \wr \mathfrak{S}_2) \rtimes \mathfrak{S}_3$
160	11324620800	4		$((\mathfrak{S}_2^9 \rtimes \mathfrak{A}_5) \wr \mathfrak{S}_2) \rtimes \mathfrak{S}_3$
161	22295347200	2	(3.87) (3.82)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_{10}))/\mathfrak{S}_2^{20}$ $\cong \mathfrak{S}_3 \times (\mathfrak{S}_2 \wr \mathfrak{S}_{10})$

Tabelle G.5: Tabelle der Automorphismengruppen für N=60, Teil 5 von 7

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
162	1244160	2		$\mathfrak{S}_5 \times (\mathfrak{S}_3 \wr \mathfrak{S}_2 \wr \mathfrak{S}_2)$
163	129879811031040	8	(1.31)	$(\mathfrak{K}_4 \wr PSL(4,2)) \rtimes \mathfrak{S}_3$
164	36238786560	2		$((\mathfrak{S}_2^9 \rtimes \mathfrak{S}_3) \wr \mathfrak{S}_2) \rtimes (\mathfrak{S}_2 \wr \mathfrak{S}_5)/\mathfrak{S}_2$
165	6011579824865280	2		$(\mathfrak{K}_4 \wr \mathfrak{S}_3 \wr \mathfrak{S}_5) \rtimes \mathfrak{S}_3$
166	3409345039564800	8	N30Gr27 $\wr\mathfrak{S}_2$	$((\mathfrak{S}_2 \wr PSL(4,2))/\mathfrak{S}_2^4) \wr \mathfrak{S}_2$
167	1546188226560	6		$\mathfrak{S}_2 \wr (\mathfrak{S}_2 \times \mathfrak{S}_3 \times \mathfrak{S}_5)$
168	7304069487211315200	4	(3.75) $\wr\mathfrak{S}_2$	$((\mathfrak{S}_2 \wr \mathfrak{S}_3 \wr \mathfrak{S}_5)/\mathfrak{S}_2^4)) \wr \mathfrak{S}_2$
169	403107840000	16	N15Gr4 $\wr\mathfrak{S}_4$	$(\mathfrak{Z}_3 \rtimes \mathfrak{S}_5) \wr \mathfrak{S}_4$
170	6449725440000	8	(3.89)	$(\mathfrak{S}_3 \times \mathfrak{S}_5) \wr \mathfrak{S}_4$
171	2308446652748267520000000	4	(3.58)	$\mathfrak{S}_2 \wr \mathfrak{S}_5 \wr \mathfrak{S}_6$
172	1036800	16	(N15Gr4$\times\mathfrak{S}_2)\wr\mathfrak{S}_2$	$((\mathfrak{Z}_3 \rtimes \mathfrak{S}_5) \times \mathfrak{S}_2) \wr \mathfrak{S}_2$
173	754974720	4		$(\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr (\mathfrak{Z}_3 \rtimes \mathfrak{S}_5))/\mathfrak{S}_2^{24})$
174	1509949440	2		$\mathfrak{S}_2 \wr (\mathfrak{S}_2 \times \mathfrak{S}_3 \times \mathfrak{S}_5)/\mathfrak{S}_2^{10}$
175	9331200	20	N30Gr31$\wr\mathfrak{S}_2$	$((\mathfrak{Z}_3 \wr \mathfrak{Z}_2) \rtimes \mathfrak{S}_5) \wr \mathfrak{S}_2$
176	1061683200	4		$(\mathfrak{S}_3 \times (\mathfrak{S}_2 \wr \mathfrak{S}_5)) \wr \mathfrak{S}_2$
177	43293270343680	4	(1.40)	$\mathfrak{S}_2 \wr (\mathfrak{S}_2 \times PSL(4,2))$
178	2264924160	2		$((\mathfrak{S}_2^9 \rtimes \mathfrak{S}_3) \wr \mathfrak{S}_2) \rtimes \mathfrak{S}_5$
179	2831155200	2		$((\mathfrak{S}_2^7 \rtimes \mathfrak{S}_5) \wr \mathfrak{S}_2) \rtimes \mathfrak{S}_3$
180	23592960	2		$(\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_5))/\mathfrak{S}_2^{30}$
181	9953280000	2		$\mathfrak{S}_3 \times (\mathfrak{S}_5 \wr \mathfrak{S}_2 \wr \mathfrak{S}_2)$
182	249312238496812892160	2	(3.131)	$\mathfrak{S}_2 \wr \mathfrak{S}_3 \wr \mathfrak{S}_2 \wr \mathfrak{S}_5$
183	7791007453025402880	2		$((\mathfrak{K}_4 \wr \mathfrak{S}_3) \rtimes \mathfrak{S}_3) \wr \mathfrak{S}_5$
184	24931223849681289216000000	4	(3.57)	$\mathfrak{S}_2 \wr \mathfrak{S}_6 \wr \mathfrak{S}_5$
185	265420800	24	N30Gr33$\wr\mathfrak{S}_2$	$(\mathfrak{Z}_3 \rtimes (\mathfrak{S}_2 \wr \mathfrak{S}_5)) \wr \mathfrak{S}_2$
186	188743680	4		$(\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr (\mathfrak{Z}_3 \rtimes \mathfrak{S}_5))/\mathfrak{S}_2^{26}$
187	377487360	2		$(\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_5))/\mathfrak{S}_2^{26}$
188	134369280000	4	N30Gr25$\wr\mathfrak{S}_2$	$((\mathfrak{Z}_3 \rtimes \mathfrak{S}_5) \wr \mathfrak{S}_2) \wr \mathfrak{S}_2$
189	2149908480000	2	(3.81)$\wr\mathfrak{S}_2$	$(\mathfrak{S}_3 \times \mathfrak{S}_5) \wr \mathfrak{S}_2 \wr \mathfrak{S}_2$
190	2308446652748267520000000	2	(3.132)	$\mathfrak{S}_2 \wr \mathfrak{S}_5 \wr \mathfrak{S}_3 \wr \mathfrak{S}_2$
191	188743680	4		$\mathfrak{S}_2^{19} \rtimes (\mathfrak{Z}_3 \rtimes \mathfrak{S}_5)$
192	7430083706880	6	(3.93)	$(\mathfrak{S}_3 \times \mathfrak{S}_4) \wr \mathfrak{S}_5$
193	172800	28		$\mathfrak{Z}_6 \rtimes ((\mathfrak{S}_2 \times \mathfrak{A}_5) \wr \mathfrak{S}_2)$
194	153896443516551168000000	2	(3.133)	$\mathfrak{S}_2 \wr \mathfrak{S}_5 \wr \mathfrak{S}_2 \wr \mathfrak{S}_3$

Tabelle G.6: Tabelle der Automorphismengruppen für N=60, Teil 6 von 7

Nr.	Ordnung	Anz	Formeltyp	Produktformel
195	2319282339840	8		$(\mathfrak{K}_4 \wr (\mathfrak{Z}_3 \rtimes \mathfrak{S}_5)) \rtimes \mathfrak{S}_3$
196	4638564679680	4		$(\mathfrak{K}_4 \wr (\mathfrak{S}_3 \times \mathfrak{S}_5)) \rtimes \mathfrak{S}_3$
197	307850752095864559239168000000	4	(3.57)	$\mathfrak{S}_2 \wr \mathfrak{S}_{10} \wr \mathfrak{S}_3$
198	1558201490605080576000000	2		$(\mathfrak{S}_2 \wr \mathfrak{S}_6 \wr \mathfrak{S}_5)/\mathfrak{S}_2^4$
199	66355200	4	(3.83)$\wr\mathfrak{S}_2$	$((\mathfrak{S}_2 \wr \mathfrak{S}_3) \times \mathfrak{S}_5) \wr \mathfrak{S}_2$
200	14427791579676672000000	4	N30Gr34$\wr\mathfrak{S}_2$	$(\mathfrak{S}_2 \wr \mathfrak{S}_5 \wr \mathfrak{S}_3)/\mathfrak{S}_2^2) \wr \mathfrak{S}_2$
201	92160	2		$\mathfrak{D}_{12} \rtimes (\mathfrak{S}_2 \wr \mathfrak{S}_5)$
202	2949120	4		$(\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr (\mathfrak{Z}_3 \rtimes \mathfrak{S}_5))/\mathfrak{S}_2^{32}$
203	367222335060486171693101875200000	2	(1.21)	$\mathfrak{S}_2 \wr \mathfrak{S}_{15} \wr \mathfrak{S}_2$
204	169114337280	4		$(\mathfrak{S}_2 \wr ((\mathfrak{S}_2 \wr PSL(4,2))/\mathfrak{S}_2^{10})/\mathfrak{S}_2^{12})$
205	44236800	12		$(\mathfrak{S}_2 \wr \mathfrak{A}_5 \wr \mathfrak{S}_2) \rtimes \mathfrak{S}_3$
206	60867245726760960	2		$(\mathfrak{S}_2 \wr \mathfrak{S}_3 \wr (\mathfrak{S}_2 \times \mathfrak{S}_5))/\mathfrak{S}_2^8$
207	5529600	2	(3.87) (3.83)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_5 \times \mathfrak{S}_6))/\mathfrak{S}_2^{24}$ $\cong (\mathfrak{S}_2 \wr \mathfrak{S}_6) \times \mathfrak{S}_5$
208	284813089515958324736640819941 8/ 67520000000	1/3	(1.19)	$\mathfrak{S}_2 \wr \mathfrak{S}_{30}$
209	11796480	4		$\mathfrak{S}_2^{15} \rtimes (\mathfrak{Z}_3 \rtimes \mathfrak{S}_5)$
210	23040	2		$\mathfrak{S}_5 \times ((\mathfrak{S}_2 \wr (\mathfrak{S}_2 \times \mathfrak{S}_3))/\mathfrak{S}_2^2)$
211	141557760	2		$(\mathfrak{K}_4 \wr \mathfrak{S}_5) \rtimes (\mathfrak{S}_4 \wr \mathfrak{S}_2)$
212	2404631929946112000000	2		$(\mathfrak{S}_2 \wr \mathfrak{S}_5 \wr (\mathfrak{S}_2 \times \mathfrak{S}_3))/\mathfrak{S}_2^4$
213	769626880239661398097920000 00	2	(3.75)	$(\mathfrak{S}_2 \wr \mathfrak{S}_{10} \wr \mathfrak{S}_3)/\mathfrak{S}_2^2$
	Anzahl Codes:	2121	davon 5	selbstdual

Tabelle G.7: Tabelle der Automorphismengruppen für N=60, Teil 7 von 7

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	135230151065285185924152732312421 06/ 18251338148256677888000000000000000	2	(1.18)	$\mathfrak{S}_{31} \wr \mathfrak{S}_2$
2	21473462090465280	72	(3.135)	$\mathfrak{S}_2 \wr PSL(5,2)$
3	639959040	48	(10.6)	$(\mathfrak{S}_2 \wr PSL(5,2))/\mathfrak{S}_2^{25}$
4	199974400819200	6/54	(3.136)	$PSL(5,2) \wr \mathfrak{S}_2$
5	655318056960	6/30	(10.6)	$(\mathfrak{S}_2 \wr PSL(5,2))/\mathfrak{S}_2^{15}$
6	671045690327040	12	(3.140)	$(\mathfrak{S}_2 \wr PSL(5,2))/\mathfrak{S}_2^5$
7	176584115499894161336717308363957 8/ 6240000000	1/3	(1.19)	$\mathfrak{S}_2 \wr \mathfrak{S}_{31}$
	Anzahl Codes:	221	davon 13	selbstdual

