Bell inequalities and large-scale quantum networks

An inaugural dissertation

submitted in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

in the Faculty of Mathematics and Natural Sciences
at the Heinrich Heine University Düsseldorf

by

Michael Epping
from Arnsberg

Düsseldorf, January 2016

from the Institute for Theoretical Physics III
at the Heinrich Heine University Düsseldorf

Published by permission of the
Faculty of Mathematics and Natural Sciences at
Heinrich Heine University Düsseldorf

Supervisor: Prof. Dr. Dagmar Bruß
Co-supervisor: PD Dr. Hermann Kampermann

Date of the oral examination: 17.12.2015

Dedication

To my loving parents and siblings.

Acknowledgment

My thesis is based on research which was carried out in the quantum information group headed by my Ph.D. advisor Dagmar Bruß at the Heinrich-Heine University of Düsseldorf. I thank her for giving me the opportunity to join her team and for her continued support that I enjoyed during my Ph.D. studies. My research benefited greatly from her experience. I am also very grateful for the "off-topic" advice that helped me to understand how science works.

I thank all my co-authors. It was a pleasure to work with you. In particular Hermann Kampermann spent many hours in discussions with me: always pushing forward, identifying weak points in any argument and giving important input to my work.

I thank my colleagues for all the feedback they gave in the group seminar and other discussions and for the time they spent to answer my questions. In particular I gratefully acknowledge that Silvio Abruzzo and Sylvia Bratzik introduced me to the topic of quantum repeaters. Junyi Wu patiently answered all my questions on graph states and the stabilizer formalism and our common interest in error correction spurred me on without doubt. The discussions with Jochen Szangolies, in particular about Bell inequalities, each made me reconsider what I deemed obvious and helped me to gain a deeper understanding.

I very much enjoyed the meetings with the research group of Otfried Gühne at the University of Siegen. He, Costantino Budroni, Matthias Kleinmann, and Tobias Moroder gave important stimuli to my work by asking the right questions and giving many hints to relevant methods and literature.

Felix Bischof, Hermann Kampermann, and Jochen Szangolies gave valuable feedback on the manuscript of my thesis.

I express my deep gratitude to my family. I cannot imagine to have written this thesis without their love and support.

Finally I acknowledge financial support by the German Research Foundation (DFG) and the German Federal Minestry of Education and Research (BMBF).

Abstract

Deutsche Zusammenfassung unter der Englischen.

In the field of quantum information theory one investigates the properties of information carriers which are subject to the laws of quantum mechanics. The differences between quantum mechanics and the laws that govern macroscopic information carriers lead to new opportunities and challenges in information processing.
One of these differences is the entanglement of particles, which leads to strong correlations of measurement outcomes. This allows the violation of so-called Bell inequalities in quantum mechanics, which is impossible in "classical" theories. I investigated the possible amount of violation for an important class of Bell inequalities. In doing so I found a simple mathematical expression for an upper bound and studied the achievability of that bound. The approach provides a basic understanding of the considered Bell inequalities, which allows to construct new inequalities with interesting properties. In particular one can understand how Bell inequalities allow to bound the dimension of a quantum system. Changing a Bell inequality with invariant quantum value proved useful in optimizing them with respect to the violation.
The distribution of entangled systems across large distances is achieved by sending photons. However, since they are absorbed in long fibers, quantum repeater become necessary for distances larger than approximately 200 km. Several approaches to counter the losses are known. In the long term error correction codes are very promising. Here the information is encoded into many photons, such that some losses can be compensated. I contributed to the analysis of this approach by showing how it naturally generalizes to networks of quantum repeaters. The formalism of graph states is useful in this context. A complete performance analysis of a quantum repeater contains many sources of errors and their propagation inside the circuit. I extended this analysis compared to the literature. At the moment it is not clear which types of quantum repeaters will prevail. My comparison of different theoretical proposals helps towards answering this question.

In der Quanteninformationstheorie werden die Eigenschaften von Informationsträgern untersucht, die den Gesetzen der Quantenmechanik folgen. Die Unterschiede der Quantenmechanik gegenüber den Gesetzen, die die makroskopischen Informationsträger beherrschen, führen zu neuen Möglichkeiten, aber auch zu neuen Herausforderungen in der Manipulation von Information.
Ein solcher Unterschied ist die Verschränkung von Teilchen, die sich in besonders starken Korrelationen von Messergebnissen äußert. Dadurch ist es möglich, dass sogenannte Bell-Ungleichungen innerhalb der Quantenmechanik verletzt werden können, was in "klassischen" Theorien nicht möglich ist. Ich habe untersucht, wie stark diese Verletzung für eine wichtige Klasse von Bell-Ungleichungen sein kann. Dabei habe ich einen einfachen mathematischen Ausdruck gefunden, der eine obere Schranke liefert, und untersucht, wann diese Schranke erreicht werden kann. Der Ansatz liefert ein einfaches Verständnis der Bell-Ungleichungen, was die Konstruktion neuer Ungleichungen mit interessanten Eigenschaften ermöglicht. Insbesondere lassen sich Ungleichungen verstehen, die die Dimension eines Quantensystems eingrenzen können. Die Abänderung einer Bell-Ungleichung mit invariantem Quantenwert hat sich als vorteilhaft für die Optimierung von Bell-Ungleichungen bezüglich der Verletzung erwiesen.
Die Verteilung von verschränkten Systemen über größere Entfernungen erfolgt über das Senden von Lichtteilchen. Da diese jedoch von langen Glasfaserkabeln verschluckt werden, werden für Entfernungen ab etwa 200 km Quantensignalverstärker nötig. Um die Verluste auszugleichen gibt es verschiedene Ansätze. Langfristig sehr vielversprechend ist der Einsatz von Fehlerkorrekturcodes. Hier wird die Information in viele Lichtteilchen kodiert, sodass vereinzelte Verluste ausgeglichen werden können. Ich habe zur Analyse dieses Ansatzes beigetragen, indem ich gezeigt habe, wie er sich in natürlicher Weise auf Netzwerke von Signalverstärkern erweitern lässt. Dafür hat sich der Formalismus der sogenannten Graphenzustände als sehr nützlich erwiesen. Für eine möglichst vollständige Analyse der Leistung eines Signalverstärkers müssen sowohl Fehlerquellen bei der Informationsverarbeitung als auch die Fortpflanzung der Fehler im gesamten Schaltkreis berücksichtigt werden. Hier habe ich bestehende Ansätze erweitert. Zum jetzigen Zeitpunkt ist nicht klar, welche Arten von Signalverstärkern sich durchsetzen werden. Der von mir durchgeführte Vergleich mit verschiedenen theoretischen Vorschlägen für Quantensignalverstärker leistet einen Beitrag zur Beantwortung dieser Frage.

Contents

List of Figures

Preface

During the past century data processing has become a key technology of our society, which enhances almost all parts of our lives. And it will become even more important in the near future. This progress is driven by the development of more powerful computers - an impressive evolution which can be described by Moore's famous law [Moo65]. It states that the complexity of the most cost efficient integrated circuits grows exponentially. The industry is reaching 10 nm size for the gates and plans to approach less than two nanometers in 2025 [Com13]. However, it is clear that at some point this advancement of the technology will reach fundamental limits. Note that a silicon atom has an extent of approximately 0.2 nm. Thus data processing technology is approaching a regime where classical physics ceases to be a good description and quantum phenomena become important. One is thus forced to consider the laws of quantum theory in the context of computation.

The physical limits on data processing technology highlight that the concept of information depends on the physical theory, because it is necessarily stored in a physical system. One might argue that the reverse is true, as well. The aim of scientific theories is to predict perceptions, i.e. to describe how the information of an observer changes. These considerations indicate that physics and information theory are inextricably linked and motivate to shift classical information theory to a theory of quantum information, i.e. information subject to the laws of quantum mechanics instead of classical theories (like classical mechanics and electrodynamics). My thesis is situated in this relatively new but rapidly expanding field of physics.

There is positive motivation for research on quantum information. Richard Feynman noticed that classical computers (i.e. Turing machines) cannot efficiently simulate quantum systems, while a *quantum computer* can [Fey82]. This opened the field of quantum computation. Quantum information theory also provides other new possibilities compared to classical information theory, e.g. new cryptographic schemes, see Chapter 3. Quantum cryptography in networks of several parties separated by long distances of more than approximately 200 km is one main topic of this thesis.

Quantum theory has a reputation of being incomprehensible, because its phenomena are different from our everyday experience. One can hope that the more quantum technology reaches daily life, the more people will get used to its logic. This *non-classicality* of quantum theory is another emphasis of this thesis. It is particularly striking in the violation of Bell inequalities, see Chapter 2.

My thesis is structured as follows. Chapter 1 gives the mathematical foundation for the rest of the text, introducing in particular the concept of entanglement. Entangled states exhibit properties which (still) contradict common sense. Some

tools to highlight these properties are introduced in Chapter 2, while Chapter 3 focuses on quantum cryptography as an application that uses entanglement as a resource. In practice entanglement tends to be fragile and susceptible to disturbance. This necessitates error correction techniques, which are discussed in Chapter 4. Chapter 5 finally sketches how the error correction methods render large scale quantum networks possible. Please find a short summary of my results in Chapter 6.

Tu as voulu de l'algèbre, et tu en auras jusqu'au menton!
You wanted algebra, and now you shall have it over head and ears.

Jules Verne [Ver70, WMP04]

1 Foundations

This chapter introduces the notation and the mathematical concepts used later on. These are essentially the Hilbert space representation for the state space and entanglement as an important consequence thereof.

1.1 Bra-ket notation

All proofs and calculations of the present thesis, just like most of quantum information theory, take place in finite dimensional vector spaces, actually finite dimensional Hilbert spaces over the field $\mathbb{C}$ of complex numbers.

Definition 1 (Hilbert space)**.** *A Hilbert space $\mathcal{H}$ is a vector space supplemented by a scalar product, which is complete with respect to the norm induced by the scalar product.*

The bra-ket notation, also named Dirac notation after its famous inventor Paul Dirac, is a convenient, basis independent notation for vectors. The ket symbol $|\psi\rangle$ (read "ket ψ") denotes an element of a Hilbert space $\mathcal{H}$. Instead of ψ, arbitrary names, even pictograms, can be placed inside the ket. A bra $\langle\psi|$ can be defined as the complex conjugated transpose of the ket, i.e. $\langle\psi| = |\psi\rangle^\dagger$. The product of a bra and a ket forms the scalar product of the two vectors $\langle\psi||\phi\rangle = \langle\psi|\phi\rangle$. The names bra and ket originate from the bracket commonly used for the scalar product.
A common (coordinate free description of a) basis of the d-dimensional Hilbertspace $\mathcal{H}$ is denoted by $\{|0\rangle, |1\rangle, ..., |d-1\rangle\}$. One may associate the canonical basis of vectors with it, i.e. $|n\rangle = (\underbrace{0, ..., 0}_{n \text{ zeros}}, 1, \underbrace{0, ..., 0}_{d-n-1 \text{ zeros}})^T$.

1.2 Postulates of quantum mechanics

Motivating the mathematical structure of quantum theory is a difficult task and even subject of ongoing research (see also Section 2.3). As a starting point it

is convenient to accept the formalism and note that it seems to be justified by its success and simplicity. Following this rule the mathematical structure and its relation to physical phenomena can be introduced via postulates. Here only the discrete and finite dimensional case is discussed, because this is the only one of importance for the present thesis. The postulates for the continuous case are analogous.

(P1) The state of a physical system is represented by an element $|\psi\rangle$ of a Hilbert space $\mathcal{H}$ with length 1. This mapping is unique up to a complex phase $e^{i\varphi}$.

(P2) An observable on this system corresponds to a linear hermitian operator $\mathcal{A}$. The possible measurement outcomes lie in the spectrum of $\mathcal{A}$.

(P3) The probability to obtain an outcome a_i is given by $\langle\psi|P_i|\psi\rangle$, where P_i is the projector onto the eigenspace of the eigenvalue a_i. The state after the measurement is $\frac{P_i}{\langle\psi|P_i|\psi\rangle}|\psi\rangle$.

(P4) The state space $\mathcal{H}_{\mathrm{AB}}$ of a system composed of subsystems A and B with Hilbert spaces $\mathcal{H}_{\mathrm{A}}$ and $\mathcal{H}_{\mathrm{B}}$, respectively, is given by the tensor product $\mathcal{H}_{\mathrm{AB}} = \mathcal{H}_A \otimes \mathcal{H}_B$.

(P5) The state of a system evolves in time according to

$$|\psi(t)\rangle = U(t)|\psi(0)\rangle, \tag{1.1}$$

where the time evolution operator $U(t)$ is unitary.

The unitarity of the time evolution follows from the conserved normalization of the state $|\psi\rangle$, which is necessary due to postulate (P3). The relation between time evolution and Hamiltonian H of the system is given by the Schrödinger equation

$$\frac{\partial}{\partial t}|\psi(t)\rangle = -\frac{i}{\hbar}H(t)|\psi(t)\rangle. \tag{1.2}$$

1.3 The Qubit

The simplest non-trivial state space is a two-dimensional complex Hilbert space. A corresponding system is called a qubit, in analogy to the bit of classical information theory. The canonical basis of this Hilbert space, the so-called computational basis, will be denoted as $\{|0\rangle, |1\rangle\}$. In contrast to a bit the qubit has more than two possible states: it can be in coherent superpositions (linear combinations) of the basis states. Thus states of qubits have the form

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{1.3}$$

where $\alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1$. After fixing the arbitrary global phase the state $|\psi\rangle$ has two degrees of freedom. It can be written as

$$|\psi\rangle = \cos\left(\frac{\vartheta}{2}\right)|0\rangle + e^{i\varphi}\sin\left(\frac{\vartheta}{2}\right)|1\rangle \tag{1.4}$$

with two real angles φ and ϑ.
A general measurement on a qubit with outcomes -1 and $+1$ is given by the observable

$$\mathcal{A} = \vec{a} \cdot \vec{\sigma}, \tag{1.5}$$

where $\vec{a} \in \mathbb{R}^3$ has $|\vec{a}| = 1$ and $\vec{\sigma} = (X, Y, Z)^T$ is the vector of Pauli matrices

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \text{ and } Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{1.6}$$

The vector $\vec{a}$ can be described in a spherical coordinate system as

$$\vec{a} = \begin{pmatrix} \sin\vartheta' \cos\varphi' \\ \sin\vartheta' \sin\varphi' \\ \cos\vartheta' \end{pmatrix}. \tag{1.7}$$

One can easily verify that $|\psi\rangle$ is an eigenstate of $\mathcal{A}$ to the eigenvalue $+1$ for matching angles, i.e. $\varphi = \varphi'$ and $\vartheta = \vartheta'$. The vector $\vec{a}$ lies on the origin-centered unit sphere, which is called the Bloch-sphere in this context, see Figure 1.1. One can also mark the state $|\psi\rangle$ on the Bloch sphere at the position corresponding to the angles φ and ϑ. On the Bloch sphere the state

$$|\psi^\perp\rangle = \sin\left(\frac{\vartheta}{2}\right)|0\rangle - e^{i\varphi}\cos\left(\frac{\vartheta}{2}\right)|1\rangle, \tag{1.8}$$

which is orthogonal to $|\psi\rangle$, i.e. $\langle\psi^\perp|\psi\rangle = 0$, lies directly opposite to it. For matching angles, $|\psi^\perp\rangle$ is the eigenvector of $\mathcal{A}$ to the eigenvalue -1. The vector $\vec{a}$ will be called the measurement direction of $\mathcal{A}$. According to (P3) measurement of $\mathcal{A}$ may lead to the post-measurement state $|\psi\rangle$ or $|\psi^\perp\rangle$.
In analogy to a qubit, a system with d-dimensional Hilbert space is called a qudit.

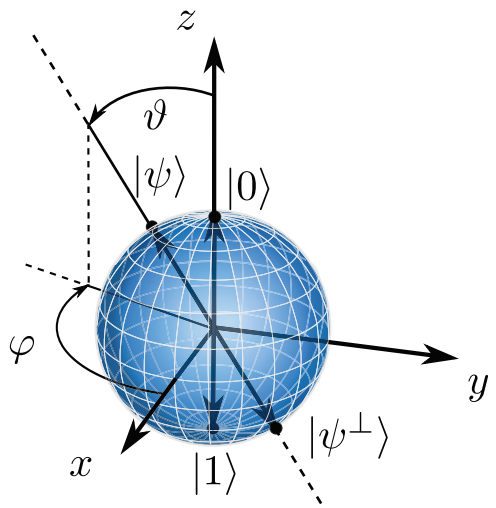


Figure 1.1: The state of a qubit can be marked on the Bloch sphere. The canonical basis states $|0\rangle$ and $|1\rangle$, the general state $|\psi\rangle$ (see Eq. (1.4)), and $|\psi^\perp\rangle$ (see Eq. (1.8)), which is orthogonal to $|\psi\rangle$, are represented.

1.4 Composite systems and entanglement

According to postulate (P4) the combined state space of a composite quantum system of two (and more) subsystems is formed via the tensor product. For two matrices $A = (A_{ij})_{ij}$ and $B = (B_{ij})_{ij}$ with dimensions $d_{A,1} \times d_{A,2}$ and $d_{B,1} \times d_{B,2}$ it reads

$$\begin{pmatrix} A_{11} & A_{21} & \dots \\ A_{21} & A_{22} & \\ \vdots & & \ddots \end{pmatrix} \otimes B = \begin{pmatrix} A_{11}B & A_{21}B & \dots \\ A_{21}B & A_{22}B & \\ \vdots & & \ddots \end{pmatrix}. \tag{1.9}$$

The resulting matrix has dimension $d_{A,1}d_{B,1} \times d_{A,2}d_{B,2}$.
Given two systems A and B with Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively, the state of the composite system AB is an element of $\mathcal{H}_A \otimes \mathcal{H}_B$. In general this state cannot be written as a tensor product of states on the subsystems. This remarkable fact leads to the following two important definitions.

Definition 2 (Separable states)**.** *A state* $|\psi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ *is* separable *if and only if it can be written in the form*

$$|\psi\rangle_{AB} = |a\rangle_A \otimes |b\rangle_B, \tag{1.10}$$

where $|a\rangle_A \in \mathcal{H}_A$ *and* $|b\rangle_B \in \mathcal{H}_B$*.*

Definition 3 (Entangled states)**.** *A state that is not separable is called* entangled*.*

Examples of separable states of a two-qubit system are $|0\rangle \otimes |0\rangle$, $|0\rangle \otimes |1\rangle$,$|1\rangle \otimes |0\rangle$ and $|1\rangle \otimes |1\rangle$. Often a shorter notation is used in which the tensor product is omitted and all labels are written inside a single ket, e.g. $|00\rangle$. Examples for entangled states are

$$\begin{aligned} |\phi^+\rangle =& \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), & |\phi^-\rangle =& \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \\ |\psi^+\rangle =& \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \quad \text{and} & |\psi^-\rangle =& \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle), \end{aligned} \tag{1.11}$$

which are usually called Bell states.

1.5 Mixed states

The measurement of pure quantum states which can be written as coherent superpositions of different eigenstates of the observable exhibits (true) randomness according to postulate (P3). For example the states

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \tag{1.12}$$

$$\text{and } |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{1.13}$$

when measured in the computational basis can be found in the state $|0\rangle$ or in the state $|1\rangle$, each with probability $\frac{1}{2}$. In contrast to an incoherent mixture of $|0\rangle$ and $|1\rangle$ with equal probability, the coherence in this superposition implies, that the two components can interfere, e.g. in the action of the Hadamard gate

$$H = \frac{1}{\sqrt{2}}\left(|+\rangle\langle 0| + |-\rangle\langle 1|\right) : \tag{1.14}$$

$$H|+\rangle = \frac{1}{2}\left(|0\rangle + |1\rangle + |0\rangle - |1\rangle\right) \tag{1.15}$$

$\downarrow$ Constructive interference in $|0\rangle$ and destructive interference in $|1\rangle$.

$$= |0\rangle. \tag{1.16}$$

Thus the state $|+\rangle$ is fundamentally different from producing the state $|0\rangle$ or $|1\rangle$ with probability $\frac{1}{2}$ and not knowing which of the two states is present. In many calculations it is also very convenient to have a description of this second type of statistical mixture, which is the *density matrix*.