Tabelle G.8: Tabelle der Automorphismengruppen für N=62

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	800171327407254689548556110031819/ 39554304000000000000	4	(1.74)	$\mathfrak{S}_{21} \wr \mathfrak{S}_3$
2	139203614417442502776584774677/ 954560000000	8	(1.114)	$\mathfrak{S}_9 \wr PSL(3,2)$
3	22112446245500878848	48	(1.95),(1.97)	$\mathfrak{S}_3 \wr (\mathfrak{S}_3 \times PSL(3,2))$
4	20158709760	48	Gruppe	$PSL(6,2)$
5	27194421808748738535216906240000000000	4	(1.90)	$\mathfrak{S}_7 \wr \mathfrak{S}_3 \wr \mathfrak{S}_3$
6	417610843252327508329754324033863/ 6800000000	4	(1.110)	$\mathfrak{S}_9 \wr \mathfrak{S}_7$
7	663373387365026365440	8	(1.95)	$\mathfrak{S}_3 \wr (\mathfrak{S}_3 \times \mathfrak{S}_7)$
8	761443810644964678986073374720000000000	4	(1.111)	$\mathfrak{S}_7 \wr \mathfrak{S}_9$
9	624101682833016804605952	16	(1.89),(1.97)	$\mathfrak{S}_3 \wr PSL(3,2) \wr \mathfrak{S}_3$
10	10584	456		$PSL(2,8) \rtimes \mathfrak{MZ}(7,3)$
11	217728	136	(1.94),(1.97)	$(\mathfrak{S}_3 \wr \mathfrak{S}_3) \times PSL(3,2)$
12	2653493549460105461760	16	$\mathfrak{S}_3 \wr$N21Gr7	$\mathfrak{S}_3 \wr (PSL(3,4) \rtimes \mathfrak{S}_3)$
13	60963840	24	(1.116)	$\mathfrak{S}_9 \times PSL(3,2)$
14	362880	144	$\mathfrak{S}_3 \rtimes$N21Gr7	$\mathfrak{S}_3 \rtimes (PSL(3,4) \rtimes \mathfrak{S}_3)$
15	6531840	12	(1.94)	$(\mathfrak{S}_3 \wr \mathfrak{S}_3) \times \mathfrak{S}_7$
16	309503487609026701059686 40	4	(1.88)	$\mathfrak{S}_3 \wr \mathfrak{S}_3 \wr \mathfrak{S}_7$
17	1828915200	4	(1.93)	$\mathfrak{S}_9 \times \mathfrak{S}_7$
18	6145155072	48	(1.96),(1.97)	$(\mathfrak{S}_3 \times PSL(3,2)) \wr \mathfrak{S}_3$
19	1031678292030089003532288	8	(1.88),(1.97)	$\mathfrak{S}_3 \wr \mathfrak{S}_3 \wr PSL(3,2)$
20	16850745436491453724360704000	4	(1.89)	$\mathfrak{S}_3 \wr \mathfrak{S}_7 \wr \mathfrak{S}_3$
21	11207794765911894087472750421606 40000	4	(1.75)	$\mathfrak{S}_3 \wr \mathfrak{S}_{21}$
22	165919186944000	8	(1.96)	$(\mathfrak{S}_7 \times \mathfrak{S}_3) \wr \mathfrak{S}_3$
23	38685353383374723313827840	8	(1.113)	$PPSL(3,2) \wr \mathfrak{S}_9$
24	10618827964416000	16	N21Gr7$\wr\mathfrak{S}_3$	$(PSL(3,4) \rtimes \mathfrak{S}_3) \wr \mathfrak{S}_3$
25	7620480	8	(1.118)	$\mathfrak{S}_9 \times \mathfrak{MZ}(7,3)$
26	138161976369195440406528	8	(1.90),(1.97)	$PSL(3,2) \wr \mathfrak{S}_3 \wr \mathfrak{S}_3$
	Anzahl Codes:	1052		

Tabelle G.9: Tabelle der Automorphismengruppen für N=63;
$\mathfrak{MZ}(7,3) := \mathfrak{Z}_7 \rtimes \mathfrak{Z}_3$ metazyklisch

Nr.	Ordnung	Anz	F-typ	Produktformel
1	1384756746908520303863323978879191673089370 2/ 6381483815731200000000000000	2	(1.18)	$\mathfrak{S}_{32} \wr \mathfrak{S}_2$
2	4599277532427412486834855086740364500926/ 4640000000000000	4	(1.22)	$\mathfrak{S}_{16} \wr \mathfrak{S}_4$
3	2682226270902341423473589904998400000000	2	(1.53)	$\mathfrak{S}_8 \wr \mathfrak{S}_2 \wr \mathfrak{S}_4$
4	8046678812707024270420769714995200000000	2	(1.54)	$\mathfrak{S}_8 \wr \mathfrak{S}_4 \wr \mathfrak{S}_2$
5	2816337584447458494647269400248320000000 0	4	(1.51)	$\mathfrak{S}_8 \wr \mathfrak{S}_8$
6	1250663156661521142932255539 20	2	(1.55)	$\mathfrak{S}_4 \wr \mathfrak{S}_2 \wr \mathfrak{S}_8$
7	3939588943483791600236604948 4800	2	(1.56)	$\mathfrak{S}_4 \wr \mathfrak{S}_8 \wr \mathfrak{S}_2$
8	2535125485131819894752255284346880 00	4	(1.23)	$\mathfrak{S}_4 \wr \mathfrak{S}_{16}$
9	5889241796446748858646528000	2	(1.20)	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_{16}$
10	915189090356915129548800	2	(1.49)	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_8 \wr \mathfrak{S}_2$
11	2905362191609254379520	2	(1.50)	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_8$
12	1906208133914831798403072 0	4	(1.57)	$\mathfrak{S}_2 \wr \mathfrak{S}_4 \wr \mathfrak{S}_8$
13	2724289124719947111884390400 00	4	(1.58)	$\mathfrak{S}_2 \wr \mathfrak{S}_8 \wr \mathfrak{S}_4$
14	3760356711019378398137363202048000000	2	(1.21)	$\mathfrak{S}_2 \wr \mathfrak{S}_{16} \wr \mathfrak{S}_2$
15	1130138339199322632554990773529330319360000000	3	(1.19)	$\mathfrak{S}_2 \wr \mathfrak{S}_{32}$
	Anzahl Codes:	41		

Tabelle G.10: Tabelle der Automorphismengruppen für N=64

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	1123525226295645019162350145893094234521 60/ 0000000000	4	(1.101)	$\mathfrak{S}_{13} \wr \mathfrak{S}_5$
2	6662489153541532286976000000000000000	4	(1.102)	$\mathfrak{S}_5 \wr \mathfrak{S}_{13}$
3	747242496000	4	(1.105)	$\mathfrak{S}_5 \times \mathfrak{S}_{13}$
	Anzahl Codes:	12		

Tabelle G.11: Tabelle der Automorphismengruppen für N=65

Nr.	Ordnung	Anz.	F.-typ	Produktformel
1	150800009738337861090715981299943973 1/ 994324217294358753312768000000000000000	2	(1.18)	$\mathfrak{S}_{33} \wr \mathfrak{S}_2$
2	852022429423244793431302545961 88/ 168518629563742289920000000000000	4	(1.74)	$\mathfrak{S}_{22} \wr \mathfrak{S}_3$
3	$291250583854141696973485095442710528*10^{12}$	2	(1.85)	$\mathfrak{S}_{11} \wr \mathfrak{S}_3 \wr \mathfrak{S}_2$
4	$194167055902761131315656730295140352*10^{12}$	2	(1.84)	$\mathfrak{S}_{11} \wr \mathfrak{S}_2 \wr \mathfrak{S}_3$
5	$291250583854141696973485095442710528*10^{13}$	4	(1.79)	$\mathfrak{S}_{11} \wr \mathfrak{S}_6$
6	10760022482802706051655270400000000000000	4	(1.78)	$\mathfrak{S}_6 \wr \mathfrak{S}_{11}$
7	2057296206731673600	8	(3.80)	$\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_{11})$
8	1076002248280270605165527040000	2	(1.82)	$\mathfrak{S}_3 \wr \mathfrak{S}_2 \wr \mathfrak{S}_{11}$
9	1961990553600	4	(3.101) (3.102)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_{11}))/\mathfrak{S}_2^{20}$ $\cong \mathfrak{S}_4 \times (\mathfrak{S}_2 \wr \mathfrak{S}_{11})$
10	2874009600	2	(3.82)	$(\mathfrak{S}_3 \wr \mathfrak{S}_2) \times \mathfrak{S}_{11}$
11	28740096000	4	(1.86)	$\mathfrak{S}_6 \times \mathfrak{S}_{11}$
12	419439126407752985276087009280000	2	(1.83)	$\mathfrak{S}_3 \wr \mathfrak{S}_{11} \wr \mathfrak{S}_2$
13	147942890910037001954640305565204480000	4	(1.75)	$\mathfrak{S}_3 \wr \mathfrak{S}_{22}$
14	124396834520369760672153600	4	(1.80)	$\mathfrak{S}_2 \wr \mathfrak{S}_3 \wr \mathfrak{S}_{11}$
15	19120211066880000	2	(3.85)	$(\mathfrak{S}_{11} \wr \mathfrak{S}_2) \times \mathfrak{S}_3$
16	502269581721600	2	(3.100)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_{11}))/\mathfrak{S}_2^{12}$
17	6744004366665646080000	4	(1.72)	$\mathfrak{S}_3 \times \mathfrak{S}_{22}$
18	114721266401280000	6	(3.81)	$(\mathfrak{S}_3 \times \mathfrak{S}_{11}) \wr \mathfrak{S}_2$
19	121481283711298594406400	2	(3.75)	$(\mathfrak{S}_2 \wr \mathfrak{S}_3 \wr \mathfrak{S}_{11})/\mathfrak{S}_2^{10}$
20	490497638400	2	(3.87) (3.86)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_{11}))/\mathfrak{S}_2^{22}$ $\cong (\mathfrak{S}_2 \wr \mathfrak{S}_{11}) \times \mathfrak{S}_3$
21	1916006400	2	(3.84) (3.83)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_{11}))/\mathfrak{S}_2^{30}$ $\cong (\mathfrak{S}_2 \wr \mathfrak{S}_3) \times \mathfrak{S}_{11}$
22	32779948083167658267786608640000 00	4	(1.81)	$\mathfrak{S}_2 \wr \mathfrak{S}_{11} \wr \mathfrak{S}_3$
23	81949870207919145669466521600000 00	2	(3.76)	$(\mathfrak{S}_2 \wr \mathfrak{S}_{11} \wr \mathfrak{S}_3)/\mathfrak{S}_2^2$
24	745891303871552937486 29/ 391052935801077760000000	3	(1.19)	$\mathfrak{S}_2 \wr \mathfrak{S}_{33}$
	Anzahl Codes:	77		

Tabelle G.12: Tabelle der Automorphismengruppen für N=66

Nr.	Ordnung	Anz.	F.-typ	Produktformel
1	174324811257518567420867674382735233018/ 54387951922787188295598080000000000000	2	(1.18)	$\mathfrak{S}_{34} \wr \mathfrak{S}_2$
2	384136258785869918312933931699641983 48/ 1879199744000000000000	4	(1.22)	$\mathfrak{S}_{17} \wr \mathfrak{S}_4$
3	10343311979337825170589201560135270 4000	4	(1.23)	$\mathfrak{S}_4 \wr \mathfrak{S}_{17}$
4	800936884316757844775927808000	2	(1.20)	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_{17}$
5	36663980910496117161984000	2	(1.28) (1.29)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_{17}))/\mathfrak{S}_2^{17}$ $\cong (\mathfrak{K}_4 \wr \mathfrak{S}_{17}) \rtimes \mathfrak{S}_3$
6	8536498274304000	2	(1.24)	$\mathfrak{S}_{17} \times \mathfrak{S}_4$
7	43469723579384014282467918615674880 00000	2	(1.21)	$\mathfrak{S}_2 \wr \mathfrak{S}_{17} \wr \mathfrak{S}_2$
8	50720608663265599749067985915996344 7328/ 7680000000	3	(1.19)	$\mathfrak{S}_2 \wr \mathfrak{S}_{34}$
	Anzahl Codes:	21		

Tabelle G.13: Tabelle der Automorphismengruppen für N=68

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	10366556898792619401678658076718214463 6616/ 59020524414566400000000000	4	(1.74)	$\mathfrak{S}_{23} \wr \mathfrak{S}_3$
2	80560064161608801819033 60	8	(2.2)	$\mathfrak{S}_3 \wr M23$
3	61205760	24	(1.73)	$M23 \times \mathfrak{S}_3$
4	204161189455851062697403621679982182 40000	4	(1.75)	$\mathfrak{S}_3 \wr \mathfrak{S}_{23}$
5	155112100433309859840000	4	(1.72)	$\mathfrak{S}_3 \times \mathfrak{S}_{23}$
6	6369045980411068416000	8	(2.8)	$M23 \wr \mathfrak{S}_3$
	Anzahl Codes:	52		

Tabelle G.14: Tabelle der Automorphismengruppen für N=69

Anhang H

Tabellen der Automorphismengruppen für zyklische Codes, Teil 5 ($70 \leq N \leq 92$)

Nr.	Ordnung	Anz	Formeltyp	Produktformel
1	213547893790460245090562901118850660/ 44771625241105414305662107648 $* 10^{16}$	2	(1.18)	$\mathfrak{S}_{35} \wr \mathfrak{S}_2$
2	139203614417442502776584/ 77467795456000000000000000	8	(1.114)	$\mathfrak{S}_{10} \wr PSL(3,2)$
3	604258831307228986785971804 8/ 64807513587344998400000000000	4	(1.101)	$\mathfrak{S}_{14} \wr \mathfrak{S}_5$
4	3451172832707346432000000000000000	8	$\mathfrak{S}_5 \wr$(3.138)	$\mathfrak{S}_5 \wr (\mathfrak{S}_2 \wr PSL(3,2))/\mathfrak{S}_2^3$
5	7247462948685427507200000000000000	12	$\mathfrak{S}_5$(3.136)	$\mathfrak{S}_5 \wr PSL(3,2) \wr \mathfrak{S}_2$
6	406103365677314495459239133184 $* 10^{11}$	2	(3.62)	$\mathfrak{S}_7 \wr \mathfrak{S}_2 \wr \mathfrak{S}_5$
7	4176108432523275083297543/ 24033863680000000000000000	4	(1.110)	$\mathfrak{S}_{10} \wr \mathfrak{S}_7$
8	692692325498880	48	(3.107)	$\mathfrak{S}_2 \wr (\mathfrak{S}_5 \times PSL(3,2))$
9	304577524257985871594429349888 $* 10^{12}$	2	(3.61)	$\mathfrak{S}_7 \wr \mathfrak{S}_5 \wr \mathfrak{S}_2$
10	8282814798497631436800000000000000000	2	(3.59)	$\mathfrak{S}_5 \wr \mathfrak{S}_2 \wr \mathfrak{S}_7$
11	5160960	24	(3.115)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_5 \times PSL(3,2)))/\mathfrak{S}_2^{27}$
12	38376768056506219820898098085888 $* 10^{12}$	4	(1.111)	$\mathfrak{S}_7 \wr \mathfrak{S}_{10}$
13	20780769764966400	8	(3.80)	$\mathfrak{S}_2 \wr (\mathfrak{S}_5 \times \mathfrak{S}_7)$
14	27609382661658771456000000000000000	8	$\mathfrak{S}_5 \wr$(3.135)	$\mathfrak{S}_5 \wr \mathfrak{S}_2 \wr PSL(3,2)$
15	6773760	24	(3.114)	$(PSL(3,2) \wr \mathfrak{S}_2) \times \mathfrak{S}_5)$
16	4838400	28	(3.111)	$(\mathfrak{S}_5 \wr \mathfrak{S}_2) \times PSL(3,2)$
17	1238630400	4	(3.101)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_5 \times \mathfrak{S}_7))/\mathfrak{S}_2^{24}$
18	609638400	32	(1.116)	$\mathfrak{S}_{10} \times PSL(3,2)$
19	652271665381688475648000000000000000000	2	(3.60)	$\mathfrak{S}_5 \wr \mathfrak{S}_7 \wr \mathfrak{S}_2$
20	322560	36	(3.115) $\mathfrak{S}_5 \times$(3.138)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_5 \times PSL(3,2)))/\mathfrak{S}_2^{31}$ $\cong ((\mathfrak{S}_2 \wr PSL(3,2))/\mathfrak{S}_2^3) \times \mathfrak{S}_5$
21	1119298177794977424211968 $* 10^{16}$	4	(1.102)	$\mathfrak{S}_5 \wr \mathfrak{S}_{14}$
22	812851200	36	(3.108)	$(\mathfrak{S}_5 \times PSL(3,2)) \wr \mathfrak{S}_2$
23	165150720	12	(3.115)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_5 \times PSL(3,2)))/\mathfrak{S}_2^{22}$
24	2580480	28	(3.115) (3.112)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_5 \times PSL(3,2)))/\mathfrak{S}_2^{28}$ $\cong (\mathfrak{S}_2 \wr PSL(3,2)) \times \mathfrak{S}_5$
25	145152000	2	(3.82)	$(\mathfrak{S}_5 \wr \mathfrak{S}_2) \times \mathfrak{S}_7$
26	5517946722523041025228 80	16	(3.135)$\wr \mathfrak{S}_5$	$\mathfrak{S}_2 \wr PSL(3,2) \wr \mathfrak{S}_5$
27	18289152000	4	(1.112)	$\mathfrak{S}_7 \times \mathfrak{S}_{10}$

Tabelle H.1: Tabelle der Automorphismengruppen für N=70, Teil 1 von 3

Nr.	Ordnung	Anz	Formeltyp	Produktformel
28	86586540687360	16	$\mathfrak{S}_2 \wr (1.118)$	$\mathfrak{S}_2 \wr (\mathfrak{S}_5 \times \mathfrak{MZ}(7,3))$
29	6096384000	2	(3.85)	$(\mathfrak{S}_7 \wr \mathfrak{S}_2) \times \mathfrak{S}_5$
30	1052464813713653760	8	(3.79)	$(((\mathfrak{S}_2 \wr PSL(3,2))/\mathfrak{S}_2^3) \wr \mathfrak{S}_5)/\mathfrak{S}_2^4$
31	10461394944000	4	(1.105)	$\mathfrak{S}_5 \times \mathfrak{S}_{14}$
32	5040	52	$\mathfrak{S}_2 \times (1.118)$	$\mathfrak{S}_2 \times (\mathfrak{S}_5 \times \mathfrak{MZ}(7,3))$
33	2642411520	4	(3.115)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_5 \times PSL(3,2)))/\mathfrak{S}_2^{18}$
34	645120	2/54	(3.115)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_5 \times PSL(3,2)))/\mathfrak{S}_2^{30}$
			(3.109)	$\cong (\mathfrak{S}_2 \wr \mathfrak{S}_5) \times PSL(3,2)$
35	731566080000	6	(3.81)	$(\mathfrak{S}_5 \times \mathfrak{S}_7) \wr \mathfrak{S}_2$
36	40320	40	(3.115)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_5 \times PSL(3,2)))/\mathfrak{S}_2^{34}$
			$\mathfrak{S}_2 \times (1.116)$	$\cong \mathfrak{S}_2 \times \mathfrak{S}_5 \times PSL(3,2)$
37	10569646080	8	(3.115)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_5 \times PSL(3,2)))/\mathfrak{S}_2^{16}$
38	16839437019418460160	12	$(3.138) \wr \mathfrak{S}_5$	$((\mathfrak{S}_2 \wr PSL(3,2))/\mathfrak{S}_2^3) \wr \mathfrak{S}_5$
39	41287680	12	(3.115)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_5 \times PSL(3,2)))/\mathfrak{S}_2^{24}$
40	169114337280	8	(3.115)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_5 \times PSL(3,2)))/\mathfrak{S}_2^{12}$
41	80640	4	(1.119)	$\mathfrak{MZ}(7,3) \times (\mathfrak{S}_2 \wr \mathfrak{S}_5)$
42	1321205760	4	(3.115)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_5 \times PSL(3,2)))/\mathfrak{S}_2^{19}$
43	604800	24	(1.120)	$\mathfrak{MZ}(7,3) \times (\mathfrak{S}_5 \wr \mathfrak{S}_2)$
44	21139292160	12	(3.115)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_5 \times PSL(3,2)))/\mathfrak{S}_2^{15}$
45	62051046025873430937600000000	4	(3.57)	$\mathfrak{S}_2 \wr \mathfrak{S}_5 \wr \mathfrak{S}_7$
46	64991393684069535167230771200	8	(1.113)	$PSL(3,2) \wr \mathfrak{S}_{10}$
47	13408610535730989691305984000000	4	(3.58)	$\mathfrak{S}_2 \wr \mathfrak{S}_7 \wr \mathfrak{S}_5$
48	12700800	12	$(1.118) \wr \mathfrak{S}_2$	$(\mathfrak{S}_5 \times \mathfrak{MZ}(7,3)) \wr \mathfrak{S}_2$
49	20683682008624476979200000000	8	$\mathfrak{S}_2 \wr (1.114)$	$\mathfrak{S}_2 \wr \mathfrak{S}_5 \wr PSL(3,2)$
50	51580471177832964418437120 0	4	$(1.113) \wr \mathfrak{S}_2$	$PSL(3,2) \wr \mathfrak{S}_5 \wr \mathfrak{S}_2$
51	77414400	2	(3.87)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_5 \times \mathfrak{S}_7))/\mathfrak{S}_2^{28}$
			(3.86)	$\cong (\mathfrak{S}_2 \wr \mathfrak{S}_7) \times \mathfrak{S}_5$
52	19353600	2	(3.84)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_5 \times \mathfrak{S}_7))/\mathfrak{S}_2^{30}$
			(3.86)	$\cong (\mathfrak{S}_2 \wr \mathfrak{S}_5) \times \mathfrak{S}_7$
53	68773961570443952557916160	2/6	$(3.136) \wr \mathfrak{S}_5$	$PSL(3,2) \wr \mathfrak{S}_2 \wr \mathfrak{S}_5$
54	3550442606428591982434759 0/ 1411974413130137600000000 0	1/3	(1.19)	$\mathfrak{S}_2 \wr \mathfrak{S}_{35}$
55	105840	2/6	(1.121)	$\mathfrak{S}_5 \times (\mathfrak{MZ}(7,3) \wr \mathfrak{S}_2)$