Definition 4 (Density matrix)**.** *The operator*

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| \tag{1.17}$$

describes a statistical mixture of states $|\psi_i\rangle$, $i \in \mathbb{N}$, which are distributed according to the probability distribution p_i. The probabilities sum up to one, i.e. $\sum_i p_i = 1$.

The density matrix of the mixed state in the example in which $|0\rangle$ or $|1\rangle$ are produced with equal probability reads

$$\rho = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) \tag{1.18}$$

and is proportional to the identity operator $\mathbb{1}$. States of this form are called completely mixed states. In contrast to Eq. (1.18) the density matrix of the state in Eq. (1.12) reads

$$|+\rangle\langle +| = \frac{1}{2}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| + |1\rangle\langle 1|), \tag{1.19}$$

which again shows that these two states are different.
The ignorance of the present state can have different causes. An important reason, the application of experimentally imperfect gates, which leads to noisy states, is discussed in Section 4.1. In this case the exact time evolution of the quantum state is not known. Furthermore the ignorance of the state can be caused by the lack of knowledge of a measurement outcome. In particular, the state of one subsystem in an entangled state may be described by a mixed state. Mathematically this reduced state is obtained using the partial trace.

Definition 5 (Partial trace)**.** *The partial trace over system B of the density matrix ρ_{AB} on the composite system of A and B is a density matrix acting on $\mathcal{H}_A$ given by*

$$\mathrm{tr}_B\, \rho_{AB} = \sum_{i,j=1}^{d_A} \sum_{k=1}^{d_B} \langle i|_A \langle k|_B \rho_{AB} |j\rangle_A |k\rangle_B |i\rangle_A \langle j|_A, \tag{1.20}$$

where d_A and d_B are the dimensions of $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively.

Sometimes, in particular for pencil and paper calculations, the short form

$$\mathrm{tr}_B\, \rho_{AB} = \sum_{k=1}^{d_B} \langle k|_B \rho_{AB} |k\rangle_B \tag{1.21}$$

is more convenient.
Separability and entanglement of a mixed state is defined via a decomposition into pure states.

Definition 6. *A mixed quantum state given by its density matrix ρ is called separable, if and only if there exists a decomposition*

$$\rho = \sum_i p_i |\phi_{A,i}\rangle|\phi_{B,i}\rangle\langle\phi_{A,i}|\langle\phi_{B,i}| \tag{1.22}$$

into an ensemble of pure separable states $|\phi_{A,i}\rangle|\phi_{B,i}\rangle$ (product states).

And, analogously to pure states, a mixed state is called entangled if it is not separable.

1.6 Quantum operations

The state evolution in measurements and in time given by postulates (P3) and (P5) exhaustively describe our possibilities to manipulate a quantum system. However this description may not be useful when one is only interested in parts of a large quantum system, e.g. a single particle which is interacting with its environment. The evolution of a subsystem (usually) can be modeled by a quantum operation [NC00], which maps the state ρ of the subsystem to

$$\varepsilon(\rho) = \sum_k E_k \rho E_k^\dagger, \tag{1.23}$$

with

$$\sum_k E_k^\dagger E_k = \mathbb{1}. \tag{1.24}$$

This is the operator-sum representation of the quantum operation. Note that the choice of operators E_k is not unique. The quantum operation is also called a *channel*, depending on the context. Other tools to calculate the evolution of "open quantum systems" interacting with the environment are known, too, e.g. the master equation approach, see [NC00].

1.7 Measures of Entanglement and the maximally entangled state

The quantification of entanglement is a subfield of quantum information theory. A *measure of entanglement* is a function that maps states to non-negative real numbers with the following properties. It is required to be invariant under local basis transformations, non-increasing under local operations and classical communication (LOCC) and to vanish only on separable states.
The entropy of the reduced state $\mathrm{tr}_B\,\rho_{AB}$ is a measure for the entanglement of the composite system AB in a *pure* state $\rho_{AB} = |\psi\rangle_{AB}\langle\psi|_{AB}$.

Definition 7 (Entropy of entanglement)**.** *The entropy of entanglement in a pure state ρ_{AB} with respect to the separation $A|B$ is given by the von-Neumann entropy of the reduced state $\rho_A = \mathrm{tr}_B\,\rho_{AB}$ of one subsystem,*

$$S(\rho_A) = -\,\mathrm{tr}[\rho_A \log(\rho_A)]. \tag{1.25}$$

With this definition one can easily see, that the two-qudit state

$$|\phi_D^+\rangle = \frac{1}{\sqrt{D}} \sum_{k=0}^{D-1} |kk\rangle \tag{1.26}$$

is *maximally entangled*, because the reduced state of one subsystem

$$\begin{aligned} \mathrm{tr}_B\, |\phi_D^+\rangle\langle\phi_D^+| =& \frac{1}{D} \sum_k \sum_{l,m} \langle k|_B |ll\rangle \langle mm||k\rangle_B & (1.27) \\ & \downarrow \text{ use orthogonality } \langle i|j\rangle = \delta_{ij} \\ =& \frac{\mathbb{1}}{D} & (1.28) \end{aligned}$$

has maximal von-Neumann entropy $S(\rho) = \log_2 D$.
Entanglement measures for mixed states need to take into account, that the decomposition of a mixed state into pure states is not unique. The following two examples are relevant to Appendix B. For the best separable approximation one decomposes the state into a sum of a separable state and an entangled state, such that the weight of the separable state is maximal [LS98]. This weight thus measures the "similarity" to a separable state. The robustness of entanglement is the minimal amount of separable states that needs to be mixed into the state to make it separable [VT99]. Intuitively it is the robustness against local noise. See [HHHH09] for a review on entanglement measures.
Entangled states exhibit interesting properties. The strong correlations they, and in particular $|\phi_D^+\rangle$ of Eq. (1.26), show are discussed in the following chapter.

While we have thus shown that the wave function does not provide a complete description of the physical reality, we left open the question whether such a description exists. We believe, however, that such a description is possible.

A. Einstein, B. Podolsky, and N. Rosen [EPR35]

2

The "non-classicality" of quantum theory

Albert Einstein, Boris Podolsky and Nathan Rosen (EPR) showed that quantum theory cannot be complete, in the sense that not every quantity that can be predicted with certainty has a counterpart in the theory [EPR35]. This becomes apparent in their thought experiment. They consider two particles which are entangled in their position and momentum state. From the wave function description of the state they conclude, that measurement of the position (the momentum) of the first particle allows to predict the position (the momentum) of the second particle with certainty. As there is no interaction, both position and momentum should be elements of physical reality. However quantum theory does not contain variables for the outcomes of the position and momentum that are to be revealed by the corresponding measurement. The position and momentum of a quantum even fulfill Heisenberg's uncertainty relation and thus it is impossible to simultaneously assign precise values to these two quantities according to quantum theory, which therefore cannot be complete. EPR conjectured, however, that a completion which adds the missing quantities should be possible.
Such a *local hidden variable theory* fulfills the following three axioms.

(LHV1) *Locality.* No action affects distant systems outside the light cone.

(LHV2) *Realism.* Properties of objects have definite values independent of measurements.

(LHV3) *Free will.* It is possible to freely choose between different measurements.

2.1 Bell's theorem

John Bell was able to show, that experimentally testable predictions of quantum theory contradict (basically) these three assumptions [Bel64]. Thus there is a conflict between local hidden variable theories and quantum mechanics and no completion in the sense of EPR is possible.
The method Bell used to show the discrepancy between quantum theory and local

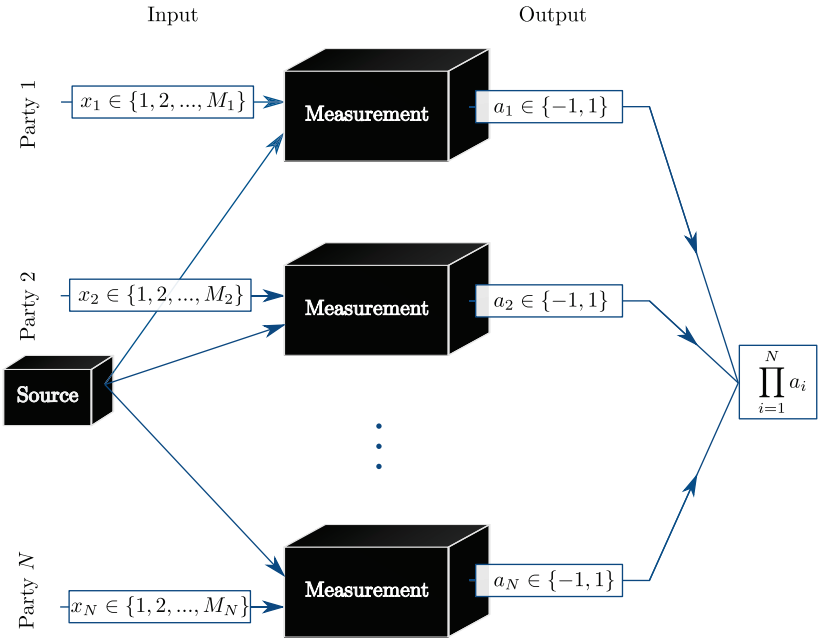


Figure 2.1: A schematic of the setup of the Bell test experiment described in the text. There are N parties labeled from 1 to N. Each party i (randomly) chooses the measurement setting x_i and performs the corresponding measurement. The outcome of the measurement is denoted by a_i and takes one of the two possible values -1 and 1. The outcome of the joint measurement is the product of the individual outcomes.

hidden variable theories are inequalities on measurable quantities, which must hold in all local hidden variable theories but which are violated in quantum theory. Such inequalities are called Bell inequalities.

2.1.1 A Bell test experiment

The experiment is subdivided into different spatially separated areas: the source and N parties, where $N \geq 2$, see Figure 2.1. The parties are labeled $i = 1, 2, ..., N$. Each party i possesses one measurement apparatus. The party i can choose between $M_i \in \mathbb{N}$ measurement settings. This setting is an input to the measurement apparatus. The source repeatedly produces a system and distributes its subsystems to each party, which causes each of the measurement apparatuses to output the measurement outcome a_i. In the present context the possible outputs a_i are restricted to the set $\{-1, 1\}$. The outcome of the joint measurement is the product of the individual outcomes, i.e. $\prod_i a_i = \pm 1$. Many repetitions of this procedure allow the estimation of the expectation value of the joint observable in an arbitrary setting $(x_1, x_2, ..., x_N)$. It is denoted by $E(x_1, x_2, ..., x_N)$.

2.1.2 CHSH type Bell inequalities

One can now form arbitrary linear combinations of these expectation values $E(x_1, x_2, ..., x_N)$ with real coefficients $g_{x_1, x_2, ..., x_N}$, i.e.

$$\sum_{x_1=1}^{M_1}\sum_{x_2=1}^{M_2}...\sum_{x_N=1}^{M_N} g_{x_1,x_2,...,x_N}E(x_1,x_2,...,x_N). \tag{2.1}$$

In a classical theory, i.e. a local and realistic theory (with free will), the measurement outcomes are probabilistic functions of the *local* settings. Any hidden variable model with shared randomness is a probability distribution over deterministic models. Thus the maximum of Eq. (2.1) over all classical theories is obtained by a deterministic strategy [BRSd10], i.e. the maximum can be calculated by maximizing over all deterministic functions $a_i(x_i)$,

$$B(g) = \max_{a_i(x_i)=\pm 1}\sum_{x_1=1}^{M_1}\sum_{x_2=1}^{M_2}...\sum_{x_N=1}^{M_N} g_{x_1,x_2,...,x_N}\prod_{i=1}^{N}a_i(x_i). \tag{2.2}$$

If there exists a classical theory that gives an adequate description of the Bell test experiment, then the experimentally obtained expectation values $E(x_1,...,x_N)$ are bounded by

$$\sum_{x_1=1}^{M_1}\sum_{x_2=1}^{M_2}...\sum_{x_N=1}^{M_N} g_{x_1,x_2,...,x_N}E(x_1,x_2,...,x_N) \leq B(g). \tag{2.3}$$

The inequality (2.3) is called a CHSH type Bell inequality. The name originates from the most prominent member of this class of inequalities, the Clauser-Horne-Shimony-Holt (CHSH) inequality [CHSH69] that is discussed in Section 2.1.3. The prediction of quantum theory for a state given by its density matrix ρ

$$E(x_1,x_2,...,x_N) = \left\langle \bigotimes_{i=1}^{N}\mathcal{A}_i(x_i)\right\rangle \tag{2.4}$$

$$= \mathrm{tr}\left(\bigotimes_{i=1}^{N}\mathcal{A}_i(x_i)\rho\right) \tag{2.5}$$

may violate the inequality 2.3. Here $\mathcal{A}_i$ is the observable of party i (with spectrum in $[-1,1]$) in the setting x_i. Other examples can be found in [BC90, Mer90].

2.1.3 The CHSH inequality

The most famous Bell inequality is the one derived by John Clauser, Michael Horne, Abner Shimony and Richard Holt in 1969 [CHSH69]. It applies to a bipartite ($N = 2$) Bell test experiment with two dichotomic observables per party ($M_1 = M_2 = 2$). It is given by Eq. (2.3) with coefficients

$$g^{\mathrm{CHSH}} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{2.6}$$

and bound $B(g^{\mathrm{CHSH}}) = 2$, i.e.

$$E(1,1) + E(2,1) + E(1,2) - E(2,2) \leq 2. \tag{2.7}$$

For a system in the state $|\phi^+\rangle$ (see Eq. (1.11)) and observables $\mathcal{A}_i(x_i)$ with

$$\begin{aligned} \mathcal{A}_1(1) &= X, & \mathcal{A}_2(1) &= \tfrac{1}{\sqrt{2}}(X+Z), \\ \mathcal{A}_1(2) &= Z, \text{ and } & \mathcal{A}_2(2) &= \tfrac{1}{\sqrt{2}}(X-Z), \end{aligned} \tag{2.8}$$

where X and Z are Pauli matrices (see Eq. (1.6)), the quantum prediction of the CHSH inequality is $2\sqrt{2} \approx 2.82843$, which is greater than the classical bound 2.

2.1.4 On experimental implementations

By now there is very strong experimental evidence that the predictions of quantum theory are correct, i.e. local hidden variable theories are ruled out [AGR82, WJS+98, RKM+01, HBD+15, GVW+15, SMSC+15]. In other words "nature" does not obey at least one of locality, realism and free will. Several loopholes made improved experiments necessary [Lar14].
Bell test experiments can be implemented in very different physical systems. First experiments used the polarization entanglement of photons emitted in a calcium cascade [FC72, AGR81, AGR82]. Then parametric down-conversion sources with higher brightness were used [SA88, TBG+98, TBZG98, WJS+98, SBvH+08, GMR+13]. Bell inequalities have also been violated in trapped ion systems [RKM+01], where very high detection efficiencies compared to the photonic setup are possible. In [AWB+09] a Bell inequality has been violated in a solid-state system (Josephson phase qubits). Also multipartite Bell inequalities ($N > 2$) have been violated in experiment [PBD+00].

2.1.5 Other types of Bell inequalities

The CHSH inequality (Eq. (2.7)) is the most famous Bell inequality and used in most cases. However, many more Bell inequalities with interesting properties are known, see also Section 2.3.2. In principle any real-valued expression that is bounded in a LHV model can be used to derive a Bell inequality (which, however, might not be violated in quantum theory).
The CHSH-type Bell inequalities contain the expectation values of the correlation measurements (i.e. the product of the ± 1 outcomes). A more general approach is to directly use the probabilities $p(x_1, x_2)$ of the measurement outcomes. An important example is the CH74 inequality [CHSH69, CH74], named after Clauser and Horne,

$$-1 \leq \frac{p(1,1) - p(1,2) + p(2,1) + p(2,2) - p(2,\mathbb{1}) - p(\mathbb{1},1)}{p(\mathbb{1},\mathbb{1})} \leq 0, \tag{2.9}$$

where the argument contains the measurement settings and the symbol $\mathbb{1}$ is used to denote a measurement of identity, e.g. absence of the polarization analyzers. Note that $p(\mathbb{1},\mathbb{1})$ is not 1 due to non-ideal detector efficiency. In contrast to the CHSH type Bell inequalities, the lower and upper bounds of CH type Bell inequalities are not symmetric in general.
A Bell inequality does not need to be linear in the outcome probabilities, see for example [WW01].

2.2 Communication Complexity

In addition to their relevance for the foundations of quantum mechanics, several intriguing applications of Bell inequalities are known. One example is the application to communication complexity [Yao79]. A standard problem in this context can be described as follows. N parties cooperate in order to calculate a function $f(x_1, x_2, ..., x_N)$, where each party i has only access to the input string x_i. What is the minimal amount of communication necessary for this distributed computation? Or similarly, if the parties are restricted to a given amount of communication, what is the maximal probability of success? In quantum communication complexity one compares the classical success probability to the case where the parties are allowed to share entangled quantum states.
A special case is the function $f(y_1, y_2, ..., y_N, x_1, x_2, ..., x_N) = \prod_i y_i \operatorname{sign}(g_{x_1,x_2,...,x_N})$, where the inputs $y_i \in \{-1, 1\}$ are equally distributed and the inputs x_i are distributed according to the probability distribution

$$Q(x_1, x_2, ..., x_N) = \frac{|g_{x_1,x_2,...,x_N}|}{\sum_{\tilde{x}_1,\tilde{x}_2,...,\tilde{x}_N} |g_{\tilde{x}_1,\tilde{x}_2,...,\tilde{x}_N}|}. \tag{2.10}$$

The classical and quantum success probability of correctly computing the value of f is directly related to the classical and quantum value of the CHSH type Bell inequality given by coefficients $g_{x_1,x_2,...,x_N}$ [BZPZ04, Epp12], respectively, see also Appendix A. This way any CHSH type Bell inequality is linked to a corresponding communication complexity task. It holds that the greater the amount of violation of the Bell inequality the larger the quantum advantage.

2.3 Tsirelson's bound

In communication complexity and other applications of Bell inequalities, the violation is directly linked to the benefit of sharing entangled resources. Thus the question "What is the maximal violation of a Bell inequality?" naturally arises. For a given Bell inequality this leads to the derivation of bounds on its quantum value. Such a bound is named *Tsirelson bound* after the Russian-Israeli mathematician Boris Tsirelson, who derived the bound $T(g^{\mathrm{CHSH}}) = 2\sqrt{2}$ for the CHSH inequality [Tsi80, Tsi93]. In analogy to Eq. (2.2) it is defined (for CHSH type Bell inequalities) as

$$T(g) = \max_{\mathcal{A},\rho} \sum_{x_1=1}^{M_1} \sum_{x_2=1}^{M_2} ... \sum_{x_N=1}^{M_N} g_{x_1,x_2,...,x_N} \operatorname{tr}\left(\rho \bigotimes_{i=1}^{N} \mathcal{A}_i(x_i)\right), \tag{2.11}$$

where now the maximization is performed over the observables $\mathcal{A}_i(x_i)$ and the state given by its density matrix ρ. Note that the dimension of the state is not restricted. As the problem of understanding the strength of correlations in quantum theory is both of fundamental and practical relevance, several different approaches to calculating the Tsirelson bound T have been developed. The principle of information causality [ABPS09, PPK$^+$09, GWAN11], macroscopic reality [NW09], uncertainty principles [OW10], the exclusivity principle [Cab13] and semidefinite programming approaches [Weh06, NPA07, NPA08, DLTW08] should be mentioned. My

approach pursued in [EKB13] is related to the semidefinite programming approach of [Weh06], see Appendix C, D, and E.
There is a close relation between the expectation value of quantum observables and the scalar product of real vectors. Tsirelson used this relation amongst others to prove the Tsirelson bound of the CHSH inequality. The parts of his theorem most relevant to this thesis are:

Theorem 1 (Tsirelson's Theorem [Tsi80, Weh06])**.** *Let $A_1, ..., A_m$ and $B_1, ..., B_n$ be observables with eigenvalues in the interval $[-1, 1]$. Then for any state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ and for all $k = 1, .., m$ and $l = 1, ..., n$ there exist real unit vectors $\vec{v}_1, ..., \vec{v}_m, \vec{w}_1, ..., \vec{w}_n \in \mathbb{R}^{m+n}$ such that*

$$\langle\psi|A_k \otimes B_l|\psi\rangle = \vec{v}_k^T \vec{w}_l. \tag{2.12}$$

Conversely, let $\vec{v}_k, \vec{w}_l \in \mathbb{R}^d$ be real unit vectors. Let $|\phi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ be any maximally entangled state where $D = \dim(\mathcal{H}_A) = \dim(\mathcal{H}_B) = 2^{\lceil \frac{d}{2} \rceil}$. Then for all k, l there exist observables A_k on $\mathcal{H}_A$ and B_l on $\mathcal{H}_B$ with eigenvalues ± 1 such that

$$\vec{v}_k^T \vec{w}_l = \langle\phi|A_k \otimes B_l|\phi\rangle \tag{2.13}$$

2.3.1 Singular Value Decomposition

The Tsirelson bound of [EKB13], see Appendix C, is based on the singular value decomposition (SVD) of matrices - a standard tool of linear algebra similar to the eigenvalue decomposition [GVL13]. Any matrix g can be decomposed into the product of a unitary matrix V, a diagonal matrix S and another unitary matrix $W^\dagger$, i.e.

$$g = VSW^\dagger. \tag{2.14}$$

If g has dimension $M_1 \times M_2$, then V has dimension $M_1 \times M_1$, S has dimension $M_1 \times M_2$ and W has dimension $M_2 \times M_2$. For real matrices g, V and W can be chosen real, too, which implies that they are orthogonal matrices and Eq. (2.14) simplifies to $g = VSW^T$. The matrix columns of V are called left singular vectors and the columns of W right singular vectors. The entries on the diagonal of S are called singular values. It is an usual convention to order the singular values in non-increasing order, i.e. $S_{1,1} \geq S_{2,2} \geq S_{3,3} \geq ... \geq S_{\min\{M_1,M_2\},\min\{M_1,M_2\}}$.
In some applications the SVD can be used to approximate a matrix, which is achieved by neglecting the parts of the SVD associated with small singular values. This concept is called a truncated singular value decomposition [GVL13].