Tabelle H.2: Tabelle der Automorphismengruppen für N=70, Teil 2 von 3;
$\mathfrak{MZ}(7,3) := \mathfrak{Z}_7 \rtimes \mathfrak{Z}_3$ metazyklisch

Nr.	Ordnung	Anz	Formeltyp	Produktformel
z1	2642411520	12	(1.122)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_5 \times \mathfrak{MZ}(7,3)))/\mathfrak{S}_2^{15}$
z3	20293720473600	2	(3.100)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_5 \times \mathfrak{S}_7))/\mathfrak{S}_2^{10}$
z5	5411658792960	4	(3.115)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_5 \times PSL(3,2)))/\mathfrak{S}_2^{7})$
z6	969547594154272358400000000	2	(3.75)	$(\mathfrak{S}_2 \wr \mathfrak{S}_5 \wr \mathfrak{S}_7)/\mathfrak{S}_2^{6}$
z7	838038158483186855706624000000	2	(3.76)	$(\mathfrak{S}_2 \wr \mathfrak{S}_7 \wr \mathfrak{S}_5)/\mathfrak{S}_2^{4}$
z8	258546025107805962240000000	4	(3.78)	$(\mathfrak{S}_2 \wr \mathfrak{S}_5 \wr PSL(3,2))/\mathfrak{S}_2^{3}$
z10	323182531384757452800000000	2/6	(3.77)	$(\mathfrak{S}_2 \wr \mathfrak{S}_5 \wr PSL(3,2))/\mathfrak{S}_2^{6}$
62	Anzahl Codes:	725	davon 9	selbstdual

Tabelle H.3: Tabelle der Automorphismengruppen für N=70, Teil 3 von 3
(Zusatzauswertung);
$\mathfrak{MZ}(7,3) := \mathfrak{Z}_7 \rtimes \mathfrak{Z}_3$ metazyklisch

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	2767580703524364776373695198500304 55/ 940240263124726169401380915118 08∗10^{16}	2	(1.18)	$\mathfrak{S}_{36} \wr \mathfrak{S}_2$
2	1433072825689091706088057692525 52/ 596745658774299729506965913 6∗10^{12}	4	(1.74)	$\mathfrak{S}_{24} \wr \mathfrak{S}_3$
3	4032508790230548054481855241 4/ 1016168579937508723261 44 ∗10^{12}	4	(1.22)	$\mathfrak{S}_{18} \wr \mathfrak{S}_4$
4	57977972225275029393044/ 9946153604368826368∗10^{12}	2	(1.84)	$\mathfrak{S}_{12} \wr \mathfrak{S}_2 \wr \mathfrak{S}_3$
5	86966958337912544089567/ 4919230406553239552∗10^{12}	2	(1.85)	$\mathfrak{S}_{12} \wr \mathfrak{S}_3 \wr \mathfrak{S}_2$
6	1154610459424035095030/ 1047550888263024642∗10^{8}	2	(3.62)	$\mathfrak{S}_9 \wr \mathfrak{S}_2 \wr \mathfrak{S}_4$
7	44716976551907349825060864∗10^{12}	4	(3.61)	$\mathfrak{S}_6 \wr \mathfrak{S}_4 \wr \mathfrak{S}_3$
8	86966958337912544089567/ 4919230406553239552∗10^{13}	4	(1.79)	$\mathfrak{S}_{12} \wr \mathfrak{S}_6$
9	3463831378272105285090/ 3142652664789073 92∗10^{8}	2	(3.61)	$\mathfrak{S}_9 \wr \mathfrak{S}_4 \wr \mathfrak{S}_2$
10	27948110344942093640663 04∗10^{12}	4	(3.94)	$\mathfrak{S}_6 \wr (\mathfrak{S}_3 \times \mathfrak{S}_4)$
11	36499735094439062090/ 6286114272182272∗10^{9}	4	(1.90)	$\mathfrak{S}_8 \wr \mathfrak{S}_3 \wr \mathfrak{S}_3$
12	1212340982395236849781/ 6099928432676175872∗10^{9}	4	(1.92)	$\mathfrak{S}_9 \wr \mathfrak{S}_8$
13	89433953103814699650121728∗10^{13}	2	(3.62)	$\mathfrak{S}_6 \wr \mathfrak{S}_2 \wr \mathfrak{S}_6$
14	89433953103814699650121728∗10^{12}	2	(3.124)	$\mathfrak{S}_6 \wr \mathfrak{S}_2 \wr \mathfrak{S}_3 \wr \mathfrak{S}_2$
15	59622635402543133100081152∗10^{12}	2	(3.125)	$\mathfrak{S}_6 \wr \mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_3$
16	60367918345074922263832 1664∗10^{12}	4	(3.62)	$\mathfrak{S}_6 \wr \mathfrak{S}_3 \wr \mathfrak{S}_4$
17	1021992582644293738 53/ 76011199621103616∗10^{10}	4	(1.91)	$\mathfrak{S}_8 \wr \mathfrak{S}_9$
18	1146309213366765559480320	8	(3.96)	$\mathfrak{S}_3 \wr (\mathfrak{S}_3 \times \mathfrak{S}_8)$
19	16098111558686645937021911 04∗10^{12}	4	(3.61)	$\mathfrak{S}_6 \wr \mathfrak{S}_4 \wr \mathfrak{S}_3$
20	20122639448358307421277388 8∗10^{14}	2	(3.61)	$\mathfrak{S}_6 \wr \mathfrak{S}_6 \wr \mathfrak{S}_2$
21	12966875608266651209921625 43042560	2	(3.59)	$\mathfrak{S}_4 \wr \mathfrak{S}_2 \wr \mathfrak{S}_9$
22	92966594251415380286301536 256∗10^{14}	4	(1.78)	$\mathfrak{S}_6 \wr \mathfrak{S}_{12}$

Tabelle H.4: Tabelle der Automorphismengruppen für N=72, Teil 1 von 3

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
23	39222389586724934123520	4	$\mathfrak{S}_2 \wr (1.28)$	$\mathfrak{S}_2 \wr ((\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_9))/\mathfrak{S}_2^9)$
24	598486169231032320	4	(3.88)	$\mathfrak{S}_2 \wr (\mathfrak{S}_4 \times \mathfrak{S}_9)$
25	2344457420244640062508151026483 20	4	(3.59)	$\mathfrak{S}_4 \wr \mathfrak{S}_3 \wr \mathfrak{S}_6$
26	92966594251415380286301536256 00	2	(3.59)	$\mathfrak{S}_3 \wr \mathfrak{S}_2 \wr \mathfrak{S}_{12}$
27	52254720	12	(3.91)	$(\mathfrak{S}_3 \wr \mathfrak{S}_3) \times \mathfrak{S}_8$
28	35672555520	4	(3.101)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_4 \times \mathfrak{S}_9))/\mathfrak{S}_2^{24}$
29	20122639448358307421277388800	2	(3.126)	$\mathfrak{S}_3 \wr \mathfrak{S}_2 \wr \mathfrak{S}_6 \wr \mathfrak{S}_2$
30	418037760	2	(3.90)	$(\mathfrak{S}_4 \wr \mathfrak{S}_2) \times \mathfrak{S}_9$
31	14631321600	4	(1.93)	$\mathfrak{S}_8 \times \mathfrak{S}_9$
32	156297161349642670/ 83387673509888000	4	(3.60)	$\mathfrak{S}_4 \wr \mathfrak{S}_6 \wr \mathfrak{S}_3$
33	32089321595303888365868285952 0	4	(3.59)	$\mathfrak{S}_3 \wr \mathfrak{S}_3 \wr \mathfrak{S}_8$
34	183805461747179780/ 9006390404762828800	2	(3.60)	$\mathfrak{S}_4 \wr \mathfrak{S}_9 \wr \mathfrak{S}_2$
35	89433953103814699650121728 0	2	(3.127)	$\mathfrak{S}_3 \wr \mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_6$
36	10085757322300697346048000	4	$\mathfrak{S}_2 \wr (3.76)$	$\mathfrak{S}_2 \wr ((\mathfrak{S}_2 \wr \mathfrak{S}_6 \wr \mathfrak{S}_3)/\mathfrak{S}_2^2)$
37	44683107750739404736/ 945350739784368128000	4	(1.23)	$\mathfrak{S}_4 \wr \mathfrak{S}_{18}$
38	65197351812680916044938739 7120	4	(3.57)	$\mathfrak{S}_3 \wr \mathfrak{S}_4 \wr \mathfrak{S}_6$
39	11533491134161312964773360435 2000	2	(3.57)	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_{18}$
40	30561258662194179396065034240000	4	(3.58)	$\mathfrak{S}_3 \wr \mathfrak{S}_6 \wr \mathfrak{S}_4$
41	47443402444102480315809792 00	2	(1.49)	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_9 \wr \mathfrak{S}_2$
42	40343029289202789384192000	4	(3.128)	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_6 \wr \mathfrak{S}_3$
43	18635576393124628/ 50284498976768000	4	(3.60)	$\mathfrak{S}_3 \wr \mathfrak{S}_8 \wr \mathfrak{S}_3$
44	72392887030185669427200	2		$((\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_9)/\mathfrak{S}_2^8) \wr \mathfrak{S}_2$
45	217437243129779147/ 5671235056107520000	2	(3.60)	$\mathfrak{S}_3 \wr \mathfrak{S}_{12} \wr \mathfrak{S}_2$
46	651535983271671024844800	2	$(1.28) \wr \mathfrak{S}_2$	$((\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_9))/\mathfrak{S}_2^9) \wr \mathfrak{S}_2$
47	293992112816425530284/ 26121521917434265600 00	4	(1.75)	$\mathfrak{S}_3 \wr \mathfrak{S}_{24}$
48	151697542348800	4	(3.89)	$(\mathfrak{S}_4 \times \mathfrak{S}_9) \wr \mathfrak{S}_2$
49	605145439338041840762880	4	(3.129)	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_3 \wr \mathfrak{S}_6$
50	71652576683732982147160473600	4	(3.57)	$\mathfrak{S}_2 \wr \mathfrak{S}_3 \wr \mathfrak{S}_{12}$

Tabelle H.5: Tabelle der Automorphismengruppen für N=72, Teil 2 von 3

Nr	Ordnung	Anz.	Formeltyp	Produktformel
51	147740585775889121280	4		$\mathfrak{S}_2 \wr \mathfrak{D}_6 \wr \mathfrak{S}_6$
52	3346977244733861045207040	2	(1.50)	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_9$
53	155092157324097363954892800	2	(3.130)	$\mathfrak{S}_2 \wr \mathfrak{S}_3 \wr \mathfrak{S}_6 \wr \mathfrak{S}_2$
54	84950623715328000	8	(3.89)	$(\mathfrak{S}_3 \times \mathfrak{S}_8) \wr \mathfrak{S}_3$
55	658785531080965865952810168320	4	(3.57)	$\mathfrak{S}_2 \wr \mathfrak{S}_4 \wr \mathfrak{S}_9$
56	25733809807850229278441472 0	2	(3.75)	$(\mathfrak{S}_2 \wr \mathfrak{S}_4 \wr \mathfrak{S}_9)/\mathfrak{S}_2^8$
57	6892984769959882842439680	2	(3.131)	$\mathfrak{S}_2 \wr \mathfrak{S}_3 \wr \mathfrak{S}_2 \wr \mathfrak{S}_6$
58	107702887030623169413120	2		$((\mathfrak{K}_4 \wr \mathfrak{S}_3) \rtimes \mathfrak{S}_3) \wr \mathfrak{S}_6$
59	199495389743677440	2	(1.66)	$\mathfrak{S}_2 \wr (\mathfrak{S}_9 \times (\mathfrak{S}_2 \wr \mathfrak{S}_2))$
60	6892984769959882842439680000000	4	(3.57)	$\mathfrak{S}_2 \wr \mathfrak{S}_6 \wr \mathfrak{S}_6$
61	6419592322744320	6	(3.95)	$(\mathfrak{S}_3 \times \mathfrak{S}_4) \wr \mathfrak{S}_6$
62	139345920	2	(3.84) (3.83)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_4 \times \mathfrak{S}_9))/\mathfrak{S}_2^{32}$ $\cong (\mathfrak{S}_2 \wr \mathfrak{S}_4) \times \mathfrak{S}_9$
63	689298476995988284243968000000	2	(3.132)	$\mathfrak{S}_2 \wr \mathfrak{S}_6 \wr \mathfrak{S}_3 \wr \mathfrak{S}_2$
64	459532317997325522829312000000	2	(3.133)	$\mathfrak{S}_2 \wr \mathfrak{S}_6 \wr \mathfrak{S}_2 \wr \mathfrak{S}_3$
65	285984975156601168017175766630400 0	4	(3.58)	$\mathfrak{S}_2 \wr \mathfrak{S}_9 \wr \mathfrak{S}_4$
z1	430811548122492677652480000 00	4	(3.76)$\wr\mathfrak{S}_2$	$((\mathfrak{S}_2 \wr \mathfrak{S}_6 \wr \mathfrak{S}_3)/\mathfrak{S}_2^2) \wr \mathfrak{S}_2$
z2	453150002301709707893882077839360000 00	4	(3.58)	$\mathfrak{S}_2 \wr \mathfrak{S}_{12} \wr \mathfrak{S}_3$
z4	563367617588816825100/ 7842252591464448000000	2	(3.58)	$\mathfrak{S}_2 \wr \mathfrak{S}_{18} \wr \mathfrak{S}_2$
z5	113287500575427426973470519459840000 00	2	(3.76)	$(\mathfrak{S}_2 \wr \mathfrak{S}_{12} \wr \mathfrak{S}_3)/\mathfrak{S}_2^2$
66	25563186766285862273530264/ 90166215774536990720000000 0	3	(1.19)	$\mathfrak{S}_2 \wr \mathfrak{S}_{36}$
70	Anzahl Codes:	235		

Tabelle H.6: Tabelle der Automorphismengruppen für N=72, Teil 3 von 3

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	49448448	48	Gruppe	PSL(3,8)$\rtimes\mathfrak{Z}_3$
	Anzahl Codes:	48		

Tabelle H.7: Tabelle der Automorphismengruppen für N=73

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	37888179831248553788555887267469 16941/ 8218892021775012591049047279665152$*10^{16}$	2	(1.18)	$\mathfrak{S}_{37} \wr \mathfrak{S}_2$
2	18916758207051538082412396 0/ 27229996731573731328000000 00	3	(1.19)	$\mathfrak{S}_2 \wr \mathfrak{S}_{37}$
	Anzahl Codes:	5		

Tabelle H.8: Tabelle der Automorphismengruppen für N=74

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	223917629013920579076259014457 1/ 134324150918348433273546342 4∗10^{18}	4	(1.74)	$\mathfrak{S}_{25} \wr \mathfrak{S}_3$
2	3106055549436611788 8∗10^{16}	16	(2.2)	$\mathfrak{S}_5 \wr PSL(4,2)$
3	458859050023927011840597339319 21/ 320563039010816000000000000000	4	(1.101)	$\mathfrak{S}_{15} \wr \mathfrak{S}_5$
4	554652776685109248000000000000000000	16	$\mathfrak{S}_5 \wr$ N15Gr4	$\mathfrak{S}_5 \wr (\mathfrak{Z}_3 \rtimes \mathfrak{S}_5)$
5	110930555337021849600000000000000000	8	(3.88)	$\mathfrak{S}_5 \wr (\mathfrak{S}_3 \times \mathfrak{S}_5)$
6	143765999716780317081 6∗10^{16}	4	(3.57)	$\mathfrak{S}_5 \wr \mathfrak{S}_3 \wr \mathfrak{S}_5$
7	159739999685311463424∗10^{18}	4	(3.58)	$\mathfrak{S}_5 \wr \mathfrak{S}_5 \wr \mathfrak{S}_3$
8	201473672003095936358154 24∗10^{18}	4	(1.102)	$\mathfrak{S}_5 \wr \mathfrak{S}_{15}$
9	399607733956902912000000	16	(2.8)	$PSL(4,2) \wr \mathfrak{S}_5$
10	848923851727616094335139840 00000	4	(3.59)	$\mathfrak{S}_3 \wr \mathfrak{S}_5 \wr \mathfrak{S}_5$
11	559872000000	32		$\mathfrak{Z}_3 \rtimes (\mathfrak{A}_5 \wr \mathfrak{S}_5) \times \mathfrak{S}_2$
12	17915904000000	12	(3.91)	$(\mathfrak{S}_5 \wr \mathfrak{S}_5) \times \mathfrak{S}_3$
13	279936000000	64		$\mathfrak{Z}_3 \rtimes (\mathfrak{A}_5 \wr \mathfrak{S}_5)$
14	8957952000000	32		$\mathfrak{Z}_3 \rtimes (\mathfrak{S}_5 \wr \mathfrak{S}_5)$
15	44098816922463829542 63/ 91822828761513984000000	4	(1.75)	$\mathfrak{S}_3 \wr \mathfrak{S}_{25}$
16	93067260259985915904000000	4	(1.72)	$\mathfrak{S}_3 \times \mathfrak{S}_{25}$
17	725594112000000	16	N15Gr4$\wr\mathfrak{S}_3$	$(\mathfrak{Z}_3 \rtimes \mathfrak{S}_5) \wr \mathfrak{S}_3$
18	23219011584000000	8	(3.95)	$(\mathfrak{S}_5 \times \mathfrak{S}_3) \wr \mathfrak{S}_5$
	Anzahl Codes:	252		

Tabelle H.9: Tabelle der Automorphismengruppen für N=75

Nr.	Ordnung	Anz.	F.-typ	Produktformel
1	54710531676322911670674701214225480639908080 0/ 79443118181474824271836479488000000000000000 0	2	(1.18)	$\mathfrak{S}_{38} \wr \mathfrak{S}_2$
2	52552057805163525300812985691581368/ 10550603607432415412224000000000000	4	(1.22)	$\mathfrak{S}_{19} \wr \mathfrak{S}_4$
3	203754971343371685600470799373416718663680 00	4	(1.23)	$\mathfrak{S}_4 \wr \mathfrak{S}_{19}$
4	17530906523925195706455507861504000	2	(1.20)	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_{19}$
5	20062530354223475311037644800 0	2	(1.28) (1.29)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_{19}))/\mathfrak{S}_2^{19} \cong (\mathfrak{K}_4 \wr \mathfrak{S}_{19}) \rtimes \mathfrak{S}_3$
6	2919482409811968000	2	(1.24)	$\mathfrak{S}_{19} \times \mathfrak{S}_4$
7	81350283979825149544553242127420746629120000 00	2	(1.21)	$\mathfrak{S}_2 \wr \mathfrak{S}_{19} \wr \mathfrak{S}_2$
8	14376736237359168942633420980/ 69479751599603580928000000000	3	(1.19)	$\mathfrak{S}_2 \wr \mathfrak{S}_{38}$
	Anzahl Codes:	21		

Tabelle H.10: Tabelle der Automorphismengruppen für N=76

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	271268463797076743427528230 0/ 14577044094976000000000000000	8	(1.114)	$\mathfrak{S}_{11} \wr PSL(3,2)$
2	81380539139123023028258469 00/ 43731132284928000000000000000	4	(1.110)	$\mathfrak{S}_{11} \wr \mathfrak{S}_7$
3	212760802105270482687059/ 05578816307200000000000000	4	(1.111)	$\mathfrak{S}_7 \wr \mathfrak{S}_{11}$
4	6706022400	24	(1.116)	$\mathfrak{S}_{11} \times PSL(3,2)$
5	201180672000	4	(1.112)	$\mathfrak{S}_{11} \times \mathfrak{S}_7$
6	12010409552816050098904246517760 0	8	(1.113)	$PSL(3,2) \wr \mathfrak{S}_{11}$
7	838252800	8	(1.118)	$\mathfrak{S}_{11} \times \mathfrak{MZ}(7,3)$
	Anzahl Codes:	60		

Tabelle H.11: Tabelle der Automorphismengruppen für N=77;
$\mathfrak{MZ}(7,3) := \mathfrak{Z}_7 \rtimes \mathfrak{Z}_3$ metazyklisch