2.3.2 Dimension Witnesses

Similar to the local hidden variable bound (see Eq. (2.2)) or the Tsirelson bound (see Eq. (2.11) of a Bell inequality), one can calculate the maximal value of the same (or any) expression for all quantum states of dimension smaller or equal to some value $D \in \mathbb{N}$, i.e.

$$T'_D(g) = \max_{\mathcal{A}, \rho \in S(\mathcal{H}_D)} \sum_{x_1=1}^{M_1} \sum_{x_2=1}^{M_2} ... \sum_{x_N=1}^{M_N} g_{x_1,x_2,...,x_N} \operatorname{tr}\left(\rho \bigotimes_{i=1}^{N} \mathcal{A}_i(x_i)\right), \tag{2.15}$$

where $S(\mathcal{H}_D)$ is the set of $(D \times D)$-dimensional density matrices. The inequality

$$\sum_{x_1=1}^{M_1} \sum_{x_2=1}^{M_2} \dots \sum_{x_N=1}^{M_N} g_{x_1,x_2,\dots,x_N} \operatorname{tr}\left(\rho \bigotimes_{i=1}^{N} \mathcal{A}_i(x_i)\right) \leq {T'}_D(g) \tag{2.16}$$

is a dimension witness: A violation of this inequality in some experiment witnesses that the measured quantum system had a dimension greater than D. This reasoning does not require knowledge of the source or the experimentally performed measurements, i.e. the dimension witness is *device independent*. Previous work on dimension witnesses includes [BPA+08, PGWP+08, WCD08, WPG09, GBHA10, BNV13].
In the present context and in the bipartite case it is more convenient to witness the dimension d' of the measurement directions. The two quantities D and d' are related, see Appendix C. The corresponding bound can be defined as

$$T_{d'}(g) = \max_{\vec{v}_{x_1} \in \mathbb{R}^{d'}, ||\vec{v}_{x_1}||=1} \sum_{x_2=1}^{M_2} \left|\left| \sum_{x_1=1}^{M_1} g_{x_1,x_2} \vec{v}_{x_1} \right|\right|, \tag{2.17}$$

see also Appendix D. I described, together with my co-authors, in [EKB13], how it can be understood from the singular value decomposition, also geometrically, whether a Bell inequality given by coefficients g is a d'-dimension witness, i.e. whether $T_{d'-1} < T_{d'}$, see Appendix C.

2.4 Entanglement Witnesses

Entanglement witnesses are another tool to verify entanglement [GT09] of a quantum state. The idea is similar to Bell inequalities: Here the set over which one maximizes the value of some expression to get the corresponding bound is the set of all separable states. In this context the dimension of the system is a fixed and known value. In the simplest case the witness is given by a single observable.

Definition 8 (Entanglement witness)**.** *An entanglement witness W is an observable that fulfills*

$$\langle W \rangle \geq 0 \text{ for all separable states} \tag{2.18}$$

$$\text{while } \langle W \rangle < 0 \text{ for some entangled state } \rho_{\text{ent.}}. \tag{2.19}$$

It detects the entanglement of the state $\rho_{\text{ent.}}$ (amongst others).

When constructed appropriately, the expectation value of an entanglement witness can also lower bound the amount of entanglement in the measured system according to some measure of entanglement, e.g. as obtained from the *best separable approximation* [LS98] or the *robustness of entanglement* [VT99, Ste03]. In some cases even macroscopic observables can be used as an entanglement witness, e.g. observables related to the cross-section in neutron scattering from magnetic materials, see Appendix A.

If you want to keep a secret, you must also hide it from yourself.
George Orwell [Orw49]

3 Quantum cryptography

Given the strong correlations exhibited by measurements on an entangled quantum system, one might be tempted to think of ways to harness this phenomenon for non-local effects. In particular it might not be obvious why entanglement itself does not allow for signalling, i.e. the transmission of information, which would be secret to any adversary. Because the entangled state could be shared in advance, before deciding on which information to send, signalling by means of entanglement would be faster than light. But this is not possible in quantum theory. Theories which do not allow for faster than light communication are called *non-signalling*. A short calculation shows that no quantum operation that acts only on one subsystem can have measureable effects to another subsystem, because the reduced state is invariant:

$$\operatorname{tr}_B \rho'_{AB} = \operatorname{tr}_B \left(\sum_l (\mathbb{1} \otimes E_l) \rho_{AB} (\mathbb{1} \otimes E_l^\dagger) \right) \tag{3.1}$$

$$\downarrow \text{ insert partial trace, see Eq. (1.20)}$$

$$= \sum_{ij} \sum_l \operatorname{tr} \left(E_l \langle i|_A \rho_{AB} |j\rangle_A E_l^\dagger \right) |i\rangle_A \langle j|_A \tag{3.2}$$

$$\downarrow \text{ cyclically permute under the trace, use linearity of the trace}$$

$$= \sum_{ij} \operatorname{tr} \left(\langle i|_A \rho_{AB} |j\rangle_A \sum_l E_l^\dagger E_l \right) |i\rangle_A \langle j|_A \tag{3.3}$$

$$\downarrow \text{ completeness relation of the quantum operation}$$

$$= \sum_{ij} \operatorname{tr} \left(\langle i|_A \rho_{AB} |j\rangle_A \right) |i\rangle_A \langle j|_A = \operatorname{tr}_B \rho_{AB}. \tag{3.4}$$

In other words, the quantum theory is non-signaling and local in the sense of Axiom (LHV1).

3.1 No-Cloning Theorem

A very simple but central theorem of quantum information theory is the No-Cloning Theorem. It is closely related to quantum theory being non-signaling. Suppose it were possible to copy an arbitrary unknown quantum state. Then let two parties, Alice and Bob, share the singlet state $|\psi^-\rangle$. This state exhibits perfectly anti-correlated outcomes whenever Alice and Bob measure in the same basis. Alice now measures in the X-basis to send a 0 and in the Z-basis to send a 1. Bob's state is projected onto $|+\rangle$ or $|-\rangle$ for an X-measurement of Alice or $|0\rangle$ or $|1\rangle$ for a Z-measurement of Alice. If Bob is in possession of a quantum copier, then he can distinguish the two cases, e.g. by measuring half of his copies in the X-basis and the other half in the Z-basis: The measurements in the same basis are all equal (to minus Alice's outcome) and the other ones are equally distributed.

Theorem 2 (No-Cloning Theorem)**.** *It is impossible to clone an arbitrary unknown quantum state perfectly.*

Proof. As the quantum copier should be implemented by a physical process, it can, according to the postulate (P5), be described by a unitary operation U. The initial state of the target qubit and the one of any third ancillary system is independent of the sample qubit and denoted by $|0\rangle$ of the respective Hilbert space. Suppose U can clone $|\psi\rangle$ and $|\varphi\rangle$ with $\langle\varphi|\psi\rangle \neq 0$ and $|\psi\rangle \neq |\varphi\rangle$, i.e.

$$U|\varphi\rangle|0\rangle|0\rangle = |\varphi\rangle|\varphi\rangle|a\rangle \tag{3.5}$$

$$\text{and } U|\psi\rangle|0\rangle|0\rangle = |\psi\rangle|\psi\rangle|a'\rangle, \tag{3.6}$$

with arbitrary states $|a\rangle$ and $|a'\rangle$ on the ancilla. Then:

$$\begin{aligned}
1 =& \frac{|(\langle\varphi|\langle 0|\langle 0|)(|\psi\rangle|0\rangle|0\rangle)|}{|\langle\varphi|\psi\rangle|} \\
&\downarrow \text{Unitarity of } U \\
=& \frac{|(\langle\varphi|\langle 0|\langle 0|)U^\dagger U(|\psi\rangle|0\rangle|0\rangle)|}{|\langle\varphi|\psi\rangle|} \\
&\downarrow \text{Apply cloning (to the left and the right)} \\
=& |\langle\varphi|\psi\rangle||\langle a|a'\rangle| \\
&\downarrow \text{with } |\langle\varphi|\psi\rangle| < 1 \text{ as } |\varphi\rangle \neq |\psi\rangle \text{ and } |\langle a|a'\rangle| \leq 1 \\
<& 1 \qquad \lightning
\end{aligned}$$

□

The no-cloning theorem implies security against eavesdroppers in a cryptographic setting: Alice wants to send a private message to Bob while an adversary Eve is eavesdropping on the communication line, see Figure 3.1. The main idea here is that Eve cannot perfectly distinguish the transmitted states due to the no-cloning theorem (Theorem 2). Any attempt to eavesdrop on the line will necessarily disturb the signal. The same holds for Bob, of course, but *after* the transmission Alice and Bob can agree upon a subset on which Bob performed measurements in the appropriate bases by chance.

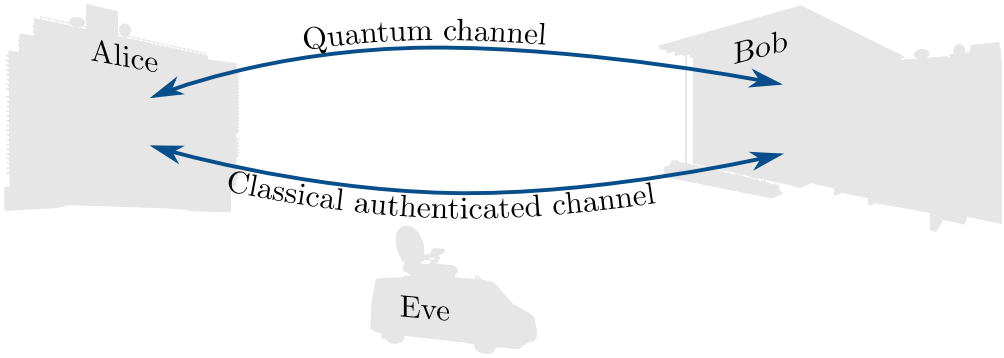


Figure 3.1: The typical situation in quantum cryptography: Alice and Bob communicate over a quantum channel and an authenticated classical channel, such that Alice can send a secret message to Bob without exposing it to the eavesdropper Eve. Protocols by which they can achieve this aim are described in the main text.

3.2 The One-Time-Pad encryption

In quantum cryptography one usually employs the One-Time-Pad encryption, which is also called Vernam cypher, after Gilbert Vernam who described the idea in 1918 and developed it together with Joseph Mauborgne [Sin99]. The text is encrypted by adding (modulo the alphabet size) a random key of the same length to it. The receiver subtracts the key to recover the original message. See Table 3.1 for an example. The cipher is secure if the eavesdropper does not know the ran-

Table 3.1: Example for the One-Time-Pad encryption.

$$
\begin{array}{ll}
 & 010000010101100011000111 \text{ (message “HELLO”)} \\
\oplus & 010011111111110110010101 1 \text{ (key “I?!YK”)} \\
\hline
= & 000011101010010101010010 0 \text{ (ciphertext “AZRUD”)}
\end{array}
$$

$$\Big\downarrow \text{ transmission}$$

$$
\begin{array}{ll}
 & 000011101010010101010010 0 \text{ (ciphertext “AZRUD”)} \\
\oplus & 010011111111110110010101 1 \text{ (key “I?!YK”)} \\
\hline
= & 010000010101100011000111 1 \text{ (message “HELLO”)}
\end{array}
$$

dom key. Quantum key distribution aims at distributing such random keys in a secure way.

3.3 The BB84 protocol

A quantum protocol to create a secret key shared by two parties Alice and Bob is the BB84 protocol [BB84], where the two B's stand for Bennett and Brassard, its two inventors. The protocol can be summarized by the following steps [NC00].

1. Alice generates L random data bits $a = (a_1, a_2, ..., a_L)$ as well as L random bits $b = (b_1, b_2, ..., b_L)$ denoting the basis (X or Z).

2. Alice transmits the state
$$|\psi\rangle = \bigotimes_{k=1}^{L} |\psi_{a_k b_k}\rangle \tag{3.7}$$
with
$$|\psi_{00}\rangle = |0\rangle, \tag{3.8}$$
$$|\psi_{10}\rangle = |1\rangle, \tag{3.9}$$
$$|\psi_{01}\rangle = |+\rangle, \tag{3.10}$$
$$\text{and } |\psi_{11}\rangle = |-\rangle. \tag{3.11}$$

3. Bob generates L random bits $b' = (b'_1, b'_2, ..., b'_L)$ and measures in the corresponding bases. The outcomes are denoted a'. He announces reception of the signal.

4. Alice announces b.

5. Alice and Bob discard the data corresponding to measurements where $b_i \neq b'_i$ (sifting).

6. Alice and Bob publicly compare a subset of their data a and a' to check for the disturbance of an eavesdropper. The estimated *error rates* in the X and Z basis are denoted e_X and e_Z, respectively. The remaining data is the *raw key*.

7. The data is post-processed to eliminate errors and reduce Eve's knowledge about the key (privacy amplification). By this procedure the key shrinks to a fraction of the raw key and in the limit of infinitely many signals this *secret fraction* reads
$$r_\infty = \max\{1 - h(e_X) - h(e_Z), 0\}, \tag{3.12}$$
where
$$h(p) = -p \log_2(p) - (1-p) \log_2(1-p) \tag{3.13}$$
is the binary entropy. The resulting string is the secret key.

3.4 Ekert protocol

In the BB84 protocol Alice prepares one of the four states in Eqs. (3.8)-(3.11) and Bob performs a measurement on it. Protocols of this type are called *prepare-and-measure* protocols. In contrast to this approach, *entanglement-based* protocols use shared entangled states between Alice and Bob. The two approaches are equivalent. In case of the BB84 protocol one can easily see that the prepared states can arise from measurements on one subsystem of a maximally entangled state, e.g. $|\psi^-\rangle$.
The first entanglement-based protocol is the Ekert-protocol [Eke91]. A simplified version [AMP06] can be summarized in the following steps.

1. Party 1 (Alice) and party 2 (Bob) each receive one qubit of a system in the maximally entangled state $|\phi^+\rangle$.

2. Alice and Bob randomly choose a setting $x_1 \in \{1,2,3\}$ and $x_2 \in \{1,2\}$, respectively, and measure along the measurement direction $\vec{a}_i(x_i)$ (see Eq. (1.5)), where $i = 1,2$ denotes the party and

$$\vec{a}_1(1) = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \qquad \vec{a}_1(2) = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \qquad \vec{a}_1(3) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \quad (3.14)$$

$$\vec{a}_2(1) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \quad \vec{a}_2(2) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}, \quad (3.15)$$

3. The steps 1 and 2 are repeated until a sufficient amount of data has been accumulated.

4. The measurement outcomes in the setting $(x_1 = 3, x_2 = 1)$ form the raw key. The measurement results for $x_1 \in \{1,2\}$ can be used to check for an eavesdropper via the CHSH inequality (2.7). The results in the setting $(x_1 = 3, x_2 = 2)$ are discarded.

Because the security analysis is based on the violation of a Bell inequality, this protocol is *device-independent*, which means that no assumptions about the Hilbert space dimension and the performed measurements are necessary for the security proof.

3.5 Security proofs

As motivated above, the security of quantum cryptography originates from the laws of quantum theory, e.g. the no-cloning theorem. This reasoning becomes explicit and quantitative in different security proofs of quantum cryptography. Three main approaches are mentioned in the following.

Quantum error correction based security proofs. If Alice and Bob share a pure maximally entangled state, then Eve cannot be correlated with the measurement outcomes of Alice and Bob and the generated key is secure [LB13]. Alice and Bob can employ error correction codes, see Chapter 4, to obtain (almost) pure states. A secret key can be generated when the noise level is below the error correction threshold.

Pure information theoretic approaches. The security analysis of [Ren05] is based on conditional entropies, which lead to upper bounds on the length of the key after post-processing it, such that Eve cannot know the secret key.

Proofs in the device-independent scenario. In the device-independent scenario, all devices are treated as black-boxes and no assumptions are made about how they work. It is possible to prove security even with these minimal assumptions using Bell inequalities. The proof of [VV14] is based on a multipartite guessing game (see also Section 2.2): If an eavesdropper Eve could gain more than a certain amount of information about the secret key, then the three parties (Alice, Bob and Eve) could beat the quantum bound of the guessing game.

An error doesn't become a mistake until you refuse to correct it.
Orlando Aloysius Battista [Bat81]

4 Quantum error correction

The previous chapters explained why entanglement is a valuable resource in various tasks. Unfortunately, in practice entanglement tends to be very fragile. It is very sensitive to experimental imperfections and environmental disturbance. Different approaches to protect quantum information are known. After introducing the most common error model, this chapter focuses on quantum error correction codes and entanglement distillation protocols.

4.1 Modelling imperfections

In experiments the evolution of a quantum system during computations or other protocols of quantum information theory deviates from the ideal and intended one for several reasons. They can be grouped into two main classes:

1. The system is not isolated perfectly from its environment. The weak interaction of the two can change the state of the system. Furthermore it entangles the system and the environment. Because the environment is not isolated, it is measured from time to time in some uncontrolled and unknown manner, such that system and environment are projected onto unknown states. Both processes lead to noise on the quantum system which can be modeled by a mixed state.

2. The gates are not applied perfectly. If the gates are implemented by the application of a specific Hamiltonian for a specific period of time, then any imprecision in the interaction strength and time implies that actually a slightly different gate has been applied. This again becomes noticeable as noise in the quantum state.

A very common error model is the *depolarizing noise* [NC00, LB13]. The noisy operation is modeled by the ideal evolution followed by a noise process. If ρ is the ideal single qubit state, then

$$\varepsilon(\rho) = (1 - p_x - p_y - p_z)\rho + p_x X\rho X + p_y Y\rho Y + p_z Z\rho Z \tag{4.1}$$

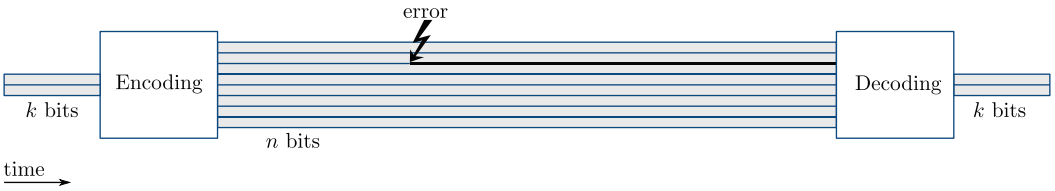


Figure 4.1: The general schematic for error correction codes: k data bits are encoded into n physical bits. The redundancy allows to correct errors that might occur, e.g. during a transmission, such that the final decoding leads to the k data bits without errors.

is the noisy state. The probabilities of X-, Y- and Z-errors are often assumed to be equal, i.e. $p_x = p_y = p_z = \frac{f}{4}$. Then the depolarizing channel of Eq. (4.1) depends only on the failure probability f and takes the form

$$\varepsilon_f(\rho) = (1-f)\rho + f\left(\frac{1}{4}\rho + \frac{1}{4}X\rho X + \frac{1}{4}XZ\rho ZX + \frac{1}{4}Z\rho Z\right), \tag{4.2}$$

which suggests the interpretation that in case of failure there are independent probabilities of $\frac{1}{2}$ for X- and Z-errors. Thus it suffices to correct X- and Z-errors (this also holds for general single qubit noise). See also Appendix G for an introduction to the error model.

4.2 Methods of error correction

Several methods to cope with errors in quantum information theory are known. This is remarkable, especially because the state reduction in a measurement, the no-cloning theorem and the continuous set of quantum errors complicate the transfer of classical error correction methods to the field of quantum information theory [LB13]. Despite these difficulties, quantum error correction codes which are derived from classical linear codes are an important tool to protect coherent quantum information.

4.2.1 Linear block codes

Error correction codes encode words of length k into codewords of length n, where $n > k$ such that the redundancy of the encoded information can be used to detect and correct errors [MS78], see Figure 4.1. In the following the k bits of the encoded information are called logical bits, while the n bits of the codeword are called physical bits. The codewords of linear codes form a vector space, the *code space*. This code space can be described as the kernel of a linear map, i.e. the kernel of a $((n-k)\times n)$-matrix H, the *parity check matrix*. All codewords c fulfill $Hc^T = 0$. Equivalently, the code space can be described via the *generator matrix* G, whose rows form a basis of the code space. The encoding is very simple in linear codes: the codeword c of a word x is obtained via $c = xG$.
The Hamming distance of two codewords is the number of different digits. The Hamming distance of a code is the minimal distance of two codewords. A linear code with k logical bits encoded into n physical bits with a Hamming distance of

d is called a $[n, k, d]$-code. A code with Hamming distance d can correct up to $\frac{d-1}{2}$ bit flip errors or $d-1$ erasure errors. Errors in a codeword are detected if the resulting vector does not fulfill the parity check condition, i.e. if the erroneous word c' has $s^T = Hc'^T \neq 0$. This nonzero vector s is called the error syndrome and the attempt to correct the error depends on the value of s.

4.2.2 Stabilizer codes

Stabilizer codes are an important class of quantum error correction codes [Got97, LB13]. Similar to the parity check matrix of classical linear codes, the code space of a stabilizer code is defined via constraints on the valid codewords. These constraints are

$$s_i|\psi\rangle = |\psi\rangle, \qquad i = 1, 2, ..., n-k \tag{4.3}$$

where the unitary operators s_i form a minimal set of generators of the stabilizer group $\mathcal{S}$ (via multiplication), i.e. $\mathcal{S} = \langle s_1, s_2, ..., s_{n-k}\rangle$. The stabilizer group does not contain $-\mathbb{1}$ and all elements commute. The stabilizer formalism is also used independent of the error correction context in the case of $k = 0$ to define a single state, e.g. a graph state, see Section 5.2.

In absence of errors Eq. (4.3) implies that measurements of s_i, see Figure 4.2, have a $+1$ outcome. All errors that anti-commute with an element of the stabilizer are detected by a -1 outcome of the measurements of s_i, $i = 1, 2, ..., n-k$. The outcomes of all those $n-k$ measurements form the syndrome. A detected error can be corrected by applying a corresponding unitary operation, e.g. Z-errors on a qubit are corrected by applying another Z-operation on the same qubit as $Z^2 = \mathbb{1}$. In general several different errors can lead to the same syndrome.

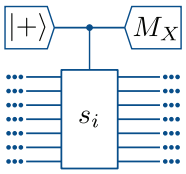


Figure 4.2: Measurement of the stabilizer s_i. The ancillary qubit is prepared in the $|+\rangle$ state. Then a controlled-s_i operation is applied to the ancilla (control) and the block qubits (target). Afterwards the ancilla is measured in the X-basis.

Operators outside of $\mathcal{S}$ that commute with the elements of $\mathcal{S}$ are logical operators acting on the k logical qubits. Among these logical operators one can identify two anti-commuting operators as $\bar{Z}$ and $\bar{X}$, where the bars above the symbols indicate logical operators. The eigenstates of $\bar{Z}^{\otimes k}$ form the logical computational basis.

Table 4.1 specifies the operators s_i ($i = 1, 2, ..., 8$), $\bar{X}$, and $\bar{Z}$ for the [[9,1,3]] Nine-qubit-Shor code. Here the double brackets denote quantum codes. The Shor code can correct an arbitrary single qubit error. The minimal number of physical qubits to protect against an arbitrary single qubit error is five [BBPS96, LMPZ96]. See Table 4.2 for a possible choice of operators of an [[5,1,3]] code.

Table 4.1: The stabilizer generators and the logical operators of the Nine-qubit-Shor code [LB13]. The tensor product is omitted.

Element	Operator
s_1	$Z\ Z\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}$
s_2	$Z\ \mathbb{1}\ Z\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}$
s_3	$\mathbb{1}\ \mathbb{1}\ \mathbb{1}\ Z\ Z\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}$
s_4	$\mathbb{1}\ \mathbb{1}\ \mathbb{1}\ Z\ \mathbb{1}\ Z\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}$
s_5	$\mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ Z\ Z\ \mathbb{1}$
s_6	$\mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ Z\ \mathbb{1}\ Z$
s_7	$X\ X\ X\ X\ X\ X\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}$
s_8	$X\ X\ X\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ X\ X\ X$
$\bar{X}$	$X\ X\ X\ X\ X\ X\ X\ X\ X$
$\bar{Z}$	$Z\ Z\ Z\ Z\ Z\ Z\ Z\ Z\ Z$

Table 4.2: The stabilizer generators and the logical operators of the five-qubit code [BBPS96, LMPZ96, LB13]. The tensor product is omitted.

Element	Operator
s_1	$X\ Z\ Z\ X\ \mathbb{1}$
s_2	$\mathbb{1}\ X\ Z\ Z\ X$
s_3	$X\ \mathbb{1}\ X\ Z\ Z$
s_4	$Z\ X\ \mathbb{1}\ X\ Z$
$\bar{X}$	$X\ X\ X\ X\ X$
$\bar{Z}$	$Z\ Z\ Z\ Z\ Z$

4.2.3 Calderbank-Shor-Steane codes

Calderbank-Shor-Steane (CSS) codes are stabilizer codes where the generators s_i of the stabilizer can be written as a tensor product of $\mathbb{1}$- and either X- or Z-operators [LB13]. One can associate a classical linear code with the generators that contain Z and X, respectively. The first code is used to detect X errors, the second to detect Z errors. This construction is possible if the dual code (generator matrix and parity check matrix exchange their role) of the second, $C_2^{\perp}$, is a subcode of C_1. The nine-qubit-Shor code given above (see Table 4.1) is an example of a CSS code, while the five-qubit code (see Table 4.2) is not. An important CSS code is the [[7,1,3]] seven-qubit-Steane code (see Table 4.3), because it is the simplest CSS code that can correct an arbitrary single qubit error. It can be derived from the [7,4,3] Hamming code [MS78]. Another important example of a CSS code is

Table 4.3: The stabilizer generators and the logical operators of the seven-qubit-Steane code [LB13]. The tensor product is omitted.

Element	Operator
s_1	$\mathbb{1}\ \mathbb{1}\ \mathbb{1}\ X\ X\ X\ X$
s_2	$\mathbb{1}\ X\ X\ \mathbb{1}\ \mathbb{1}\ X\ X$
s_3	$X\ \mathbb{1}\ X\ \mathbb{1}\ X\ \mathbb{1}\ X$
s_4	$\mathbb{1}\ \mathbb{1}\ \mathbb{1}\ Z\ Z\ Z\ Z$
s_5	$\mathbb{1}\ Z\ Z\ \mathbb{1}\ \mathbb{1}\ Z\ Z$
s_6	$Z\ \mathbb{1}\ Z\ \mathbb{1}\ Z\ \mathbb{1}\ Z$
$\bar{X}$	$X\ X\ X\ X\ X\ X\ X$
$\bar{Z}$	$Z\ Z\ Z\ Z\ Z\ Z\ Z$

the [[23,1,7]] quantum Golay code, see Table 4.4. It is derived from the Golay code [Gol49, Goe71] using the CSS construction.

4.2.4 Distillation

The error correction codes of the previous sections are used for forward error correction, i.e. the receiver of the message can correct errors in the received message single-handed without conferring with the sender. A different approach to error correction uses additional classical communication between sender and receiver [LB13]. The main idea is to use n imperfect copies of the wanted quantum state as a resource to produce $k < n$ copies of that state with a higher quality, i.e. with less noise. The aim is to create quantum states that are entangled across the bipartition sender vs. receiver. This explains why this error correction scheme is usually called *entanglement distillation*. In most cases the targeted state is a Bell pair, e.g. $|\phi^+\rangle$ (see Eq. (1.11)). The additional classical communication is used during the protocol to transmit measurement results.

Table 4.4: The stabilizer generators and the logical operators of the quantum Golay code [Goe71]. The tensor product is omitted.

Element	Operator
s_1	$\mathbb{1}\ X\ X\ X\ X\ X\ X\ X\ X\ X\ X\ X\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}$
s_2	$X\ X\ X\ \mathbb{1}\ X\ X\ X\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ X\ \mathbb{1}\ \mathbb{1}\ X\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}$
s_3	$X\ X\ \mathbb{1}\ X\ X\ X\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ X\ \mathbb{1}\ X\ \mathbb{1}\ \mathbb{1}\ X\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}$
s_4	$X\ \mathbb{1}\ X\ X\ X\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ X\ \mathbb{1}\ X\ X\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ X\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}$
s_5	$X\ X\ X\ X\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ X\ \mathbb{1}\ X\ X\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ X\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}$
s_6	$X\ X\ X\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ X\ \mathbb{1}\ X\ X\ \mathbb{1}\ X\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ X\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}$
s_7	$X\ X\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ X\ \mathbb{1}\ X\ X\ \mathbb{1}\ X\ X\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ X\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}$
s_8	$X\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ X\ \mathbb{1}\ X\ X\ \mathbb{1}\ X\ X\ X\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ X\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}$
s_9	$X\ \mathbb{1}\ \mathbb{1}\ X\ \mathbb{1}\ X\ X\ \mathbb{1}\ X\ X\ X\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ X\ \mathbb{1}\ \mathbb{1}$
s_{10}	$X\ \mathbb{1}\ X\ \mathbb{1}\ X\ X\ \mathbb{1}\ X\ X\ X\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ X\ \mathbb{1}$
s_{11}	$X\ X\ \mathbb{1}\ X\ X\ \mathbb{1}\ X\ X\ X\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ X$
s_{12}	$\mathbb{1}\ Z\ Z\ Z\ Z\ Z\ Z\ Z\ Z\ Z\ Z\ Z\ Z\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}$
s_{13}	$Z\ Z\ Z\ \mathbb{1}\ Z\ Z\ Z\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ Z\ \mathbb{1}\ \mathbb{1}\ Z\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}$
s_{14}	$Z\ Z\ \mathbb{1}\ Z\ Z\ Z\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ Z\ \mathbb{1}\ Z\ \mathbb{1}\ \mathbb{1}\ Z\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}$
s_{15}	$Z\ \mathbb{1}\ Z\ Z\ Z\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ Z\ \mathbb{1}\ Z\ Z\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ Z\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}$
s_{16}	$Z\ Z\ Z\ Z\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ Z\ \mathbb{1}\ Z\ Z\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ Z\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}$
s_{17}	$Z\ Z\ Z\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ Z\ \mathbb{1}\ Z\ Z\ \mathbb{1}\ Z\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ Z\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}$
s_{18}	$Z\ Z\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ Z\ \mathbb{1}\ Z\ Z\ \mathbb{1}\ Z\ Z\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ Z\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}$
s_{19}	$Z\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ Z\ \mathbb{1}\ Z\ Z\ \mathbb{1}\ Z\ Z\ Z\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ Z\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}$
s_{20}	$Z\ \mathbb{1}\ \mathbb{1}\ Z\ \mathbb{1}\ Z\ Z\ \mathbb{1}\ Z\ Z\ Z\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ Z\ \mathbb{1}\ \mathbb{1}$
s_{21}	$Z\ \mathbb{1}\ Z\ \mathbb{1}\ Z\ Z\ \mathbb{1}\ Z\ Z\ Z\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ Z\ \mathbb{1}$
s_{22}	$Z\ Z\ \mathbb{1}\ Z\ Z\ \mathbb{1}\ Z\ Z\ Z\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ \mathbb{1}\ Z$
$\bar{X}$	$X\ X\ X\ X\ X\ X\ X\ X\ X\ X\ X\ X\ X\ X\ X\ X\ X\ X\ X\ X\ X\ X$
$\bar{Z}$	$Z\ Z\ Z\ Z\ Z\ Z\ Z\ Z\ Z\ Z\ Z\ Z\ Z\ Z\ Z\ Z\ Z\ Z\ Z\ Z\ Z\ Z$

Distillation protocols

A distillation protocol using a $[[n, k, d]]$-code consists of the following steps [LB13].

1. *Physical preparation.* The sender prepares n copies of the target state $|\phi^+\rangle^{\otimes n}$.

2. *Transmission.* The second qubit of each pair is send through the channel. Errors occur on the qubits that are now in possession of the receiver, i.e. the state is $\mathbb{1} \otimes E_B|\phi^+\rangle^{\otimes n}$.

3. *Measurement.* Both parties perform measurements of the stabilizer generators $s_1, s_2, ..., s_{n-k}$ and obtain binary strings of measurement outcomes a and b, respectively.

4. *Correction.* The sender corrects according to the syndrome a. The receiver corrects according to the syndrome a and the syndrome $a \oplus b$. This requires the sender to send a via a classical channel. Note that the two "errors" at the receiver's site can cancel each other.

5. *(Decoding.)* Both parties perform a decoding operation to obtain k physical $|\phi^+\rangle$ states. This step is not always necessary: If the final state is to be measured, a logical measurement can be performed instead.

The two most-common distillation protocols, [DEJ$^+$96] and [DBCZ99], use variants of a two qubit repetition code. They can detect a single error, and abort in case of an detected error, because they cannot correct it. If the protocol does not abort, then the fidelity increases. The two protocols differ in the concatenation of different distillation rounds.

Bound entanglement

A state is called bound entangled, if it is entangled but no maximally entangled state can be distilled from it. Bound entanglement is related to the positive partial transposition criterion [Per96], which is a necessary condition for separable states: All separable bipartite states have a positive semidefinite partial transposition (PPT) with respect to one party. If a state is distillable, i.e. it allows to distill a maximally entangled state from it, then it violates the PPT criterion [HHH98]. But entangled PPT states exist [Hor97, HHH98]. This implies, that there exist entangled states, from which no maximally entangled state can be distilled. It is not known whether also bound entangled states with a non-positive partial transpose (NPT) exist, i.e. whether the PPT criterion is sufficient for distillability.

We are all now connected by the Internet, like neurons in a giant brain.

Stephen Hawking [Swa14]

5

Long distance entanglement distribution

The distribution of entanglement over long distances is hindered by (photonic) qubit losses during the transmission. The probability η_T of a photon to cross a fiber (i.e. of successful transmission) drops exponentially with the distance. It can be described by

$$\eta_T(l) = 10^{-\alpha l/10} \tag{5.1}$$

where α is the attenuation coefficient. A typical value at the telecom wavelength (around 850 nm, 1300 nm, or 1550 nm) is $\alpha = 0.2$db/km [GYS04].
These losses imply that a direct fiber link of more than approximately 200 km is not useful for quantum key distribution. To achieve entanglement distribution over larger distances *quantum repeaters* are necessary. These repeater stations are situated along the transmission line to cut it into shorter parts. The repeater stations can employ different approaches to tackle the effects of losses at the cost of increased resources.

1. *Quantum memories.* The transmission of a quantum state from one repeater station to the neighboring one, e.g. the distribution of a Bell pair, can be retried until success. Quantum memories can store the transmitted state until transmission was successful on every repeater link.

2. *Error correction.* Error correction schemes like distillation or stabilizer codes, see Chapter 4, can correct the noise caused by imperfections in transmission and processing of the quantum system.

3. *Multiplexing.* Different transmission lines can be operated in parallel and repeater links of different lines can be composed to achieve connection over the full distance [CJKK07, AKB14]. This is a spatial analog of 1.

The additional qubits inserted by a quantum repeater are measured after they have been processed. This way any quantum repeater scheme finally outputs a Bell pair across the large distance of the full transmission line. Different schemes, some of which are introduced below, can thus be compared by the quality of the

produced Bell pair and the required costs as measured by the used resources. The actual costs strongly depend on the concrete physical implementation and many other influences, of course. A simple figure of merit is the cost function [MKL+14]

$$C = \frac{n}{R}, \tag{5.2}$$

where n denotes the total number of qubits used in the protocol and R is the secret key rate in a cryptographic application of the repeater scheme. Note that the secret key rate depends on the quality of the finally produced state.

5.1 Different quantum repeater approaches

In 1998 Briegel, Dür, Cirac and Zoller proposed the first explicit quantum repeater scheme [BDCZ98]. It applies a nested distillation protocol, where rounds of entanglement swapping and entanglement distillation alternate. The number of initially distributed Bell pairs is a power of two and in each entanglement swapping step two pairs each are merged into a single one across the doubled distance, until the final entangled pair spans the whole distance. Several variants and improved versions of this protocol have been analyzed, e.g. in [DBCZ99, DCB05, MDN11, SSdRG11, ZDB12, ABB+13, AKB14].
Error correction codes in the transmission of quantum information have been discussed in [KL96] as an application of code concatenations. Protocols based on encoding only require to store the qubits for the time needed to process them via quantum gates. This is an advantage compared to memory-based quantum repeaters, because the qubits are subject to noise during storage. Error correction similar to a surface code [BK98, DKLP02] has been applied on a quantum network in [PJS+08]. The protocol of [JTN+09] uses encoded Bell-pairs between neighboring repeater stations and exemplifies the analysis for several different CSS codes. The transmitted qubits can also be encoded using the surface code [FWH+10, FMMC12]. Several subsequent works used different codes or improved the analysis of quantum repeater schemes with encoding, in particular with respect to quantum key distribution [MSD+12, BKB14, MKL+14, MZL+15].
In [EKB15], see Appendix F, I developed, with the aid of my co-authors, an approach that generalizes the repeaters with encoding to general networks of these devices. These networks can distribute general multipartite graph states, which are defined in the following section.

5.2 Graph states

A graph state [SW01, BR01] $|G\rangle$ is a quantum state which is associated with a (mathematical) simple undirected graph $G = (V, E)$, i.e. a set of vertices V and a set of edges $E \subset V \times V$ connecting the vertices [Die96], see Figure 5.1. The terms simple and undirected mean that there are no edges from a vertex to itself and the edges have no direction, respectively. Let $N = |V|$ denote the number of vertices.