Nr.	Ordnung	Anz.	F.-typ	Produktformel
1	832147186796871486510962205468369560533 00/ 189800832982754023207717463285301248∗10^{16}	2	(1.18)	$\mathfrak{S}_{39} \wr \mathfrak{S}_2$
2	393557624754866809784432843809822568812 7/ 654089206321585051402240000000000000000000	4	(1.74)	$\mathfrak{S}_{26} \wr \mathfrak{S}_3$
3	419772897208061309024421176121/ 559942483564874956800000000000	2	(1.85)	$\mathfrak{S}_{13} \wr \mathfrak{S}_3 \wr \mathfrak{S}_2$
4	279848598138707539349614117414/ 373294989043249971200000000000	2	(1.84)	$\mathfrak{S}_{13} \wr \mathfrak{S}_2 \wr \mathfrak{S}_3$
5	419772897208061309024421176121/ 559942483564874956800000000000	4	(1.79)	$\mathfrak{S}_{13} \wr \mathfrak{S}_6$
6	870167322193247959479782379356 16∗10^{15}	4	(1.78)	$\mathfrak{S}_6 \wr \mathfrak{S}_{13}$
7	20540045328009029222400	8	(3.80)	$\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_{13})$
8	870167322193247959479782379356 1600	2	(1.82)	$\mathfrak{S}_3 \wr \mathfrak{S}_2 \wr \mathfrak{S}_{13}$
9	1224282105446400	4	(3.101) (3.102)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_{13}))/\mathfrak{S}_2^{24}$ $\cong \mathfrak{S}_4 \times (\mathfrak{S}_2 \wr \mathfrak{S}_{13})$
10	448345497600	2	(3.82)	$(\mathfrak{S}_3 \wr \mathfrak{S}_2) \times \mathfrak{S}_{13}$
11	4483454976000	4	(1.86)	$\mathfrak{S}_6 \times \mathfrak{S}_{13}$
12	1322888187201576333798379408135815168 0000	2	(1.83)	$\mathfrak{S}_3 \wr \mathfrak{S}_{13} \wr \mathfrak{S}_2$
13	687941543990435740865 17/ 124361286796181504000000	4	(1.75)	$\mathfrak{S}_3 \wr \mathfrak{S}_{26}$
14	447112078506493808598281355264 00	4	(1.80)	$\mathfrak{S}_2 \wr \mathfrak{S}_3 \wr \mathfrak{S}_{13}$
15	4653094565235916800 00	2	(3.85)	$(\mathfrak{S}_{13} \wr \mathfrak{S}_2) \times \mathfrak{S}_3$
16	1253664875977113600	2	(3.100)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_{13}))/\mathfrak{S}_2^{14}$
17	241974876675963381350400 0000	4	(1.72)	$\mathfrak{S}_3 \times \mathfrak{S}_{26}$
18	27918567391415500800 00	6	(3.81)	$(\mathfrak{S}_3 \times \mathfrak{S}_{13}) \wr \mathfrak{S}_2$
19	109158222291624464989814784 00	2	(3.75)	$(\mathfrak{S}_2 \wr \mathfrak{S}_3 \wr \mathfrak{S}_{13})/\mathfrak{S}_2^{12}$
20	306070526361600	2	(3.86)	$(\mathfrak{S}_2 \wr \mathfrak{S}_{13}) \times \mathfrak{S}_3$
21	298896998400	2	(3.83)	$(\mathfrak{S}_2 \wr \mathfrak{S}_3) \times \mathfrak{S}_{13}$
22	796456444045484982594287140010459136000000	4	(1.81)	$\mathfrak{S}_2 \wr \mathfrak{S}_{13} \wr \mathfrak{S}_3$
23	199114111011371245648571785002614784000000	2	(3.76)	$(\mathfrak{S}_2 \wr \mathfrak{S}_{13} \wr \mathfrak{S}_3)/\mathfrak{S}_2^2$
24	112138542651401517752540683649/ 419420624769079312384000000 00	3	(1.19)	$\mathfrak{S}_2 \wr \mathfrak{S}_{39}$
	Anzahl Codes:	77		

Tabelle H.12: Tabelle der Automorphismengruppen für N=78

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	133143549887499437841753952874939/ 129685280303681332772406437132347 941256481996800000000000000000	2	(1.18)	$\mathfrak{S}_{40} \wr \mathfrak{S}_2$
2	840832924882616404813007771065301889 6/ 880965771891864659558400000000000000000	4	(1.22)	$\mathfrak{S}_{20} \wr \mathfrak{S}_4$
3	481148587237889290367766195673983 30/ 630709193805398016000000000000000000	4	(1.101)	$\mathfrak{S}_{16} \wr \mathfrak{S}_5$
4	115461045942403509503010475 50/ 888263024640000000000000000	2	(1.53)	$\mathfrak{S}_{10} \wr \mathfrak{S}_2 \wr \mathfrak{S}_4$
5	346383137827210528509031426 5/ 266478907392000000000000000000	2	(1.54)	$\mathfrak{S}_{10} \wr \mathfrak{S}_4 \wr \mathfrak{S}_2$
6	436050168594898661776043 1/ 445171670876160000000000	2	(3.62)	$\mathfrak{S}_8 \wr \mathfrak{S}_2 \wr \mathfrak{S}_5$
7	29638572818895202765535143840972 80	4	$\mathfrak{S}_4 \wr (1.28)$	$\mathfrak{S}_4 \wr ((\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_5))/\mathfrak{S}_2^5)$
8	121234098239523684978160999 28/ 432676175872000000000000000000	4	(1.51)	$\mathfrak{S}_{10} \wr \mathfrak{S}_8$
9	3270376264461739963320323/ 583878753157120000000000000	2	(3.61)	$\mathfrak{S}_8 \wr \mathfrak{S}_5 \wr \mathfrak{S}_2$
10	11577567507380938580287165562880	4	(3.88)	$\mathfrak{S}_4 \wr (\mathfrak{S}_4 \times \mathfrak{S}_5)$
11	810647932926689280	10	$\mathfrak{S}_2 \wr (3.101)$	$\mathfrak{S}_2 \wr ((\mathfrak{S}_2 \wr (\mathfrak{S}_4 \times \mathfrak{S}_5))/\mathfrak{S}_2^{12})$
12	$1908360529573854283038 72 * 10^{17}$	2	(3.59)	$\mathfrak{S}_5 \wr \mathfrak{S}_2 \wr \mathfrak{S}_8$
13	4120674093221792353783607 7/ 156872289779712000000000000	4	(1.52)	$\mathfrak{S}_8 \wr \mathfrak{S}_{10}$
14	$5452458655925297951539 2 * 10^{16}$	2	$(1.53) \wr \mathfrak{S}_2$	$\mathfrak{S}_5 \wr \mathfrak{S}_2 \wr \mathfrak{S}_4 \wr \mathfrak{S}_2$
15	151996487423754240	4	$\mathfrak{S}_2 \wr (1.61)$	$\mathfrak{S}_2 \wr ((\mathfrak{S}_4 \wr \mathfrak{S}_2) \times \mathfrak{S}_5)$
16	5319877059831398400	8	(3.80)	$\mathfrak{S}_2 \wr (\mathfrak{S}_8 \times \mathfrak{S}_5)$
17	14937840700723182193829712495850291200	2	(1.55)	$\mathfrak{S}_4 \wr \mathfrak{S}_2 \wr \mathfrak{S}_{10}$
18	$1817486218641765983846 4 * 10^{16}$	2	(3.125)	$\mathfrak{S}_5 \wr \mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_4$
19	$1472163837099830446915584 * 10^{16}$	4	(3.67)	$\mathfrak{S}_5 \wr \mathfrak{S}_4 \wr \mathfrak{S}_4$
20	11855429127558081106214057536389 1200	2	$(1.55) \wr \mathfrak{S}_2$	$\mathfrak{S}_4 \wr \mathfrak{S}_2 \wr \mathfrak{S}_5 \wr \mathfrak{S}_2$
21	19818086400	4	(3.101)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_5 \times \mathfrak{S}_8))/\mathfrak{S}_2^{28}$
22	132816557330708771635200	4	$\mathfrak{S}_2 \wr (1.67)$	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr (\mathfrak{S}_2 \times \mathfrak{S}_5) \wr \mathfrak{S}_2$

Tabelle H.13: Tabelle der Automorphismengruppen für N=80, Teil 1 von 3

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
23	119534901597637894471680 0	4	$\mathfrak{S}_2 \wr (1.28) \wr \mathfrak{S}_2$	$(\mathfrak{S}_2 \wr (\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_5))/\mathfrak{S}_2^5)) \wr \mathfrak{S}_2$
24	$60113356681576409915719 68*10^{18}$	2	(3.60)	$\mathfrak{S}_5 \wr \mathfrak{S}_8 \wr \mathfrak{S}_2$
25	35389440	2		$(\mathfrak{S}_2 \wr \mathfrak{S}_4 \wr \mathfrak{S}_2) \times \mathfrak{S}_5$
26	158072388367441081416187433818521 60	2	(3.127)	$\mathfrak{S}_4 \wr \mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_5$
27	384115903732881827841335464179007 4880	4	(3.65)	$\mathfrak{S}_4 \wr \mathfrak{S}_4 \wr \mathfrak{S}_5$
28	11796480	6		$(\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_4) \times \mathfrak{S}_5$
29	18239578490850508800	8	$\mathfrak{S}_2 \wr$ (1.64)	$\mathfrak{S}_2 \wr (\mathfrak{S}_4 \times \mathfrak{S}_5) \wr \mathfrak{S}_2$
30	$38682945024594419780765614 08*10^{19}$	4	(1.102)	$\mathfrak{S}_5 \wr \mathfrak{S}_{16}$
31	2000603665275426186673622209 2656640000	4	(3.66)	$\mathfrak{S}_4 \wr \mathfrak{S}_5 \wr \mathfrak{S}_4$
32	955514880	12	(3.90)	$(\mathfrak{S}_4 \wr \mathfrak{S}_4) \times \mathfrak{S}_5$
33	68852103320239427215687680	4	$\mathfrak{S}_2 \wr (3.75)$	$\mathfrak{S}_2 \wr (\mathfrak{S}_2 \wr \mathfrak{S}_4 \wr \mathfrak{S}_5)/\mathfrak{S}_2^4)$
34	1087163596800	6	$N40\#11 \wr \mathfrak{S}_2$	$((\mathfrak{S}_2 \wr (\mathfrak{S}_4 \times \mathfrak{S}_5))/\mathfrak{S}_2^{12}) \wr \mathfrak{S}_2$
35	1058719459663755537 98/ 7680873143389388800 00	2	(1.55)	$\mathfrak{S}_4 \wr \mathfrak{S}_2 \wr \mathfrak{S}_{10}$
36	390168576000	2	(3.85)	$(\mathfrak{S}_8 \wr \mathfrak{S}_2) \times \mathfrak{S}_5$
37	1106804644422573096960	4	$\mathfrak{S}_2 \wr (1.66)$	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr (\mathfrak{S}_5 \times (\mathfrak{S}_2 \wr \mathfrak{S}_2))$
38	2510734786560000	4	(1.105)	$\mathfrak{S}_5 \times \mathfrak{S}_{16}$
39	471859200	2		$(\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_2) \times \mathfrak{S}_5) \wr \mathfrak{S}_2$
40	97802386244818409088225/ 98369924002495856640000	4	(1.23)	$\mathfrak{S}_4 \wr \mathfrak{S}_{20}$
41	38220595200	4	$(1.61) \wr \mathfrak{S}_2$	$((\mathfrak{S}_4 \wr \mathfrak{S}_2) \times \mathfrak{S}_5) \wr \mathfrak{S}_2$
42	50665495807918080	10	$\mathfrak{S}_2 \wr (1.60)$	$\mathfrak{S}_2 \wr ((\mathfrak{S}_2 \wr \mathfrak{S}_4) \times \mathfrak{S}_5)$
43	48318382080	4		$(\mathfrak{S}_2 \wr ((\mathfrak{S}_2 \wr \mathfrak{S}_4) \times \mathfrak{S}_5))/\mathfrak{S}_2^{20}$
44	28049450438280313130328812578406 40000	2	(1.20)	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_{20}$
45	46820229120000	6	(3.81)	$(\mathfrak{S}_8 \times \mathfrak{S}_5) \wr \mathfrak{S}_2$
46	30363777564225587402118266880000	2	(1.49)	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_{10} \wr \mathfrak{S}_2$
47	1006632960	2		$(\mathfrak{K}_4 \wr \mathfrak{S}_5) \rtimes (\mathfrak{S}_2 \wr \mathfrak{K}_4 \wr \mathfrak{S}_2)$
48	188743680	4		$(\mathfrak{S}_2 \wr ((\mathfrak{S}_2 \wr \mathfrak{S}_4) \times \mathfrak{S}_5))/\mathfrak{S}_2^{24}$
49	57376752766866189346406 40000	4	(3.128)	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_5 \wr \mathfrak{S}_4$