The quantum state $|G\rangle$ can be defined as the unique state stabilized by the

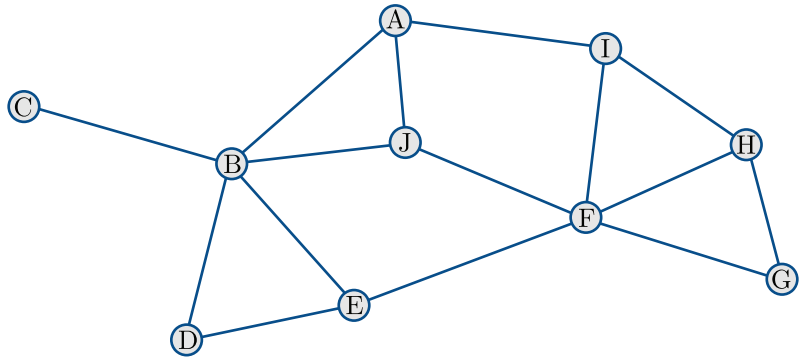


Figure 5.1: Example for a graph with vertices $V = \{\mathrm{A}, \mathrm{B}, ..., \mathrm{J}\}$ and edges $E = \{(\mathrm{A}, \mathrm{B}), (\mathrm{A}, \mathrm{I}), (\mathrm{A}, \mathrm{J}), (\mathrm{B}, \mathrm{A}), (\mathrm{B}, \mathrm{C}), ..., (\mathrm{J}, \mathrm{F})\}$.

stabilizer generators

$$g_i = X_i \prod_{\substack{j \\ (i,j)\in E}} Z_j, \tag{5.3}$$

i.e. the state fulfills

$$g_i|G\rangle = |G\rangle \tag{5.4}$$

for all $i \in V$. It can be constructed from a product state $|+\rangle^{\otimes N}$ by applying a controlled-phase gate C_Z for each edge, i.e.

$$|G\rangle = \Big(\prod_{\substack{(i,j)\in E \\ i<j}} C_Z^{(i,j)} \Big) |+\rangle^{\otimes N}. \tag{5.5}$$

5.3 Quantum Networks

The non-classicality of quantum systems in terms of the violation of Bell inequalities can increase exponentially with the number of parties [Mer90], which leads to larger advantages of quantum protocols compared to their classical counterparts, see Section 2.2. These parties may form a network and they may communicate quantum information along the network links. In general quantum networks are capable of creating and distributing multipartite entangled states, see also Appendix F.

Because quantum repeaters are not available yet, hybrid networks of quantum links together with classical nodes are used in cryptographic applications [PPA+09]. In this case the security of the communication between two nodes in the network depends on whether one can trust the intermediate network nodes and networks of this type are called trusted node networks.

Routing denotes the path-selection for a signal that is traveling from one party to another in a larger network. It is interesting to optimize the routing strategy, because each individual link has only a finite capacity, such that the routing influences the overall throughput of the network. This classical problem has been considered in quantum information theory, too [Ell02, VMSL+13].

Different to the routing approach, in a network coding scheme the signal is not send along a single route only, but it is encoded into the signal of several channels.

This technique allows to efficiently use all links and relieves bottlenecks of the network. The quantum analog of network coding has been investigated, e.g. in [LOW06, Hay07, SINV15].
Large scale quantum networks rise many more research problems. As another example I mention the interoperability of different network technologies, e.g. different encodings, analyzed in [NCD+15]. See also [PJC+13] for a review on entanglement distribution in quantum networks.

6 Overview of results

This chapter lists the main results of my attached work.

Appendix A: An explicit example for a communication complexity task is given, in which the parties benefit from bound entanglement (see Section 4.2.4). The three parties receive three different inputs ($M_1 = M_2 = M_3 = 3$). The function and the probability distribution are given by (see Section 2.2)

$$\begin{aligned} g(x_1, x_2, x_3) = \quad & 2[(\delta_{x_1,x_2,x_3} + x_1 + x_2 + x_3) \bmod 2] - 1 \\ & \times (1 + 4\delta_{0,x_1,x_2,x_3})(1 - \delta_{2,(x_1+x_2+x_3) \bmod 3}), \\ & \times (1 - \delta_{3,x_1})(1 - \delta_{3,x_2})(1 - \delta_{3,x_3}) \end{aligned} \tag{6.1}$$

where the symbol δ is 1 if all subscripts are equal and 0 otherwise.

Appendix B: For a given lattice of N spins entanglement witnesses $\hat{W}$ are constructed as

$$\hat{W} = a\hat{S} + b\mathbb{1}, \tag{6.2}$$

where $\hat{S}$ is a particular combination of spin observables that typically arises in neutron scattering. The two real coefficients a and b depend on the bounds

$$c_{\min} \leq \langle \hat{S} \rangle_{\text{sep.}} \leq c_{\max} \tag{6.3}$$

on the expectation value of the scattering observable for separable states. Furthermore they are rescaled, such that the expectation value of the witnesses $\hat{W}$ give lower bounds on the entanglement in the system according to different entanglement measures. For thermal states given by different model Hamiltonians it is shown that $\hat{W}$ can be used to detect entanglement in the system.

Appendix C: It is shown that

$$T(g) = \sqrt{M_1 M_2} \sum_{x_3,\ldots,x_n}^{M_3,\ldots,M_n} ||g_{*,*,x_3,\ldots,x_n}||_2, \tag{6.4}$$

where $||g_{*,*,x_3,\ldots,x_n}||_2$ is the largest singular value of the matrix $(g_{x_1,x_2,x_3,\ldots,x_n})_{x_1,x_2}$, is a Tsirelson bound for the CHSH-type inequality given by coefficients $g_{x_1,\ldots,x_n}$. For two parties this bound simplifies to

$$T(g) = \sqrt{M_1 M_2}||g||_2. \tag{6.5}$$

Conditions for achievability of the bound are given and interpreted geometrically and dimension witnesses are constructed from this.

Appendix D: Operations on g which leave $T(g)$ in Eq. (6.5) invariant are discussed. These are

- special rotations of the singular vectors and
- modifications of non-maximal singular values.

Rotations of the local coordinate system are identified with the first. The fact that the operations affect the classical bound of the Bell inequality associated with g is used to optimize w.r.t. the violation.

Appendix E: This paper summarizes the previous two papers and is intended to be accessible by readers outside of the scientific community. It contains a simplified example of a Bell experiment without common reference frame.

Appendix F: A network of quantum repeaters with encoding (see Section 5) is described in the graph state formalism (see Section 5.2) and a detailed error analysis (see Section 4) is done. The quality of general graph states distributed by this network is analyzed. The Golay code (see Section 4.2.3) is identified as a very efficient error correction code in this context. The graph state repeater with Golay code outperforms all other investigated repeater schemes in the considered parameter regime.

Appendix G: Gives more details about the error analysis of quantum repeaters. Contains the comparison of the standard repeater and the graph state repeater. The result strongly depends on the time required for local operations. For fast local operations quantum repeaters with encoding outperform the standard repeater scheme due to the classical communication. The impact on the key rate of different strategies to abort in case of an fatal amount of noticed errors is discussed.

Bibliography

[ABB+13] Silvestre Abruzzo, Sylvia Bratzik, Nadja K. Bernardes, Hermann Kampermann, Peter van Loock, and Dagmar Bruß, *Quantum repeaters and quantum key distribution: Analysis of secret-key rates*, Phys. Rev. A **87** (2013), 052315.

[ABPS09] Jonathan Allcock, Nicolas Brunner, Marcin Pawlowski, and Valerio Scarani, *Recovering part of the boundary between quantum and nonquantum correlations from information causality*, Phys. Rev. A **80** (2009), 040103.

[AGR81] Alain Aspect, Philippe Grangier, and Gérard Roger, *Experimental Tests of Realistic Local Theories via Bell's Theorem*, Phys. Rev. Lett. **47** (1981), 460–463.

[AGR82] A. Aspect, P. Grangier, and G. Roger, *Experimental Realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A New Violation of Bell's Inequalities*, Phys. Rev. Lett. **49** (1982), 91–94.

[AKB14] Silvestre Abruzzo, Hermann Kampermann, and Dagmar Bruß, *Finite-range multiplexing enhances quantum key distribution via quantum repeaters*, Phys. Rev. A **89** (2014), 012303.

[AMP06] Antonio Acín, Serge Massar, and Stefano Pironio, *Efficient quantum key distribution secure against no-signalling eavesdroppers*, New Journal of Physics **8** (2006), no. 8, 126.

[AWB+09] M. Ansmann, H. Wang, R. C. Bialczak, M. Hofheinz, E. Lucero, M. Neeley, A. D. O'Connell, D. Sank, M. Weides, J. Wenner, A. N. Cleland, and J. M. Martinis, *Violation of Bell's inequality in Josephson phase qubits*, Nature **461** (2009), 504–506.

[Bat81] Orlando Aloysius Battista, *Quotoons: a speaker's dictionary*, Perigee Books, 1981.

[BB84] C.H. Bennett and G. BRassard, *Quantum cryptography: Public key distribution and coin tossing*, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing (1984), 175–179.

[BBPS96] Charles H. Bennett, Herbert J. Bernstein, Sandu Popescu, and Benjamin Schumacher, *Concentrating partial entanglement by local operations*, Phys. Rev. A **53** (1996), 2046–2052.

[BC90] SL Braunstein and CM Caves, *Wringing out better Bell inequalities*, Ann. Phys.-NY **202** (1990), no. 1, 22–56.

[BDCZ98] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, *Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication*, Phys. Rev. Lett. **81** (1998), 5932–5935.

[Bel64] J. S. Bell, *On the Einstein Podolski Rosen Paradox*, Physics **1** (1964), 195–200.

[BK98] S. B. Bravyi and A. Y. Kitaev, *Quantum codes on a lattice with boundary*, ArXiv e-prints:quant-ph/9811052 (1998).

[BKB14] Sylvia Bratzik, Hermann Kampermann, and Dagmar Bruß, *Secret key rates for an encoded quantum repeater*, Phys. Rev. A **89** (2014), 032335.

[BNV13] Nicolas Brunner, Miguel Navascués, and Tamás Vértesi, *Dimension Witnesses and Quantum State Discrimination*, Phys. Rev. Lett. **110** (2013), 150501.

[BPA+08] Nicolas Brunner, Stefano Pironio, Antonio Acin, Nicolas Gisin, André Allan Méthot, and Valerio Scarani, *Testing the Dimension of Hilbert Spaces*, Phys. Rev. Lett. **100** (2008), 210503.

[BR01] Hans J. Briegel and Robert Raussendorf, *Persistent Entanglement in Arrays of Interacting Particles*, Phys. Rev. Lett. **86** (2001), 910–913.

[BRSd10] H. Buhrman, O. Regev, G. Scarpa, and R. de Wolf, *Near-Optimal and Explicit Bell Inequality Violations*, ArXiv e-prints:quant-ph/1012.5043 (2010).

[BZPZ04] Caslav Brukner, Marek Żukowski, Jian-Wei Pan, and Anton Zeilinger, *Bell's Inequalities and Quantum Communication Complexity*, Phys. Rev. Lett. **92** (2004), 127901.

[Cab13] Adán Cabello, *Simple Explanation of the Quantum Violation of a Fundamental Inequality*, Phys. Rev. Lett. **110** (2013), no. 6, 060402.

[CH74] John F. Clauser and Michael A. Horne, *Experimental consequences of objective local theories*, Phys. Rev. D **10** (1974), 526–535.

[CHSH69] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, *Proposed experiment to test local hidden-variable theories*, Phys. Rev. Lett. **23** (1969), no. 15, 880–884.

[CJKK07] O. A. Collins, S. D. Jenkins, A. Kuzmich, and T. A. B. Kennedy, *Multiplexed Memory-Insensitive Quantum Repeaters*, Phys. Rev. Lett. **98** (2007), 060502.

[Com13] International Roadmap Committee, *International Technology Roadmap For Semiconductors, 2013 Edition. Executive Summary*, `http://www.itrs.net/ITRS%201999-2014%20Mtgs,%20Presentations%20&%20Links/2013ITRS/2013TableSummaries/2013ORTC_SummaryTable.pdf`, 2013, Accessed: 2015-08-27.

[DBCZ99] W. Dür, H.-J. Briegel, J. I. Cirac, and P. Zoller, *Quantum repeaters based on entanglement purification*, Phys. Rev. A **59** (1999), 169–181.

[DCB05] W. Dür, J. Calsamiglia, and H.-J. Briegel, *Multipartite secure state distribution*, Phys. Rev. A **71** (2005), 042336.

[DEJ+96] David Deutsch, Artur Ekert, Richard Jozsa, Chiara Macchiavello, Sandu Popescu, and Anna Sanpera, *Quantum privacy amplification and the security of quantum cryptography over noisy channels*, Phys. Rev. Lett. **77** (1996), 2818–2821.

[Die96] R. Diestel, *Graphentheorie*, Springer-Lehrbuch, Springer, 1996.

[DKLP02] E. Dennis, A. Kitaev, A. Landahl, and J. Preskill, *Topological quantum memory*, Journal of Mathematical Physics **43** (2002), 4452–4505.

[DLTW08] A. C. Doherty, Y.-C. Liang, B. Toner, and S. Wehner, *The quantum moment problem and bounds on entangled multi-prover games*, P. IEEE CCC (2008), 199–210.

[EKB13] Michael Epping, Hermann Kampermann, and Dagmar Bruß, *Designing Bell Inequalities from a Tsirelson Bound*, Phys. Rev. Lett. **111** (2013), 240404.

[EKB15] M. Epping, H. Kampermann, and D. Bruß, *Graph State Quantum Repeater Networks*, ArXiv e-prints (2015).

[Eke91] Artur K. Ekert, *Quantum cryptography based on Bell's theorem*, Phys. Rev. Lett. **67** (1991), 661–663.

[Ell02] Chip Elliott, *Building the quantum network*, New Journal of Physics **4** (2002), no. 1, 46.

[Epp12] Michael Epping, *Quantenkommunikationskomplexität mit nichtidealen Detektoren*, Master's thesis, University of Vienna, Austria, 2012.

[EPR35] A. Einstein, B. Podolsky, and N. Rosen, *Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?*, Phys. Rev. **47** (1935), 777–780.

[FC72] Stuart J. Freedman and John F. Clauser, *Experimental Test of Local Hidden-Variable Theories*, Phys. Rev. Lett. **28** (1972), 938–941.

[Fey82] Richard P. Feynman, *Simulating physics with computers*, International Journal of Theoretical Physics **21** (1982), no. 6-7, 467–488.

[FMMC12] Austin G. Fowler, Matteo Mariantoni, John M. Martinis, and Andrew N. Cleland, *Surface codes: Towards practical large-scale quantum computation*, Phys. Rev. A **86** (2012), 032324.

[FWH+10] A. G. Fowler, D. S. Wang, C. D. Hill, T. D. Ladd, R. Van Meter, and L. C. Hollenberg, *Surface Code Quantum Communication*, Phys. Rev. Lett. **104** (2010), 180503.

[GBHA10] Rodrigo Gallego, Nicolas Brunner, Christopher Hadley, and Antonio Acín, *Device-independent tests of classical and quantum dimensions*, Phys. Rev. Lett. **105** (2010), 230501.

[GMR+13] M. Giustina, A. Mech, S. Ramelow, B. Wittmann, J. Kofler, J. Beyer, A. Lita, B. Calkins, T. Gerrits, S. W. Nam, R. Ursin, and A. Zeilinger, *Bell violation using entangled photons without the fair-sampling assumption*, Nature **497** (2013), 227–230.

[Goe71] J.-M Goethals, *On the golay perfect binary code*, Journal of Combinatorial Theory, Series A **11** (1971), no. 2, 178 – 186.

[Gol49] Marcel Jules Edouard Golay, *Notes on Digital Coding*, Proc. IRE **37** (1949), 657.

[Got97] D. Gottesman, *Stabilizer codes and quantum error correction*, Ph.D. thesis, California Institute of Technology, 1997.

[GT09] Otfried Gühne and Géza Tóth, *Entanglement detection*, Physics Reports **474** (2009), 1 – 75.

[GVL13] Gene H. Golub and Charles F. Van Loan, *Matrix Computations*, 4th ed., The Johns Hopkins University Press, Baltimore, 2013.

[GVW+15] Marissa Giustina, Marijn A. M. Versteegh, Sören Wengerowsky, Johannes Handsteiner, Armin Hochrainer, Kevin Phelan, Fabian Steinlechner, Johannes Kofler, Jan-Åke Larsson, Carlos Abellán, Waldimar Amaya, Valerio Pruneri, Morgan W. Mitchell, Jörn Beyer, Thomas Gerrits, Adriana E. Lita, Lynden K. Shalm, Sae Woo Nam, Thomas Scheidl, Rupert Ursin, Bernhard Wittmann, and Anton Zeilinger, *Significant-loophole-free test of bell's theorem with entangled photons*, Phys. Rev. Lett. **115** (2015), 250401.

[GWAN11] Rodrigo Gallego, Lars Erik Würflinger, Antonio Acín, and Miguel Navascués, *Quantum Correlations Require Multipartite Information Principles*, Phys. Rev. Lett. **107** (2011), 210403.

[GYS04] C. Gobby, Z. L. Yuan, and A. J. Shields, *Quantum key distribution over 122 km of standard telecom fiber*, Applied Physics Letters **84** (2004), no. 19, 3762–3764.

[Hay07] Masahito Hayashi, *Prior entanglement between senders enables perfect quantum network coding with modification*, Phys. Rev. A **76** (2007), 040301.

[HBD+15] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson, *Experimental loophole-free violation of a Bell inequality using entangled electron spins separated by 1.3 km*, Nature **526** (2015), 682–686.

[HHH98] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki, *Mixed-state entanglement and distillation: Is there a "bound" entanglement in nature?*, Phys. Rev. Lett. **80** (1998), 5239–5242.

[HHHH09] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki, *Quantum entanglement*, Rev. Mod. Phys. **81** (2009), 865–942.

[Hor97] Pawel Horodecki, *Separability criterion and inseparable mixed states with positive partial transposition*, Physics Letters A **232** (1997), no. 5, 333–339.

[JTN+09] Liang Jiang, J. M. Taylor, Kae Nemoto, W. J. Munro, Rodney Van Meter, and M. D. Lukin, *Quantum repeater with encoding*, Phys. Rev. A **79** (2009), 032325.

[KL96] E. Knill and R. Laflamme, *Concatenated Quantum Codes*, ArXiv e-prints:quant-ph/9608012 (1996).

[Lar14] Jan-Åke Larsson, *Loopholes in Bell inequality tests of local realism*, Journal of Physics A: Mathematical and Theoretical **47** (2014), no. 42, 424003.

[LB13] D.A. Lidar and T.A. Brun, *Quantum Error Correction*, Cambridge University Press, 2013.

[LMPZ96] Raymond Laflamme, Cesar Miquel, Juan Pablo Paz, and Wojciech Hubert Zurek, *Perfect quantum error correcting code*, Phys. Rev. Lett. **77** (1996), 198–201.

[LOW06] D. Leung, J. Oppenheim, and A. Winter, *Quantum network communication – the butterfly and beyond*, ArXiv e-prints:quant-ph/0608223 (2006).

[LS98] Maciej Lewenstein and Anna Sanpera, *Separability and Entanglement of Composite Quantum Systems*, Phys. Rev. Lett. **80** (1998), 2261–2264.

[MDN11] William J. Munro, Simon J. Devitt, and Kae Nemoto, *Designing quantum repeaters and networks*, 2011, pp. 816307–816307–8.

[Mer90] ND Mermin, *Extreme quantum entanglement in a superposition of macroscopically distinct states*, Phys. Rev. Lett. **65** (1990), no. 15, 1838–1840.

[MKL+14] Sreraman Muralidharan, Jungsang Kim, Norbert Lütkenhaus, Mikhail D. Lukin, and Liang Jiang, *Ultrafast and Fault-Tolerant Quantum Communication across Long Distances*, Phys. Rev. Lett. **112** (2014), 250501.

[Moo65] G. E. Moore, *Cramming More Components onto Integrated Circuits*, Electronics **38** (1965), no. 8, 114–117.

[MS78] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, 2nd ed., North-Holland Publishing Company, 1978.

[MSD+12] W. J. Munro, A. M. Stephens, S. J. Devitt, K. A. Harrison, and K. Nemoto, *Quantum communication without the necessity of quantum memories*, Nat. Photon. **6** (2012), 777–781.

[MZL+15] S. Muralidharan, C.-L. Zou, L. Li, J. Wen, and L. Jiang, *Overcoming erasure errors with multilevel systems*, ArXiv e-prints:quant-ph/1504.08054 (2015).

[NC00] M.A. Nielsen and I.L. Chuang, *Quantum Computation and Quantum Information*, Cambridge Series on Information and the Natural Sciences, Cambridge University Press, 2000.

[NCD+15] S. Nagayama, B.-S. Choi, S. Devitt, S. Suzuki, and R. Van Meter, *Interoperability in encoded quantum repeater networks*, ArXiv e-prints:quant-ph/1508.04599 (2015).

[NPA07] Miguel Navascués, Stefano Pironio, and Antonio Acín, *Bounding the Set of Quantum Correlations*, Phys. Rev. Lett. **98** (2007), 010401.

[NPA08] M Navascués, Stefano Pironio, and A Acín, *A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations*, New J. Phys. **10** (2008), 1–33.