Tabelle H.14: Tabelle der Automorphismengruppen für N=80, Teil 2 von 3

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
50	1101633653123830835451002880	4	$\mathfrak{S}_2 \wr (1.57)$	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_4 \wr \mathfrak{S}_5$
51	87549976756082442240000	4		$\mathfrak{S}_2 \wr (\mathfrak{S}_2 \times \mathfrak{S}_5) \wr \mathfrak{S}_4$
52	29183325585360814080000	2	$(1.67) \wr \mathfrak{S}_2$	$\mathfrak{S}_2 \wr (\mathfrak{S}_2 \times \mathfrak{S}_5) \wr \mathfrak{S}_2 \wr \mathfrak{S}_2$
53	4533471823554859405148160	2	$\mathfrak{S}_2 \wr (1.50)$	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_5$
54	318504960	2		$(\mathfrak{S}_4 \wr \mathfrak{S}_2 \wr \mathfrak{S}_2) \times \mathfrak{S}_5$
55	850025966916536138465280	4	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr (1.28)$	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr (\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_5))/\mathfrak{S}_2^5)$
56	7091548117242677821440000	2	$(1.28) \wr \mathfrak{S}_4$	$((\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_5))/\mathfrak{S}_2^5) \wr \mathfrak{S}_4$
57	340010386766614455386112000	2	$\mathfrak{S}_2 \wr (1.49)$	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_5 \wr \mathfrak{S}_2$
58	3320413933267719290880	4	$\mathfrak{S}_2 \wr (1.65)$	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr (\mathfrak{S}_4 \times \mathfrak{S}_5)$
59	1651129712640000	6	(3.89)	$(\mathfrak{S}_4 \times \mathfrak{S}_5) \wr \mathfrak{S}_4$
60	428413087325934213786501120 0	2	(1.50)	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_{10}$
61	25297364393509089389879104634880 0	4	(1.57)	$\mathfrak{S}_2 \wr \mathfrak{S}_4 \wr \mathfrak{S}_{10}$
62	550376570880000	2	$(1.64) \wr \mathfrak{S}_2$	$(\mathfrak{S}_4 \times \mathfrak{S}_5) \wr \mathfrak{S}_2 \wr \mathfrak{S}_2$
63	16888498602639360	2		$\mathfrak{S}_2 \wr (\mathfrak{S}_5 \times (\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_2))$
64	19062081339148317984030720000000 00	4	(3.57)	$\mathfrak{S}_2 \wr \mathfrak{S}_5 \wr \mathfrak{S}_8$
65	20077273328181816976094527488 00	2	$\mathfrak{S}_2 \wr (1.56)$	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_4 \wr \mathfrak{S}_5$
66	78426848938210222562869248 00	4	$(3.75) \wr \mathfrak{S}_2$	$((\mathfrak{S}_2 \wr \mathfrak{S}_4 \wr \mathfrak{S}_5)/\mathfrak{S}_2^4) \wr \mathfrak{S}_2$
67	54463089540423765668659200000000	2	(3.132)	$\mathfrak{S}_2 \wr \mathfrak{S}_5 \wr \mathfrak{S}_4 \wr \mathfrak{S}_2$
68	3932160	2		$(\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_2) \times \mathfrak{S}_5$
69	26769697770909089301459369984 0	2	(3.131)	$\mathfrak{S}_2 \wr \mathfrak{S}_4 \wr \mathfrak{S}_2 \wr \mathfrak{S}_5$
70	$1405994720111465824655086347878 4 * 10^6$	4	(3.58)	$\mathfrak{S}_2 \wr \mathfrak{S}_8 \wr \mathfrak{S}_5$
71	2026619832316723200	4	$(1.66) \wr \mathfrak{S}_2$	$(\mathfrak{S}_2 \wr (\mathfrak{S}_5 \times (\mathfrak{S}_2 \wr \mathfrak{S}_2))) \wr \mathfrak{S}_2$
72	18154363180141255222886400000000	2	(3.133)	$\mathfrak{S}_2 \wr \mathfrak{S}_5 \wr \mathfrak{S}_2 \wr \mathfrak{S}_4$
73	$4575759602505618688274812266086 4 * 10^8$	4	(1.58)	$\mathfrak{S}_2 \wr \mathfrak{S}_{10} \wr \mathfrak{S}_4$
74	1238630400	2	(3.86)	$(\mathfrak{S}_2 \wr \mathfrak{S}_8) \times \mathfrak{S}_5$
z2	87874670006966614040942896742400 0000	2	(3.75)	$(\mathfrak{S}_2 \wr \mathfrak{S}_8 \wr \mathfrak{S}_5)/\mathfrak{S}_2^4$
75	120795955200	2		$((\mathfrak{S}_2 \wr \mathfrak{S}_5) \times (\mathfrak{S}_2 \wr \mathfrak{K}_4)) \wr \mathfrak{S}_2$
76	1301604543677202392712851/ 8740387319460659200000000	2	(1.21)	$\mathfrak{S}_2 \wr \mathfrak{S}_{20} \wr \mathfrak{S}_2$
77	9059696640	2		$(\mathfrak{K}_4 \wr \mathfrak{S}_5) \rtimes ((\mathfrak{S}_2 \wr \mathfrak{S}_4)/\mathfrak{S}_2) \wr \mathfrak{S}_2)$
78	4246732800	4	$(1.60) \wr \mathfrak{S}_2$	$((\mathfrak{S}_2 \wr \mathfrak{S}_4) \times \mathfrak{S}_5) \wr \mathfrak{S}_2$
79	897108341211212142020325469195/ 3553649981526344990720000000 00	3	(1.19)	$\mathfrak{S}_2 \wr \mathfrak{S}_{40}$
	Anzahl Codes:	281		

Tabelle H.15: Tabelle der Automorphismengruppen für N=80, Teil 3 von 3

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	774639472805004341698699166470873762194166/ 154378480277585667502899200000000000000000	4	(1.74)	$\mathfrak{S}_{27} \wr \mathfrak{S}_3$
2	1414074521865804261585269895652387349153 7/ 1008000000000	4	(1.90)	$\mathfrak{S}_9 \wr \mathfrak{S}_3 \wr \mathfrak{S}_3$
3	3959408661224251932438755707826684577630/ 3882240000000000	4	(3.2)	$\mathfrak{S}_9 \wr \mathfrak{S}_9$
4	37428984708762455389948768734412 80	4	(1.88)	$\mathfrak{S}_3 \wr \mathfrak{S}_3 \wr \mathfrak{S}_9$
5	29344324011669765025719834687779635 2000	4	(1.89)	$\mathfrak{S}_3 \wr \mathfrak{S}_9 \wr \mathfrak{S}_3$
6	1114465301264505900201577414652846098140/ 3648000000	4	(1.75)	$\mathfrak{S}_3 \wr \mathfrak{S}_{21}$
	Anzahl Codes:	24		

Tabelle H.16: Tabelle der Automorphismengruppen für N=81

Nr.	Ordnung	Anz.	F.-typ	Produktformel
1	605577012673101171654202984666750 6/ 120689544424463927112637739786912 8 541676196010109222081737523 2∗10^{20}	2	(1.18)	$\mathfrak{S}_{46} \wr \mathfrak{S}_2$
2	107198560988876131782289010508637823 0433/ 991397721186192020132799376558915584∗10^{16}	4	(1.22)	$\mathfrak{S}_{23} \wr \mathfrak{S}_4$
3	566891054592444764255837589217518551040	8	(1.36)	$\mathfrak{S}_4 \wr M23)$
4	2940226537908565432074240	12	(1.42)	$\mathfrak{S}_2 \wr ((\mathfrak{S}_2 \wr M23)/\mathfrak{S}_2^{11})$
5	1026862255964160	8	(1.46) (1.48)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times M23))/\mathfrak{S}_2^{45} \cong$ $((\mathfrak{K}_4 \wr M23))/\mathfrak{K}_4^{11}) \rtimes \mathfrak{S}_3$
6	244823040	20	(1.37)	$\mathfrak{S}_4 \times M23$
7	1464508462116394513182228 4800	12	(1.34)	$\mathfrak{S}_2 \wr M23 \wr \mathfrak{S}_2$
8	1436656651182637629656586 81/ 217430331600192600539136 0000	4	(1.23)	$\mathfrak{S}_4 \wr \mathfrak{S}_{23}$
9	1526033717028693029493/ 1146877857096007680000	2	(1.20)	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_{23}$
10	1091504371425170681114040389861376 0000	2	(1.28) (1.29)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times \mathfrak{S}_{23}))/\mathfrak{S}_2^{23}$ $\cong (\mathfrak{K}_4 \wr \mathfrak{S}_{23}) \rtimes \mathfrak{S}_3$
11	3491660266200052531200	8	(1.43)	$((\mathfrak{S}_2 \wr M23)/\mathfrak{S}_2^3) \wr \mathfrak{S}_2$
12	6204484017332394393600 00	2	(1.24)	$\mathfrak{S}_{23} \times \mathfrak{S}_4$
13	6021583949636742004888043520	8	(1.33)	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr M23$
14	81607680	4	(1.39)	$M23 \times (\mathfrak{S}_2 \wr \mathfrak{S}_2)$
15	2598815331373363698755174400 00	8	(1.35)	$M23 \wr \mathfrak{S}_4$
16	9405863093549879077945397402 10/ 1050924251766199418880000 0000	2	(1.21)	$\mathfrak{S}_2 \wr \mathfrak{S}_{23} \wr \mathfrak{S}_2$
17	43069724676395001446 40	4	(1.30) (1.31)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_3 \times M23))/\mathfrak{S}_2^{23}$ $\cong (\mathfrak{K}_4 \wr M23) \rtimes \mathfrak{S}_3$
18	3872126110701618388180999522272 600/ 2739993435932433237927788544∗10^{10}	1/3	(1.19)	$\mathfrak{S}_2 \wr \mathfrak{S}_{46}$
19	8662717771244545662517248 0000	2/2	(1.38)	$M23 \wr \mathfrak{S}_2 \wr \mathfrak{S}_2$
20	1435657489213166714880	2/2	(1.40)	$\mathfrak{S}_2 \wr (\mathfrak{S}_2 \times M23)$
21	342287418654720	4	(1.41)	$(\mathfrak{S}_2 \wr (\mathfrak{S}_2 \times M23))/\mathfrak{S}_2^{22}$
	Anzahl Codes:	121	davon 5	selbstdual

Tabelle H.17: Tabelle der Automorphismengruppen für N=92

Anhang I

Tabellen der Automorphismengruppen für zyklische Codes, Teil 6 ($N > 92$)

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	185003413056501583802694144647176736 4/ 698973614843803975412278542037621141/ 434720868884766426280896430604288$*10^{24}$	2	(1.18)	$\mathfrak{S}_{50} \wr \mathfrak{S}_2$
2	138929335041583466789846557/ 619194618664245285144665730/ 485809210799202035459686 4$*10^{24}$	4	(1.22)	$\mathfrak{S}_{25} \wr \mathfrak{S}_4$
3	102283205574397767170728641624527347961/ 466979106800206415254233633657978 88$*10^{21}$	4	(1.101)	$\mathfrak{S}_{20} \wr \mathfrak{S}_5$
4	152041292591011274205648219/ 180544687781006907801 6$*10^{21}$	2	(3.62)	$\mathfrak{S}_{10} \wr \mathfrak{S}_2 \wr \mathfrak{S}_5$
5	28265545672316744580779212 8$*10^{21}$	4		$(\mathfrak{S}_5 \wr \mathfrak{K}_4 \wr \mathfrak{S}_5) \rtimes \mathfrak{S}_3$
6	114030969443258455654236164385/ 4085158357551808512$*10^{22}$	2	(3.61)	$\mathfrak{S}_{10} \wr \mathfrak{S}_5 \wr \mathfrak{S}_2$
7	11041228778248728351866 88$*10^{21}$	4	(3.88)	$\mathfrak{S}_5 \wr (\mathfrak{S}_4 \times \mathfrak{S}_5)$
8	143679021498505654124337567125 6/ 147299530515278725 12$*10^{22}$	4	(3.2)	$\mathfrak{S}_{10} \wr \mathfrak{S}_{10}$
9	14245835018847639268712723251 2$*10^{22}$	2	(3.59)	$\mathfrak{S}_5 \wr \mathfrak{S}_2 \wr \mathfrak{S}_{10}$
10	11306218268926697832311685 12$*10^{22}$	2	(3.126)	$\mathfrak{S}_5 \wr \mathfrak{S}_2 \wr \mathfrak{S}_5 \wr \mathfrak{S}_2$
11	15074957691902263776415580 16$*10^{22}$	2	(3.127)	$\mathfrak{S}_5 \wr \mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_5$
12	36632147191322500976689859788 8$*10^{21}$	4	(3.70)	$\mathfrak{S}_4 \wr \mathfrak{S}_5 \wr \mathfrak{S}_5$
13	19079243328813802592025968 64$*10^{24}$	4	(3.69)	$\mathfrak{S}_5 \wr \mathfrak{S}_5 \wr \mathfrak{S}_4$
14	10096735569608264331700142604288$*10^{24}$	2	(3.60)	$\mathfrak{S}_5 \wr \mathfrak{S}_{10} \wr \mathfrak{S}_2$
15	93271623844927224243379577349891686 4$*10^{24}$	4	(1.102)	$\mathfrak{S}_5 \wr \mathfrak{S}_{20}$
16	95580328557660450985415/ 186222590791254016000000	4	(3.68)	$\mathfrak{S}_4 \wr \mathfrak{S}_5 \wr \mathfrak{S}_5$
17	71663616000000	6	(3.99)	$(\mathfrak{S}_5 \wr \mathfrak{S}_5) \times \mathfrak{S}_4$
18	49650853864871956480931640 2287/ 439226010265627463254016000000	4	(1.23)	$\mathfrak{S}_4 \wr \mathfrak{S}_{25}$
19	10478441965681638538694787742669209 6$*10^{6}$	2	(1.29)	$\cong (\mathfrak{K}_4 \wr \mathfrak{S}_{25}) \rtimes \mathfrak{S}_3$
20	705045537999251734688641843200000 0	4		$(\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_5 \wr \mathfrak{S}_5)/\mathfrak{S}_2^4$
21	37226904103994366361600000 0	2	(1.24)	$\mathfrak{S}_{25} \times \mathfrak{S}_4$
22	11280728607988027755018269491200000 0	4	(3.129)	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_5 \wr \mathfrak{S}_5$
23	10758141143787410502451200000 0	4	(3.75)$\wr\mathfrak{S}_5$	$((\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_5)/\mathfrak{S}_2^4) \wr \mathfrak{S}_5$
24	6115295232000000	4		$(((\mathfrak{S}_2 \wr \mathfrak{S}_2) \times \mathfrak{S}_5) \wr \mathfrak{S}_5)/\mathfrak{S}_2^4$
25	78794979080474198016000000	4		$((\mathfrak{S}_5 \wr \mathfrak{K}_4 \wr \mathfrak{S}_5 \wr \mathfrak{S}_5)/\mathfrak{K}_4^4) \rtimes \mathfrak{S}_3$
26	26142282979403407520956416000000	2	(1.29)$\wr\mathfrak{S}_5$	$((\mathfrak{K}_4 \wr \mathfrak{S}_5) \rtimes \mathfrak{S}_3) \wr \mathfrak{S}_5$
27	23776267862016000000	6	(3.95)	$(\mathfrak{S}_5 \times \mathfrak{S}_4) \wr \mathfrak{S}_5$

Tabelle I.1: Tabelle der Automorphismengruppen für N=100, Teil 1 von 2

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
28	$252973643935090893898791046348 8*10^{12}$	4	(3.57)	$\mathfrak{S}_2 \wr \mathfrak{S}_5 \wr \mathfrak{S}_{10}$
29	$2007727332818181697609452748 8*10^{12}$	2	(3.130)	$\mathfrak{S}_2 \wr \mathfrak{S}_5 \wr \mathfrak{S}_5 \wr \mathfrak{S}_2$
30	$2676969777090908930145936998 4*10^{11}$	2	(3.131)	$\mathfrak{S}_2 \wr \mathfrak{S}_5 \wr \mathfrak{S}_2 \wr \mathfrak{S}_5$
31	$850151242013306321715795/$ $904060125609984*10^{11}$	4	(3.58)	$\mathfrak{S}_2 \wr \mathfrak{S}_{10} \wr \mathfrak{S}_5$
32	$541777714188473034889654890361020/$ $5332369017330865274880000000000000$	2	(1.21)	$\mathfrak{S}_2 \wr \mathfrak{S}_{25} \wr \mathfrak{S}_2$
33	$342432247025119762482464328952081859/$ $751186750537191988279156544634 88*10^{12}$	3	(1.19)	$\mathfrak{S}_2 \wr \mathfrak{S}_{50}$
zus				
1	$585996947339018123325 35/$ $6040109712486694912000000$	2	(1.20)	$\mathfrak{S}_2 \wr \mathfrak{S}_2 \wr \mathfrak{S}_{25}$
3	$201715146446013946920960 00000$	2		$(\mathfrak{K}_4 \wr \mathfrak{S}_5 \wr \mathfrak{S}_5) \rtimes \mathfrak{S}_3$
7	$784268489382102225628692480 00000000000000$	4	$\mathfrak{S}_2 \wr (3.75)$	$\mathfrak{S}_2 \wr ((\mathfrak{S}_2 \wr \mathfrak{S}_5 \wr \mathfrak{S}_5)/\mathfrak{S}_2^4)$
9	$531344526258316451072372/$ $4400375785062400000000000$	2	(3.76)	$(\mathfrak{S}_2 \wr \mathfrak{S}_{10} \wr \mathfrak{S}_5)/\mathfrak{S}_2^4$
	Anzahl Codes: 119			

Tabelle I.2: Tabelle der Automorphismengruppen für N=100, Teil 2 von 2

Nr.	Ordnung	Anz.	Formeltyp	Pr.-formel
1	$163632142352196034231928583502594534360467132/$ $513607642768427722997760000000000000000000000000$	4	(3.2)	$\mathfrak{S}_{11} \wr \mathfrak{S}_{11}$
	Anzahl Codes: 4			

Tabelle I.3: Tabelle der Automorphismengruppen für N=121

Nr.	Ordnung	Anz.	Formeltyp	Produktformel
1	$107748104850515247767931453982269921133 9499/$ $270048713888955191434343205514240483560 7159/$ $711977177088000000000000000000000000000000000$	4	(1.101)	$\mathfrak{S}_{25} \wr \mathfrak{S}_5$
2	$284851576559723767594740349717 70/$ $880000000000000000000000000000000$	4	(3.74)	$\mathfrak{S}_5 \wr \mathfrak{S}_5 \wr \mathfrak{S}_5$
3	$147971075370526184084807754244637258 651/$ $931770880000000000000000000000000000000$	4	(1.102)	$\mathfrak{S}_5 \wr \mathfrak{S}_{25}$
	Anzahl Codes: 12			

Tabelle I.4: Tabelle der Automorphismengruppen für N=125

Literaturverzeichnis

[1] Abdukhalikov, K. S., (1997). *Modular permutation representations of PSL(n,p)*. Sbornik Mathematics, Vol 188, pp. 1107-1117.

[2] Castagnoli, G., et al. (1991). *On Repeated-Rool Cyclic Codes*. IEEE Trans. on Info. Theory, Vol 37, No 2, pp. 337-342.

[3] Grunewald, Fritz (2004). *Vorlesung Kodierungstheorie SS2004*. Heinrich Heine Universität Düsseldorf

[4] Huppert, B. (1967). *Endliche Gruppen I*. Springer-Verlag, Berlin, Heidelberg, New York.

[5] L. A. Kaluznin / P. M. Beleckij / V. Z. Fejnberg (1987). *Kranzprodukte*. B.G. Teubner, Leipzig.

[6] Kantor, W. M. and McDonough, T. P. (1974). *On the Maximality of PSL(d+1,q),d* ≥ 2. J. London Math. Soc., Vol 8, p. 426.

[7] Liebeck, Martin W., Praeger, Cheryl E. and Saxl, Jan (1987). *The classification of the maximal subgroups of the finite symmetric and alternating groups*. J. Algebra, Vol 111, pp. 365-383.

[8] van Lint, J.H. (1999). *Introduction to Coding Theory*. Springer-Verlag, Berlin, Heidelberg, New York.

[9] van Lint, J.H. (1991). *Repeated-Rool Cyclic Codes*. IEEE Trans. on Info. Theory, Vol 37, No 2, pp. 343-345.

[10] Lütkebohmert, W. (2003). *Codierungstheorie*. Vieweg Verlag, Braunschweig/Wiesbaden.

[11] Meldrum, J.D.P. (1995). *Wreath products of groups and semigroups*. Longman Group Ltd., Essex, England .

[12] Peterson, P.P. (1967). *Prüfbare und korrigierbare Codes*. Oldenbourg Verlag, München.

[13] Phelps, K.T. (1985). *Every finite group is the automorphism group of some linear code*. Congr. Numer. **49** (1985), pp 139-141.

[14] Pless, V.S. and Huffman, W.C. (1998). *Handbook of Coding Theory*. Elsevier Science B.V., Amsterdam, Lausanne, New York, et al.

[15] Rotman, J. J. (1995). *An Introduction to the Theory of Groups, Fourth Edition*. Springer-Verlag, Berlin, Heidelberg, New York.

[16] MacWilliams, F.J. und Sloane, N.J.A (2003). *The Theory of Error-Correcting Codes*. North Holland, Amsterdam, London, New York, Tokyo.

[17] Zalesskii, A. E., and Suprunenko, I. D. (1990). *Permutation representations and a fragment of the decomposition matrix of symplectic and special linear groups over a finite field*. Siber. Math. J. 31 (1990), pp. 744-755.

Index

Die hier vorliegende Dissertation habe ich eigenständig und ohne unerlaubte Hilfe angefertigt. Die Dissertation wurde in der vorliegenden oder in ähnlicher Form noch bei keiner anderen Institution eingereicht. Ich habe bisher keine erfolglosen Promotionsversuche unternommen.

Düsseldorf, den 16.05.2007

Rolf Bienert