[NW09] M Navascués and H Wunderlich, *A glance beyond the quantum model*, Proc. Roy. Soc. Lond. A **466** (2009), 881–890.

[Orw49] George Orwell, *1984*, London, 1949.

[OW10] Jonathan Oppenheim and Stephanie Wehner, *The uncertainty principle determines the nonlocality of quantum mechanics.*, Science **330** (2010), no. 6007, 1072–4.

[PBD+00] Jian-Wei Pan, Dik Bouwmeester, Matthew Daniell, Harald Weinfurter, and Anton Zeilinger, *Experimental test of quantum nonlocality in three-photon Greenberger-Horne-Zeilinger entanglement*, Nature **403** (2000), 515–519.

[Per96] Asher Peres, *Separability criterion for density matrices*, Phys. Rev. Lett. **77** (1996), 1413–1415.

[PGWP+08] D. Perez-Garcia, M.M. Wolf, C. Palazuelos, I. Villanueva, and M. Junge, *Unbounded Violation of Tripartite Bell Inequalities*, Communications in Mathematical Physics **279** (2008), no. 2, 455–486.

[PJC+13] S Perseguers, G J Lapeyre Jr, D Cavalcanti, M Lewenstein, and A Acin, *Distribution of entanglement in large-scale quantum networks*, Reports on Progress in Physics **76** (2013), no. 9, 096001.

[PJS+08] S. Perseguers, L. Jiang, N. Schuch, F. Verstraete, M. D. Lukin, J. I. Cirac, and K. G. H. Vollbrecht, *One-shot entanglement generation over long distances in noisy quantum networks*, Phys. Rev. A **78** (2008), 062324.

[PPA+09] M Peev, C Pacher, R Alléaume, C Barreiro, Bouda. J, W Boxleitner, T Debuisschert, E Diamanti, M Dianati, J F Dynes, S Fasel, S Fossier, Fürst. M, J-D Gautier, O Gay, N Gisin, P Grangier, A Happe, Y Hasani, M Hentschel, H Hübel, G Humer, T Länger, M Legré, R Lieger, J Lodewyck, T Lorünser, N Lütkenhaus, A Marhold, T Matyus, O Maurhart, L Monat, S Nauerth, J-B Page, A Poppe, E Querasser, G Ribordy, S Robyr, L Salvail, A W Sharpe, A J Shields, D Stucki, M Suda, C Tamas, T Themel, R T Thew, Y Thoma, A Treiber, P Trinkler, R Tualle-Brouri, F Vannel, N Walenta, H Weier, H Weinfurter, I Wimberger, Z L Yuan, H Zbinden, and A Zeilinger, *The SECOQC quantum key distribution network in Vienna*, New Journal of Physics **11** (2009), no. 7, 075001.

[PPK+09] Marcin Pawlowski, Tomasz Paterek, Dagomir Kaszlikowski, Valerio Scarani, Andreas Winter, and Marek Zukowski, *Information Causality as a Physical Principle*, Nature **461** (2009), 1–9.

[Ren05] R. Renner, *Security of Quantum Key Distribution*, Ph.D. thesis, PhD Thesis, 2005, December 2005.

[RKM+01] M. A. Rowe, D. Kielpinski, V. Meyer, C. A. Sackett, W. M. Itano, C. Monroe, and Wineland D.J., *Experimental violation of a Bell's inequality with efficient detection*, Nature **409** (2001), 791–794.

[SA88] Y. H. Shih and C. O. Alley, *New Type of Einstein-Podolsky-Rosen-Bohm Experiment Using Pairs of Light Quanta Produced by Optical Parametric Down Conversion*, Phys. Rev. Lett. **61** (1988), 2921–2924.

[SBvH+08] D. Salart, A. Baas, J. A. W. van Houwelingen, N. Gisin, and H. Zbinden, *Spacelike Separation in a Bell Test Assuming Gravitationally Induced Collapses*, Phys. Rev. Lett. **100** (2008), 220404.

[Sin99] Simon Singh, *The Code Book*, Fourth Estate, 1999.

[SINV15] T. Satoh, K. Ishizaki, S. Nagayama, and R. Van Meter, *Analysis of Quantum Network Coding for Realistic Repeater Networks*, ArXiv e-prints:quant-ph/1508.02141 (2015).

[SMSC+15] Lynden K. Shalm, Evan Meyer-Scott, Bradley G. Christensen, Peter Bierhorst, Michael A. Wayne, Martin J. Stevens, Thomas Gerrits, Scott Glancy, Deny R. Hamel, Michael S. Allman, Kevin J. Coakley, Shellee D. Dyer, Carson Hodge, Adriana E. Lita, Varun B. Verma, Camilla Lambrocco, Edward Tortorici, Alan L. Migdall, Yanbao Zhang, Daniel R. Kumor, William H. Farr, Francesco Marsili, Matthew D. Shaw, Jeffrey A. Stern, Carlos Abellán, Waldimar Amaya, Valerio Pruneri, Thomas Jennewein, Morgan W. Mitchell, Paul G. Kwiat, Joshua C. Bienfang, Richard P. Mirin, Emanuel Knill, and Sae Woo Nam, *Strong loophole-free test of local realism*, Phys. Rev. Lett. **115** (2015), 250402.

[SSdRG11] Nicolas Sangouard, Christoph Simon, Hugues de Riedmatten, and Nicolas Gisin, *Quantum repeaters based on atomic ensembles and linear optics*, Rev. Mod. Phys. **83** (2011), 33–80.

[Ste03] Michael Steiner, *Generalized robustness of entanglement*, Phys. Rev. A **67** (2003), 054305.

[SW01] D. Schlingemann and R. F. Werner, *Quantum error-correcting codes associated with graphs*, Phys. Rev. A **65** (2001), 012308.

[Swa14] Jon Swartz, *Stephen Hawking opens up*, `http://usatoday30.usatoday.com/MONEY/usaedition/2014-12-02-QampA-with-Stephen-Hawking_ST_U.htm`, January 2014, Accessed: 2015-08-27.

[TBG+98] W. Tittel, J. Brendel, B. Gisin, T. Herzog, H. Zbinden, and N. Gisin, *Experimental demonstration of quantum correlations over more than 10 km*, Phys. Rev. A **57** (1998), 3229–3232.

[TBZG98] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, *Violation of Bell Inequalities by Photons More Than 10 km Apart*, Phys. Rev. Lett. **81** (1998), 3563–3566.

[Tsi80] B. S. Tsirelson, *Quantum generalizations of Bell's inequality*, Lett. Math. Phys. **4** (1980), 93–100.

[Tsi93] B.S. Tsirelson, *Some results and problems on quantum Bell-type inequalities*, Hadronic J. **8** (1993), no. 4, 329–345.

[Ver70] Jules Verne, *Autour de la Lune*, Voyages extraordinaires, Pierre-Jules Hetzel, 1870.

[VMSL+13] Rodney Van Meter, Takahiko Satoh, ThaddeusD. Ladd, WilliamJ. Munro, and Kae Nemoto, *Path selection for quantum repeater networks*, Networking Science **3** (2013), no. 1-4, 82–95.

[VT99] Guifré Vidal and Rolf Tarrach, *Robustness of entanglement*, Phys. Rev. A **59** (1999), 141–155.

[VV14] Umesh Vazirani and Thomas Vidick, *Fully device-independent quantum key distribution*, Phys. Rev. Lett. **113** (2014), 140501.

[WCD08] Stephanie Wehner, Matthias Christandl, and Andrew C. Doherty, *Lower bound on the dimension of a quantum system given measured data*, Phys. Rev. A **78** (2008), 062112.

[Weh06] Stephanie Wehner, *Tsirelson bounds for generalized Clauser-Horne-Shimony-Holt inequalities*, Phys. Rev. A **73** (2006), no. 022110, 1–9.

[WJS+98] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger, *Violation of Bell's Inequality under Strict Einstein Locality Conditions*, Phys. Rev. Lett. **81** (1998), 5039–5043.

[WMP04] Norm Wolcott, Gregory Margo, and PG Distributed Proofreaders, *The Moon-Voyage*, 2004.

[WPG09] Michael M. Wolf and David Perez-Garcia, *Assessing quantum dimensionality from observable dynamics*, Phys. Rev. Lett. **102** (2009), 190504.

[WW01] R. F. Werner and M. M. Wolf, *All-multipartite Bell-correlation inequalities for two dichotomic observables per site*, Phys. Rev. A **64** (2001), 032112.

[Yao79] Andrew Chi-Chih Yao, *Some Complexity Questions Related to Distributive Computing(Preliminary Report)*, Proceedings of the Eleventh Annual ACM Symposium on Theory of Computing (New York, NY, USA), STOC '79, ACM, 1979, pp. 209–213.

[ZDB12] M. Zwerger, W. Dür, and H. J. Briegel, *Measurement-based quantum repeaters*, Phys. Rev. A **85** (2012), 062326.

Declaration of Originality

I, Michael Epping, declare that this dissertation is the result of my own independent research. All relevant resources are listed in the bibliographies. My contribution to the attached publications matches the given percentage.

Düsseldorf, September 10, 2015

Michael Epping

A

Bound entanglement helps to reduce communication complexity

Title:	Bound entanglement helps to reduce communication complexity
Authors:	M.E. and Časlav Brukner
Journal:	Physical Review A
Impact factor:	2.808
Date of submission:	17 January 2013
Publication status:	Published
Contribution by M.E.:	First author (input approx. 80%)
Results:	Construction of an explicit communication complexity task, where the success probability with bound entanglement is larger than the one without entanglement.

Bound entanglement helps to reduce communication complexity

Michael Epping*
Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, Universitätsstrasse 1, D-40225 Düsseldorf, Germany

Časlav Brukner
Vienna Center for Quantum Science and Technology (VCQ) and Faculty of Physics, University of Vienna, Boltzmanngasse 5, A-1090 Vienna, Austria and Institute of Quantum Optics and Quantum Information (IQOQI), Austrian Academy of Sciences, Boltzmanngasse 3, 1090 Vienna, Austria

(Received 17 January 2013; published 6 March 2013)

We present a simple communication complexity problem where three parties benefit from sharing bound entanglement. This demonstrates that entanglement distillability of the shared state is not necessary in order to surpass classical communication complexity.

DOI: 10.1103/PhysRevA.87.032305 PACS number(s): 03.67.Hk, 03.65.Ud, 03.67.Mn

I. INTRODUCTION

Quantum information studies communication or computation schemes which allow more efficient solutions when considering the laws of quantum theory instead of those of classical physics. In this research field, entanglement has proven to be a beneficial resource and many applications make use of maximally entangled states [1]. Because these states are important for such applications, methods have been developed to create one maximally entangled state out of several copies of less entangled states using local operations and classical communication (LOCC) [2]. This process is called entanglement distillation. Entangled states that allow for the creation of a maximally entangled state by LOCC in at least one bipartition of the composite system are called distillable states. States which are entangled but not distillable are called bound entangled states [3].

Bell inequalities are constraints on probabilities for local measurements, which are satisfied by local hidden variable theories [4,5]. However, they are not satisfied by quantum mechanics. Entangled states that violate a Bell inequality are called nonlocal. There exist (mixed) entangled local states, i.e., states which do not violate any Bell inequality [6]. Yet, it was shown that all entangled states, including bound entangled ones, violate a Bell inequality when combined with another state which on its own cannot violate the same Bell inequality [7].

Every distillable state may be transformed into a nonlocal state using only LOCC, but not every nonlocal state is distillable. This was found recently by giving an explicit example of a nonlocal bound entangled state [8] (strengthening previous results [9–11] to fully bound entangled states; see below for the definition of fully bound entangled states). Even though no pure entanglement can be distilled from bound entangled states, they constitute a useful resource in quantum-information protocols. These are entanglement activation [12,13], enhancement of the teleportation power of some other state [14], quantum steering [15], quantum data hiding [16], and quantum key distribution [17]. The last two tasks are "classical" in the sense that they can be stated outside the framework of quantum theory. Quantum theory can then enable advantages in comparison to how the tasks can be performed on the basis of classical laws. In this paper we consider another task of this type—communication complexity—for which we show that bound entangled states can provide an advantage over all possible classical solutions. This task allows to quantify the advantage of the bound entangled states with respect to classical resources of shared (classically) correlated bit strings. Communication complexity studies the amount of information that must be communicated between distant parties in order to calculate a function of arguments which are distributed among the parties [18]. We consider a similar question: If the parties are restricted to communicate only a given amount of information, what is the highest possible probability for them to estimate the value of the function correctly?

It is well known that nonlocal states can be useful in such a task [19]. Here we give a surprisingly simple example illustrating the fact that this includes even fully bound entangled states.

II. A GENERAL QUANTUM COMMUNICATION COMPLEXITY SCHEME

We make use of a generalization of the quantum communication complexity scheme introduced in Ref. [19] to more than two bits of input per party. Consider the situation where n parties labeled 1 to n are spatially separated. Let us assume an inequality of the form

$$\sum_{x_1,\ldots,x_n=0}^{2^m-1} g(x_1,\ldots,x_n)E(x_1,\ldots,x_n) \leqslant B, \qquad (1)$$

where the coefficients $g(x_1,\ldots,x_n)$ and the local hidden variable bound B are real numbers and $E(x_1,\ldots,x_n)$ is the correlation function of a measurement for the choice of measurement setting x_i by each party i. The correlation function can be expressed as $E(x_1,\ldots,x_n) = P(a_1\cdots a_n = 1|x_1,\ldots,x_n) - P(a_1\cdots a_n = -1|x_1\cdots x_n)$, where $a_i = \pm 1$ is the measurement result of observer i. We call inequality (1) a Bell inequality if it can be violated by a value $S > B$ using quantum-mechanical expectation values. Following the idea of Ref. [19] we introduce a quantum communication complexity problem associated with this Bell inequality. Each party i receives one bit $y_i \in \{-1,1\}$ and m bits $x_i \in \{0,1,\ldots,2^m-1\}$ unknown to all the other parties. The two possible values of y_i

*epping@thphy.uni-duesseldorf.de

occur with equal probability whereas the values of x_i follow the probability distribution

$$Q(x_1,\ldots,x_n)=\frac{|g(x_1,\ldots,x_n)|}{\sum_{x_1',\ldots,x_n'=0}^{2^m-1}|g(x_1',\ldots,x_n')|}, \tag{2}$$

which is fixed beforehand and known to all parties. Their common task is to output the value of the function

$$f(y_1,\ldots,y_n,x_1,\ldots,x_n)=\prod_{i=1}^{n} y_i \operatorname{sign}\left[g(x_1,\ldots,x_n)\right]. \tag{3}$$

The parties do not evaluate the function correctly with certainty. The aim is to maximize the probability of successful evaluation. Each party is allowed to broadcast a single bit of information to its fellow parties. It is required that all parties broadcast the bit simultaneously. (In this way the communicated bit of one party does not depend on the broadcasted bits of others, but only on the local input.) Afterwards one of the parties is asked to output the value of the function. We consider two different protocols. In the classical protocol the bit s_i sent by party i could be in general any function of y_i and x_i. However, it was shown in Ref. [20] (analog to Ref. [19]) that in the optimal classical protocol $s_i=y_i a_i(x_i)$, where $a_i(x_i)$ is an appropriate chosen function $\{0,1,\ldots,2^m-1\}\to\{-1,1\}$ and the best guess is given by

$$A(y_1,\ldots,y_n,x_1,\ldots,x_n)=\prod_{i=1}^{n} y_i a_i(x_i). \tag{4}$$

Intuitively one can understand this in the following way. Opposite values of any y_i lead to opposite values of the function f. Missing a single y_i would completely destroy the information about the result. Therefore, it is crucial to communicate y_i in a way that allows to reconstruct the product of all the y_i's. In the quantum protocol, $a_i(x_i)$ is replaced by the measurement result a_i. Each party i chooses one out of 2^m possible measurement settings according to the input x_i and sends y_i multiplied by the measurement result a_i. The best guess is then again given by Eq. (4).

The probability of success of the protocol, i.e., the probability for $A(y_1,\ldots,y_n,x_1,\ldots,x_n)$ to equal $f(y_1,\ldots,y_n,x_1,\ldots,x_n)$ can be written as

$$P(A=f)=\tfrac{1}{2}[1+(f,A)] \tag{5}$$

using the weighted scalar product

$$(f,A)=\sum_{y_1,\ldots,y_n=\pm1}\sum_{x_1,\ldots,x_n=0}^{2^m-1}\frac{1}{2^n}Q(x_1,\ldots,x_n)\times f(y_1,\ldots,x_n)A(y_1,\ldots,x_n). \tag{6}$$

Inserting Q, f, and A gives the probability of guessing correctly:

$$P_C=\frac{1}{2}\left(1+\frac{B}{\sum_{x_1,\ldots,x_n=0}^{2^m-1}|g(x_1,\ldots,x_n)|}\right), \tag{7}$$

in the classical protocol and

$$P_Q=\frac{1}{2}\left(1+\frac{S}{\sum_{x_1,\ldots,x_n=0}^{2^m-1}|g(x_1,\ldots,x_n)|}\right) \tag{8}$$

in the quantum case.

III. BOUND ENTANGLEMENT AS A RESOURCE

We now come to the explicit example. We choose $n=3$, so there are three separated parties. They share the state

$$\rho=\sum_{i=1}^{4} p_i|\psi_i\rangle\langle\psi_i| \tag{9}$$

with $p_1=0.0636039$, $p_2=p_3=0.273734$, $p_4=0.388929$, and

$$\begin{aligned}
|\psi_1\rangle &= 0.183013|000\rangle-0.408248(|001\rangle+|010\rangle+|100\rangle)\\
&\quad+0.683013|111\rangle,\\
|\psi_2\rangle &= -0.344106(|001\rangle-2|010\rangle+|100\rangle)\\
&\quad+0.219677(|011\rangle-2|101\rangle+|110\rangle),\\
|\psi_3\rangle &= 0.596008(|100\rangle-|001\rangle)+0.380492(|110\rangle-|011\rangle),\\
|\psi_4\rangle &= -0.933013|000\rangle+0.149429(|011\rangle+|101\rangle+|110\rangle)\\
&\quad+0.25|111\rangle.
\end{aligned}$$

It was introduced by Vértesi and Brunner in Ref. [8]. See the reference for an analytic expression for the amplitudes. It is constructed such that it is symmetric under permutations of the parties and invariant under partial transpose with respect to party 3. The last condition is sufficient for ρ to be biseparable on the partition (1,2)|3 [21]. Together these conditions ensure that the state is separable along any biseparation. Therefore, it is fully nondistillable. Here "fully nondistillable" refers to the fact that none of the three groupings (1,2)|3, (1,3)|2, and (2,3)|1 of subsystems to parties is distillable. Vértesi and Brunner also found that ρ can be used to violate the Bell inequality

$$\begin{aligned}
-13\leqslant \operatorname{sym}[&A_1+A_1B_2-A_2B_2-A_1B_1C_1\\
&-A_2B_1C_1+A_2B_2C_2]\leqslant 3,
\end{aligned} \tag{10}$$

which is listed under number 5 in Ref. [22]. The symbol $\operatorname{sym}[X]$ denotes the symmetrization of X with respect to the three parties, e.g., $\operatorname{sym}[A_1B_2]=A_1B_2+A_1C_2+A_2B_1+A_2C_1+B_1C_2+B_2C_1$. Because ρ is fully nondistillable and nonlocal it is fully bound entangled.

We now use the method of homogenization described by Wu and Żukowski in Ref. [23]: By adding a constant 5 to inequality (10), the bounds become symmetric. Then we introduce new observables A_0, B_0, and C_0 which also take the values -1 and 1. Substituting the observables A_i by A_i/A_0, B_i by B_i/B_0, and C_i by C_i/C_0 and factoring out $1/(A_0B_0C_0)$, one expands lower-order correlation terms to full correlation terms. We arrive at the inequality

$$\begin{aligned}
&\left|\frac{1}{A_0B_0C_0}\operatorname{sym}[5A_0B_0C_0+A_1B_0C_0+A_1B_2C_0-A_2B_2C_0\right.\\
&\quad\left.-A_1B_1C_1-A_2B_1C_1+A_2B_2C_2]\right|\leqslant 8\\
\Leftrightarrow\ &|\operatorname{sym}[5A_0B_0C_0+A_1B_0C_0+A_1B_2C_0-A_2B_2C_0\\
&\quad-A_1B_1C_1-A_2B_1C_1+A_2B_2C_2]|\leqslant 8,
\end{aligned} \tag{11}$$

which is expression H05 given in Table I of Ref. [23]. This inequality has the required form to link to the communication complexity problem described above. Like in Ref. [8] we

choose

$$A_1 = B_1 = C_1 = \begin{pmatrix} \cos\left(\frac{2\pi}{9}\right) & \sin\left(\frac{2\pi}{9}\right) \\ \sin\left(\frac{2\pi}{9}\right) & -\cos\left(\frac{2\pi}{9}\right) \end{pmatrix} \tag{12}$$

and

$$A_2 = B_2 = C_2 = \begin{pmatrix} \sin\left(\frac{\pi}{18}\right) & -\cos\left(\frac{\pi}{18}\right) \\ -\cos\left(\frac{\pi}{18}\right) & -\sin\left(\frac{\pi}{18}\right) \end{pmatrix}. \tag{13}$$

For the new observables it is sufficient to choose $A_0 = B_0 = C_0 = \mathbb{1}$. With these observables we calculate the left-hand side of inequality (11) using the quantum-mechanical expectation values as

$$S = 5 + 3.00685 = 8.00685. \tag{14}$$

This violation of the Bell inequality (11) implies a quantum advantage in the quantum communication complexity task associated with it. We write the coefficients in front of correlations $A_{x_1} B_{x_2} C_{x_3}$ in inequality (11) as

$$\begin{aligned} g(x_1,x_2,x_3) = &\left\{2\left[\left(\delta_{x_1,x_2,x_3} + x_1 + x_2 + x_3\right) \bmod 2\right] - 1\right\} \\ &\times \left(1 + 4\delta_{0,x_1,x_2,x_3}\right)\left(1 - \delta_{2,(x_1+x_2+x_3) \bmod 3}\right) \\ &\times \prod_{i=1}^{3}\left(1 - \delta_{3,x_i}\right), \end{aligned} \tag{15}$$

where the symbol δ is 1 if all subscripts are equal and 0 otherwise. The firstfactor of Eq. (15) gives the sign of the coefficient while the others define the probability distribution for x_1, x_2, and x_3 [see Eq. (2)]. The task for the three parties is to calculate the function

$$\begin{aligned} f &= y_1 y_2 y_3 \operatorname{sign}\left[g(x_1,x_2,x_3)\right] \\ &= y_1 y_2 y_3 \left\{2\left[\left(\delta_{x_1,x_2,x_3} + x_1 + x_2 + x_3\right) \bmod 2\right] - 1\right\}, \end{aligned} \tag{16}$$

which is basically the parity of the sum of x_1, x_2, x_3, and δ_{x_1,x_2,x_3}. As we chose $A_0 = B_0 = C_0 = \mathbb{1}$, a party i performs no measurement if $x_i = 0$ and simply sends y_i. Using equations (7) and (8) we get $P_C = 0.681818$ and $P_Q = 0.681974$. This shows that, albeit slightly, the parties still can increase the probability of success if they share the bound entangled state ρ, as compared to any classical protocol. This is striking, especially if you remind yourself that the state ρ is separable along any bipartition; i.e., it satisfies all Bell inequalities across every bipartition. The presented task is a simple application associated with the Bell inequality (10) the authors of Ref. [8] were asking for. We note that a similar advantage can be shown using the nonlocal games from Ref. [24].

ACKNOWLEDGMENTS

We thank Sylvia Bratzik and Dagmar Bruß for advising us on this topic. C.B. acknowledges support from the European Commission, Q-ESSENCE (Grant No. 248095), and the Austrian Science Fund (FWF): SFB-FOCUS, P 24621, and the doctoral program CoQuS.

[1] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*, Cambridge Series on Information and the Natural Sciences (Cambridge University Press, Cambridge, 2000).
[2] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).
[3] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **80**, 5239 (1998).
[4] J. S. Bell, Physics **1**, 195 (1964).
[5] A. Peres, Found. Phys. **29**, 589 (1999).
[6] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).
[7] Y.-C. Liang, L. Masanes, and D. Rosset, Phys. Rev. A **86**, 052115 (2012).
[8] T. Vértesi and N. Brunner, Phys. Rev. Lett. **108**, 030403 (2012).
[9] W. Dür, Phys. Rev. Lett. **87**, 230402 (2001).
[10] R. Augusiak and P. Horodecki, Phys. Rev. A **74**, 010305 (2006).
[11] A. Acín, Phys. Rev. Lett. **88**, 027901 (2001).
[12] P. Horodecki, M. Horodecki, and R. Horodecki, Phys. Rev. Lett. **82**, 1056 (1999).
[13] L. Masanes, J. Math. Phys. **49**, 022102 (2008).
[14] L. Masanes, Phys. Rev. Lett. **96**, 150501 (2006).
[15] N. Brunner and D. Cavalcanti, arXiv:1210.1556.
[16] I. Chattopadhyay and D. Sarkar, Phys. Lett. A **365**, 273 (2007).
[17] K. Horodecki, L. Pankowski, M. Horodecki, and P. Horodecki, IEEE Trans. Inf. Theory **54**, 2621 (2008).
[18] E. Kushilevitz and N. Nisan, *Communication Complexity* (Cambridge University Press, New York, 1997).
[19] C. Brukner, M. Żukowski, J.-W. Pan, and A. Zeilinger, Phys. Rev. Lett. **92**, 127901 (2004).
[20] M. Epping, Master's thesis, University of Vienna, Austria, 2012.
[21] B. Kraus, J. I. Cirac, S. Karnas, and M. Lewenstein, Phys. Rev. A **61**, 062302 (2000).
[22] C. Sliwa, Phys. Lett. A **317**, 165 (2003).
[23] Y.-C. Wu and M. Żukowski, Phys. Rev. A **85**, 022119 (2012).
[24] J. Silman, S. Machnes, and N. Aharon, Phys. Lett. A **372**, 3796 (2008).

B

Quantifying entanglement with scattering experiments

Title:	Quantifying entanglement with scattering experiments
Authors:	Oliver Marty, M.E., Hermann Kampermann, Dagmar Bruß, Martin B. Plenio, and Marcus Cramer
Journal:	Physical Review B
Impact factor:	3.736
Date of submission:	17 October 2013
Publication status:	Published
Contribution by M.E.:	Second author (input approx. 20%)
Results:	Construction of entanglement witnesses based on typical observables in neutron scattering. Generalizes previous results and contains numerical simulations for different interaction models.

Quantifying entanglement with scattering experiments

O. Marty,[1,2] M. Epping,[3] H. Kampermann,[3] D. Bruß,[3] M. B. Plenio,[1,2] and M. Cramer[1,2]
[1]*Institut für Theoretische Physik, Albert-Einstein Allee 11, Universität Ulm, D-89069 Ulm, Germany*
[2]*Institute for Integrated Quantum Science and Technology, Albert-Einstein Allee 11, Universität Ulm, D-89069 Ulm, Germany*
[3]*Institute for Theoretical Physics III, Heinrich-Heine-Universität Düsseldorf, Universitätsstrasse 1, D-40225 Düsseldorf, Germany*
(Received 17 October 2013; revised manuscript received 29 January 2014; published 19 March 2014)

We show how the entanglement contained in states of spins arranged on a lattice may be lower bounded with observables arising in scattering experiments. We focus on the partial differential cross section obtained in neutron scattering from magnetic materials but our results are sufficiently general such that they may also be applied to, e.g., optical Bragg scattering from ultracold atoms in optical lattices or from ion chains. We discuss resonating valence bond states and ground and thermal states of experimentally relevant models—such as the Heisenberg, Majumdar-Ghosh, and *XY* models—in different geometries and with different spin numbers. As a by-product, we find that for the one-dimensional *XY* model in a transverse field such measurements reveal factorization and the quantum phase transition at zero temperature.

DOI: 10.1103/PhysRevB.89.125117 PACS number(s): 03.67.Mn, 03.65.Ud, 28.20.Cz, 78.70.Nx

I. INTRODUCTION

Entanglement is a key resource for performing quantum information tasks [1,2]. At low temperatures, it occurs naturally in quantum many-body systems and its amount (more concretely, its scaling with the size of system partitions) relates to the complexity of descriptions of such systems [3–7]. It also serves to characterize exotic states of matter, a prominent example being topological spin liquids; see, e.g., the recent Refs. [8,9]. While the task of merely verifying that entanglement is present [10,11] is quite established and it has been demonstrated in a number of experiments [12–22], quantifying its amount rigorously and without any assumptions is a delicate task and has only very recently been experimentally achieved for a large many-body system of bosons in optical lattices in Ref. [23] (see also, e.g., Ref. [24] where the entanglement of a small photonic system was quantified using few measurements). Generally speaking, the difficulty increases with the number of particles carrying the quantum information, i.e., it is especially delicate for large systems for which the available measurements are usually very limited and very far from being informationally complete (in which case full state tomography [15,25,26] would be possible). Here, we are interested in such large systems, namely, a large number of spins arranged on a lattice. In order to quantify the amount of entanglement that is shared between the spins, we rely only on global measurements typically obtained in scattering experiments. We achieve this by generalizing results of the recent Refs. [27,28] to arbitrary spin and to more general observables. In the case of neutron scattering from magnetic materials, this enables us to quantify entanglement for arbitrary lattice geometries relying solely on the Fourier transform of the scattering cross section (or, alternatively, measurements that do not resolve the energy of the scattered neutrons). Our strategy adopts a principle from quantum information theory that is simple yet powerful [29–33]: Given certain observables and their experimentally obtained expectation values, we ask what is the minimal amount of entanglement that is consistent with the obtained outcomes, i.e., given the expectation values of the observables, we minimize over all density matrices that are consistent with them. In this way, we arrive at the least amount of entanglement that is consistent with the measurement outcomes and thus we put a lower bound on the entanglement contained in the sample on which the measurements were performed. By the very nature of this principle, we need not make *any* assumptions on the system (such as, e.g., the temperature, details of external potentials, the Hamiltonian governing the system, or even the system being in equilibrium).

We consider observables that arise in scattering experiments from N spins arranged on a lattice. Examples include optical Bragg scattering from ultracold atoms in optical lattices [34] or from ion chains [35] and neutron scattering from magnetic materials [36]. These observables may be written as

$$\hat{S}(\boldsymbol{q}) = \sum_{\alpha,\beta} M_{\alpha,\beta}(\boldsymbol{q})\hat{S}_{\alpha,\beta}(\boldsymbol{q}), \tag{1}$$

where, usually, $\boldsymbol{q} = \boldsymbol{k}_{\text{out}} - \boldsymbol{k}_{\text{in}}$ is the scattering vector, i.e., the difference between the final and the initial wave vectors. Here,

$$\hat{S}_{\alpha,\beta}(\boldsymbol{q}) = \sum_{i,j=1}^{N} f^*_{i,\alpha}(\boldsymbol{q}) f_{j,\beta}(\boldsymbol{q}) e^{i\boldsymbol{q}(\boldsymbol{r}_i - \boldsymbol{r}_j)} \hat{S}_i^{\alpha} \hat{S}_j^{\beta}, \tag{2}$$

where $\boldsymbol{r}_i$ is the position of the i'th spin with corresponding spin operators $\hat{S}_i^{\alpha}$, $\alpha = x,y,z$, and spin quantum number s, and the coefficients $M_{\alpha,\beta}(\boldsymbol{q})$ and $f_{i,\alpha}(\boldsymbol{q})$ depend on the system under consideration. While keeping our results as general as possible, we will focus on neutron scattering experiments, in which such observables arise as follows. The neutrons interact magnetically with the atoms of the target sample, whose magnetic moments mostly originate from the orbital motion and spins of unpaired electrons. In many cases an effective spin value can be assigned to either the magnetic atoms or to the entire unit-cell. [36] With the formalism introduced by Van Hove in Ref. [37], the partial differential cross-section can be expressed in terms of time-dependent correlation functions. Accordingly, for unpolarized neutrons,

the magnetic cross-section is proportional to [36]

$$\frac{d^2\sigma}{d\Omega d\omega} \propto \frac{k_{\text{out}}}{k_{\text{in}}} \sum_{\substack{\alpha,\beta \\ i,j}} (\delta_{\alpha,\beta} - \bar{q}_\alpha \bar{q}_\beta) f^*_{i,\alpha}(\boldsymbol{q}) f_{j,\beta}(\boldsymbol{q}) e^{i\boldsymbol{q}(\boldsymbol{r}_i - \boldsymbol{r}_j)} \times \int dt\, e^{-i\omega t} \langle \hat{S}^\alpha_i \hat{S}^\beta_j(t) \rangle, \tag{3}$$

where ω is the energy transferred to the sample and Ω the solid angle under which the scattered neutrons are observed. Furthermore, $f_{i,\alpha}(\boldsymbol{q}) = F_i(\boldsymbol{q}) g_{i,\alpha}$, where $F_i(\boldsymbol{q})$ and $g_{i,\alpha}$ denote the magnetic form factor and the Landé factor of the ith site, respectively, and $\bar{\boldsymbol{q}} = \boldsymbol{q}/|\boldsymbol{q}|$. In general, we allow the g factor to be anisotropic and $f_{i,\alpha}(\boldsymbol{q})$ to be site dependent, where i labels the lattice sites with corresponding effective values of $f_{i,\alpha}$ and $\hat{S}^\alpha_i$ (corresponding to an effective spin quantum number s). The magnetic form factor $F_i(\boldsymbol{q})$ stems from the finite extent of the electron orbitals seen by the neutron with wavelength of the order of interatomic distances. To determine it, a detailed knowledge about the electronic wave functions of the magnetic atoms in the scatterer is required, and its values may be found in the literature. As $k_{\text{in,out}}$ are known, one may multiply (3) by $k_{\text{in}}/k_{\text{out}}$ and take the Fourier transform to obtain the instantaneous scattering function $S(\boldsymbol{q}) = \langle \hat{S}(\boldsymbol{q}) \rangle$, where $\hat{S}(\boldsymbol{q})$ is as in Eq. (1) with $M_{\alpha,\beta}(\boldsymbol{q}) = \delta_{\alpha,\beta} - \bar{q}_\alpha \bar{q}_\beta$. Alternatively, $S(\boldsymbol{q})$ may be obtained if the requirements of the static approximation are fulfilled [38] and the final energy is not resolved. For quasi-one- or two-dimensional systems one may also consider a special scattering geometry [39–41] to obtain $S(\boldsymbol{q})$.

In Sec. II, we show how a lower bound to the entanglement shared among N spins—as quantified in terms of the *best separable approximation* [42] or the *(generalized) robustness of entanglement* [43,44]—may be obtained from the expectation value of $\hat{S}(\boldsymbol{q})$ in Eq. (1). In this way, we quantify entanglement of a collection of N spins without any assumption on the system. In Secs. III and IV we show that our method allows quantification of the entanglement of ground and thermal states corresponding to several model Hamiltonians. We conclude with a summary and outlook in Sec. V.

II. MAIN RESULTS

In this section we will show how observables as in Eq. (1) may serve as lower bounds to the entanglement. We will consider several entanglement monotones and a particular simple form will be derived for the best separable approximation (BSA) $\mathcal{E}_{\text{BSA}}[\hat{\varrho}]$ in the neutron scattering setting: For any scattering vector $\boldsymbol{q}$, we find (see below and Appendix A for details)

$$\mathcal{E}_{\text{BSA}}[\hat{\varrho}] \geqslant 1 - \frac{1}{c_{\min}} \sum_{\alpha,\beta} (\delta_{\alpha,\beta} - \bar{q}_\alpha \bar{q}_\beta) \langle \hat{S}_{\alpha,\beta}(\boldsymbol{q}) \rangle, \tag{4}$$

where $c_{\min}$ is a constant that depends on the spin quantum number s and the magnetic form factors $F_i(\boldsymbol{q})$ and Landé factors $g_{i,\alpha}$. Hence, a measurement of the Fourier transform of the magnetic scattering cross section at a single scattering vector directly provides a lower bound to the entanglement contained in the sample. A numerical analysis of the above bound may be found in Sec. III (see Figs. 1–3) for different physical models that describe, among others, the magnetic compounds summarized in Table I.

In the remainder of this section, we detail the derivation of the above bound and the bounds on robustness of entanglement measures. We start with a detailed description of the scattering observables under consideration.

A. The observables under consideration

We will see below that for many systems, a measurement of $\langle \hat{S}(\boldsymbol{q}) \rangle$ at a single scattering vector $\boldsymbol{q}$ suffices to put meaningful tight lower bounds on the entanglement quantified via the best separable approximation. For the robustness measures, however, we have found that measurements at a single scattering vector $\boldsymbol{q}$ do not suffice to obtain nontrivial bounds for large systems (see also Ref. [27]). To this end, we incorporate knowledge of $\langle \hat{S}(\boldsymbol{q}) \rangle$ at several $\boldsymbol{q}$ by slightly generalizing the observables in the Introduction to observables of the form

$$\hat{S} = \sum_{\boldsymbol{q} \in Q} \hat{S}(\boldsymbol{q}). \tag{5}$$

As we will see, this summation over measurements obtained at several scattering vectors will result in positive entanglement bounds even in the thermodynamic limit. Here, $Q \subset \mathbb{R}^3$ is some collection of scattering vectors and $\hat{S}(\boldsymbol{q})$ is defined as in Eq. (1), where we make the following assumptions on the coefficients $M_{\alpha,\beta}(\boldsymbol{q}) \in \mathbb{C}$ and $f_{i,\alpha}(\boldsymbol{q}) \in \mathbb{C}$: We assume that the 3×3 matrix $M(\boldsymbol{q})$ with entries $M_{\alpha,\beta}(\boldsymbol{q})$ is Hermitian, i.e., $M_{\alpha,\beta}(\boldsymbol{q}) = M^*_{\beta,\alpha}(\boldsymbol{q})$, and positive semidefinite. We further assume that for each $i = 1, \ldots, N$ the 3×3 matrix $M^{(i)}$ with entries

$$M^{(i)}_{\alpha,\beta} = \sum_{\boldsymbol{q} \in Q} f^*_{i,\alpha}(\boldsymbol{q}) f_{i,\beta}(\boldsymbol{q}) M_{\alpha,\beta}(\boldsymbol{q}) \tag{6}$$

is real and symmetric, i.e., $M^{(i)}_{\alpha,\beta} = M^{(i)}_{\beta,\alpha} \in \mathbb{R}$. All these assumptions are fulfilled, e.g., in the neutron scattering setting, for which we have $M(\boldsymbol{q}) = \mathbb{1} - \bar{\boldsymbol{q}}\bar{\boldsymbol{q}}^t$ [see Eq. (3)] and $f_{i,\alpha}(\boldsymbol{q}) = F_i(\boldsymbol{q}) g_{i,\alpha}$ with $g_{i,\alpha} \in \mathbb{R}$.

B. Lower bounds to the entanglement

In what follows, we consider multipartite entanglement in the following sense. Every state $\hat{\varrho}$ that is not fully separable, i.e., of the form

$$\sum_n p_n \bigotimes_{i=1}^N \hat{\varrho}^{(n)}_i \in \mathcal{S}, \tag{7}$$

with $p_n > 0$ and $\sum_n p_n = 1$, will be called entangled. Here, we denoted the set of separable states by $\mathcal{S}$. The degree of entanglement is then quantified using entanglement monotones [1,2], that is, functionals $\mathcal{E}[\hat{\varrho}]$ that do not increase under local operations and classical communication. The monotones under consideration are part of a larger family of monotones that may be expressed as [30]

$$\mathcal{E}_{\mathcal{C}}[\hat{\varrho}] = - \min_{\hat{W} \in \mathcal{W} \cap \mathcal{C}} \text{tr}[\hat{W}\hat{\varrho}] \tag{8}$$

with the convention that $\mathcal{E}_{\mathcal{C}}[\hat{\varrho}] = 0$ if the minimization results in a positive number. Here, $\mathcal{W}$ is the set of *entanglement*

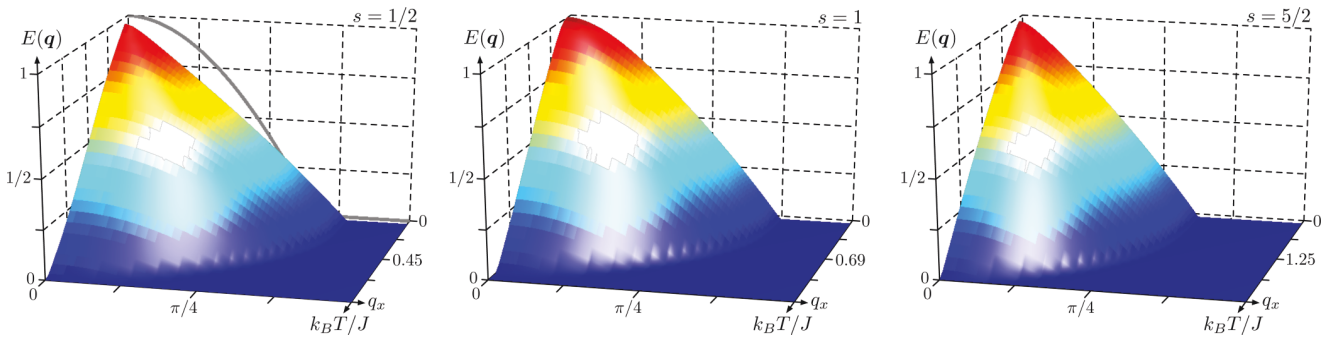


FIG. 1. (Color online) Lower bound $E_{\mathrm{BSA}}[\hat{\varrho}](\boldsymbol{q}) = E_{\mathrm{BSA}}[\hat{\varrho}](q_x)$ [Eq. (20)] to the entanglement $\mathcal{E}_{\mathrm{BSA}}[\hat{\varrho}]$ vs temperature for thermal states of the quasi-one-dimensional Heisenberg model Eqs. (26) and (27) for $s = 1/2,1,5/2$ (left to right) and $L = 900$ [56]. The gray solid line in the leftmost plot depicts the entanglement bound for a ground state of the Majumdar-Ghosh model in the limit $L \to \infty$. Note that for all shown models the bound $\mathcal{E}_{\mathrm{BSA}}[\hat{\varrho}] \leqslant 1$, which holds for any state $\hat{\varrho}$, is attained at $T = 0$, $q_x = 0$.

witnesses (Hermitian operators with non-negative expectation value for every separable state, i.e.,$\langle \hat{W} \rangle_{\mathrm{sep.}} \geqslant 0$; see Ref. [11] for a review) and the set $\mathcal{C}$ depends on the chosen entanglement measure: If

$$\mathcal{C} = \{\hat{W} \in \mathcal{W} \,|\, \mathbb{1} + \hat{W} \geqslant 0\} \tag{9}$$

then $\mathcal{E}_{\mathcal{C}}[\hat{\varrho}] = \mathcal{E}_{\mathrm{BSA}}[\hat{\varrho}]$ quantifies entanglement in terms of the best separable approximation [42], which, in essence, answers the question of how much of a separable state is contained in the state $\hat{\varrho}$. For

$$\mathcal{C} = \{\hat{W} \in \mathcal{W} \,|\, \mathrm{tr}[\hat{W}\hat{\sigma}] \leqslant 1 \,\forall\, \hat{\sigma} \in \mathcal{S}\} \tag{10}$$

we have $\mathcal{E}_{\mathcal{C}}[\hat{\varrho}] = \mathcal{E}_{R}[\hat{\varrho}]$, quantifying entanglement in terms of the robustness of entanglement. Finally, if

$$\mathcal{C} = \{\hat{W} \in \mathcal{W} \,|\, \mathbb{1} - \hat{W} \geqslant 0\} \tag{11}$$

then $\mathcal{E}_{\mathcal{C}}[\hat{\varrho}] = \mathcal{E}_{\mathrm{GR}}[\hat{\varrho}]$ is the generalized robustness of entanglement. These robustness measures [43,44] quantify the minimal amount of noise (in the form of a general state in the case of the generalized robustness and in the form of a separable state in the case of the robustness) that must be mixed in to make $\hat{\varrho}$ separable.

Instead of minimizing over all the entanglement witnesses $\hat{W} \in \mathcal{W} \cap \mathcal{C}$, we construct a single member of the set $\mathcal{W} \cap \mathcal{C}$ of the form

$$\hat{W}_{\hat{S},\mathcal{C}} = a_{\mathcal{C}}\hat{S} + b_{\mathcal{C}}\mathbb{1} \tag{12}$$

with appropriate real coefficients $a_{\mathcal{C}}$ and $b_{\mathcal{C}}$ [which will depend on the set of scattering vectors Q and the matrices $M(\boldsymbol{q})$] and $\hat{S}$ as in the previous section. By inspection of Eq. (8), we see that any $\hat{W} \in \mathcal{W} \cap \mathcal{C}$ gives a lower bound to the entanglement monotone and thus for any state $\hat{\varrho}$, one has

$$\mathcal{E}_{\mathcal{C}}[\hat{\varrho}] \geqslant -a_{\mathcal{C}}\langle \hat{S} \rangle - b_{\mathcal{C}}, \tag{13}$$

which depends only on the expectation value $\langle \hat{S} \rangle = \mathrm{tr}[\hat{S}\hat{\varrho}]$. The coefficients are found in the following way. As the matrices $M(\boldsymbol{q})$ are assumed to be positive semidefinite, it is straightforward to show that $\hat{S}$ is also positive semidefinite; see Appendix A. Furthermore, one may derive bounds on the minimal and maximal achievable expectation values in fully separable states

$$c_{\mathrm{min}} \leqslant \langle \hat{S} \rangle_{\mathrm{sep.}} \leqslant c_{\mathrm{max}}. \tag{14}$$

Together with the positive semidefiniteness of $\hat{S}$, such bounds allow us to arrive at witnesses that are of the form as in Eq. (12) and members of the set $\mathcal{W} \cap \mathcal{C}$. One readily verifies that the coefficients

$$\begin{aligned} a_{\mathrm{BSA}} &= \frac{1}{c_{\mathrm{min}}}, \quad b_{\mathrm{BSA}} = -1, \\ a_R &= -\frac{1}{c_{\mathrm{max}} - c_{\mathrm{min}}}, \quad b_R = -c_{\mathrm{max}} a_R, \\ a_{\mathrm{GR}} &= -\frac{1}{c_{\mathrm{max}}}, \quad b_{\mathrm{GR}} = 1, \end{aligned} \tag{15}$$

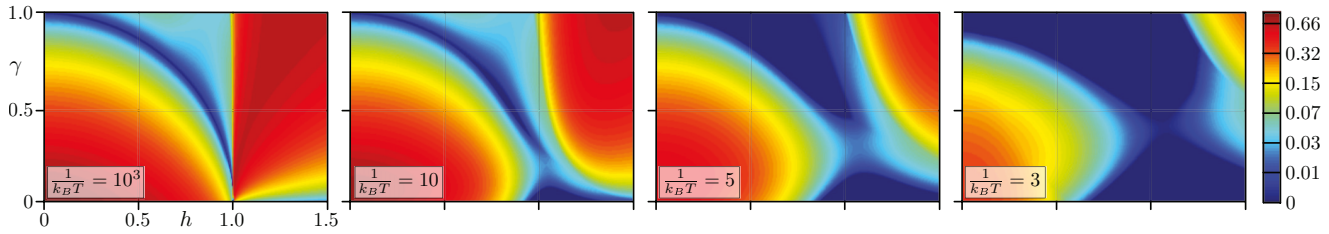


FIG. 2. (Color online) Lower bound $E_{\mathrm{BSA}}[\hat{\varrho}]$ [Eq. (20)] to the best separable approximation $\mathcal{E}_{\mathrm{BSA}}[\hat{\varrho}]$ for thermal states of a system of mutually uncoupled chains, Eq. (26), each of which is described by the XY model in Eq. (28). The linear dimension is $L = 200$ and the depicted bounds are obtained by optimizing $E_{\mathrm{BSA}}[\hat{\varrho}](\boldsymbol{q})$ over certain $\boldsymbol{q}$ and over the orientation of the chains (see the main text). For low temperature, the phase boundary and factorization circle $\gamma^2 + h^2 = 1$ are clearly visible. Note also that for higher temperature, there are regions on this circle with finite entanglement.

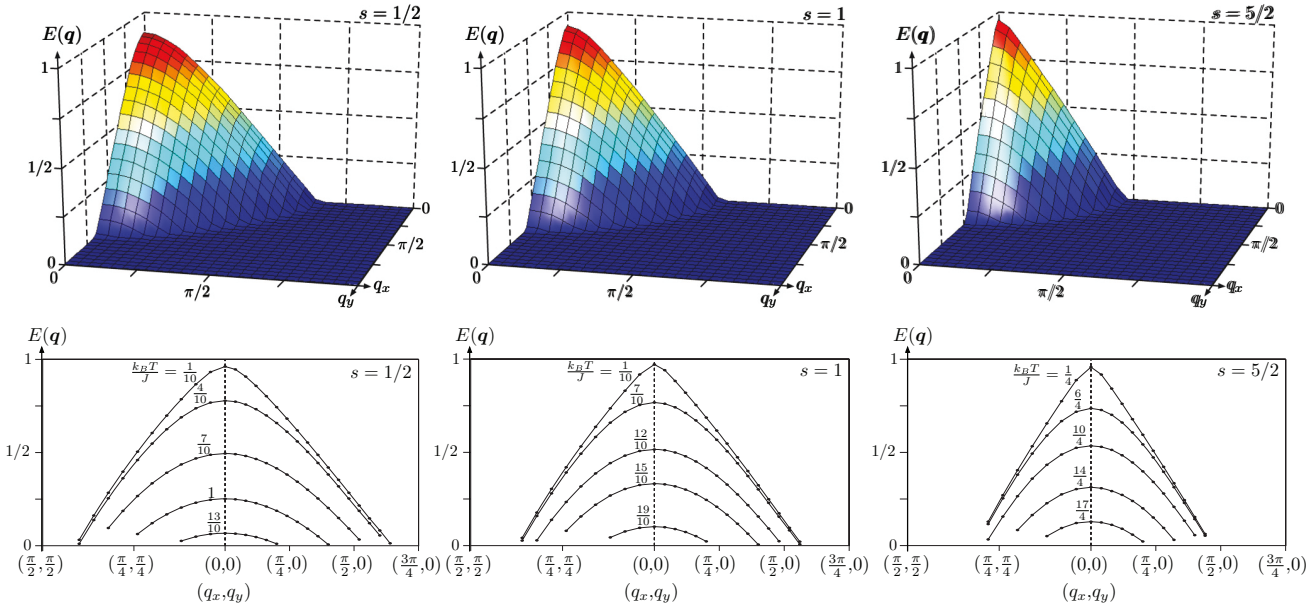


FIG. 3. (Color online) Lower bound $E_{\mathrm{BSA}}[\hat{\varrho}](\boldsymbol{q}) = E_{\mathrm{BSA}}[\hat{\varrho}](q_x,q_y)$ [Eq. (20)] to the entanglement $\mathcal{E}_{\mathrm{BSA}}[\hat{\varrho}]$ for thermal states of the quasi-two-dimensional Heisenberg model in Eq. (29) with $s = 1/2,1,5/2$ (left to right). The top row shows $E_{\mathrm{BSA}}[\hat{\varrho}](q_x,q_y)$ for $T/J = 1/4$, and the bottom row shows cuts through the first Brillouin zone for different temperatures. Cuts are along the line from $(q_x,q_y) = (\pi/2,\pi/2)$ to $(0,0)$ and and along the x axis from $(0,0)$ to $(3\pi/4,0)$. The simulated system size is $L = 30$ [56]. The lines are guides to the eye and only data points with $E_{\mathrm{BSA}}[\hat{\varrho}](q_x,q_y) > 0$ and $(q_x,q_y) \in 2\pi\{0,\ldots,L-1\}^{\times 2}/L$ are shown.

fulfil the necessary requirements as defined in Eqs. (9)–(11). It remains to make the bounds $c_{\min}$ and $c_{\max}$ explicit. To obtain these bounds, we will make use of ingredients that also enter the derivation of spin-squeezing inequalities [45–47], such as the reduction to bounds on single-spin variances as, e.g., in Eq. (16). In contrast to the situation encountered for spin-squeezing inequalities, however, we have the added difficulty of not having access to first moments and having to consider $\boldsymbol{q} \neq \boldsymbol{0}$ and general $M_{\alpha,\beta}(\boldsymbol{q})$.

1. Lower bound to the best separable approximation

For each $i = 1,\ldots,N$, denote the eigenvalues of the 3×3 matrix $M^{(i)}$ in Eq. (6) by $m_\alpha^{(i)}$. For product states, and so for each summand in Eq. (7), the expectation value $\langle \hat{S}_i^\alpha \hat{S}_j^\beta \rangle$ can be written as the product $\langle \hat{S}_i^\alpha \rangle \langle \hat{S}_j^\beta \rangle$ for lattice sites $i \neq j$. The resulting expression can then be bounded with the help of the eigenvalues of the coefficient matrices $M^{(i)}$ in the following way (see Appendix A for details):

$$c_{\min} = \sum_{i=1}^{N} \min_{|\psi\rangle} \sum_{\alpha} m_\alpha^{(i)} \left(\langle \psi | \hat{S}_\alpha^2 | \psi \rangle - \langle \psi | \hat{S}_\alpha | \psi \rangle^2 \right), \quad (16)$$

where $\hat{S}_\alpha$, $\alpha = x,y,z$, are the spin operators for a single spin. For each i, the minimization over pure states $|\psi\rangle \in \mathbb{C}^{2s+1}$ may be solved numerically; to obtain analytical solutions, the methods developed in Refs. [45–47] may be useful. For some special cases, $c_{\min}$ may be given explicitly: For example, for $f_{i,\alpha}(\boldsymbol{q}) = f(\boldsymbol{q})$ and $M_{\alpha,\beta}(\boldsymbol{q}) = \delta_{\alpha,\beta}/|f(\boldsymbol{q})|^2$ (similar observables were considered in Ref. [28]), one finds

$$c_{\min} = N|Q|s, \quad (17)$$

where we recall that s is the spin quantum number corresponding to the $\hat{S}_i^\alpha$ and $|Q|$ denotes the number of scattering vectors in the set Q. If $f_{i,\alpha}(\boldsymbol{q}) = f(\boldsymbol{q})$, if $M(\boldsymbol{q}) = (\mathbb{1} - \bar{\boldsymbol{q}}\bar{\boldsymbol{q}}^t)/|f(\boldsymbol{q})|^2$ as in the neutron scattering setting, and if Q contains only one scattering vector, we have

$$c_{\min} = NC_s, \quad (18)$$

where [48]

$$C_s = \begin{cases} \frac{1}{4} & \text{for} \quad s = \frac{1}{2}, \\ \frac{7}{16} & \text{for} \quad s = 1, \end{cases} \quad (19)$$

and further values are listed in Ref. [49]. The latter yields the following bound on the best separable approximation. For each $\boldsymbol{q} \in \mathbb{R}^3$, inserting Eq. (18) into Eqs. (13) and (15) leads to

$$\mathcal{E}_{\mathrm{BSA}}[\hat{\varrho}] \geqslant 1 - \sum_{\alpha,\beta} \frac{\delta_{\alpha,\beta} - \bar{q}_\alpha \bar{q}_\beta}{NC_s} \sum_{i,j} e^{i\boldsymbol{q}(\boldsymbol{r}_i - \boldsymbol{r}_j)} \langle \hat{S}_i^\alpha \hat{S}_j^\beta \rangle$$
$$=: E_{\mathrm{BSA}}[\hat{\varrho}](\boldsymbol{q}). \quad (20)$$

Note that this is a general bound for *any* state. Whenever the expectation value $E_{\mathrm{BSA}}[\hat{\varrho}](\boldsymbol{q})$ is accessible, it provides a lower bound to the entanglement contained in $\hat{\varrho}$—no matter what the underlying Hamiltonian of the system or the temperature might be, no matter whether the system is in equilibrium or not. If, depending on the experimental situation, $E_{\mathrm{BSA}}[\hat{\varrho}](\boldsymbol{q})$ is not accessible, i.e., the special form of $M(\boldsymbol{q})$ and $f_{i,\alpha}(\boldsymbol{q})$ is not given, one has to use the observable given in Eqs. (1) and (2) and the general bound in Eq. (16) needs to be applied. Note that, for any state, $\mathcal{E}_{\mathrm{BSA}}[\hat{\varrho}] \leqslant 1$, i.e., whenever we find $E_{\mathrm{BSA}}[\hat{\varrho}](\boldsymbol{q}) = 1$, the bound is in fact equal to the exact entanglement. In Sec. III, we present $E_{\mathrm{BSA}}[\hat{\varrho}](\boldsymbol{q})$ for several

numerically simulated states (see Figs. 1–3), and in Sec. IV, we discuss some examples for which $E_{\mathrm{BSA}}[\hat{\varrho}](\boldsymbol{q})$ may be obtained analytically.

2. Lower bound to robustness measures

The derivation of the general bound may be found in Appendix A; for clarity, we state it here only for the following special case. We let $f_{i,\alpha}(\boldsymbol{q}) = f(\boldsymbol{q})$ and $M_{\alpha,\beta}(\boldsymbol{q}) = \delta_{\alpha,\beta}/|f(\boldsymbol{q})|^2$ such that our observable reads

$$\hat{S} = \sum_{\boldsymbol{q}\in Q} \sum_{i,j=1}^{N} e^{i\boldsymbol{q}(\boldsymbol{r}_i - \boldsymbol{r}_j)} \sum_{\alpha} \hat{S}_i^{\alpha} \hat{S}_j^{\alpha}. \tag{21}$$

We further assume that the $N = N_1 N_2 N_3$ spins are arranged on a finite three-dimensional Bravais lattice with primitive vectors $\boldsymbol{a}_d$, $d = 1,2,3$, such that $\boldsymbol{r}_i = \sum_{d=1}^{3} i_d \boldsymbol{a}_d$ with $i_d \in \{1,\ldots,N_d\}$. Further we assume that

$$Q \subset \left\{ \sum_{d=1}^{3} q_d \boldsymbol{b}_d \,\middle|\, q_d = \frac{i-1}{N_d},\, i \in \{1,\ldots,N_d\} \right\} =: \mathcal{Q}, \tag{22}$$

where the $\boldsymbol{b}_d$ are the reciprocal primitive vectors. The upper bound is derived in Appendix A and reads

$$c_{\max} = N|Q|s + N^2 s^2; \tag{23}$$

see Eq. (A18). Hence, whenever the expectation of the observable in Eq. (21) may be obtained, we have the following lower bounds to the robustness measures for *any* state. For all $Q \subset \mathcal{Q}$, we have

$$\begin{aligned} \mathcal{E}_R[\hat{\varrho}] &\geqslant \frac{\langle \hat{S} \rangle - N|Q|s}{N^2 s^2} - 1 =: E_R[\hat{\varrho}], \\ \mathcal{E}_{\mathrm{GR}}[\hat{\varrho}] &\geqslant \frac{\langle \hat{S} \rangle}{N|Q|s + N^2 s^2} - 1 =: E_{\mathrm{GR}}[\hat{\varrho}]. \end{aligned} \tag{24}$$

We present $E_R[\hat{\varrho}]$ and $E_{\mathrm{GR}}[\hat{\varrho}]$ for several numerically simulated states in Sec. III (see Fig. 4), and discuss some analytic examples in Sec. IV.

III. NUMERICAL ANALYSIS OF MAGNETIC MATERIALS

For all our numerical examples we assume that $f_{i,\alpha}(\boldsymbol{q}) = f(\boldsymbol{q})$, that the $N = L^3$ spins are arranged on a simple cubic lattice with $\boldsymbol{r}_i = \boldsymbol{i} \in \{1,\ldots,L\}^{\times 3}$ and periodic boundary conditions, and that

$$Q \subset 2\pi \{0,\ldots,L-1\}^{\times 3}/L. \tag{25}$$

We will consider ground and thermal states $\hat{\varrho} = e^{-\hat{H}/(k_B T)}/Z$ of quasi-one- and two-dimensional Hamiltonians, that is, Hamiltonians of the form

$$\hat{H} = \sum_{i_z,i_y=1}^{N} \hat{H}_{\mathrm{1D}}^{(i_z,i_y)} \quad \text{or} \quad \hat{H} = \sum_{i_z=1}^{N} \hat{H}_{\mathrm{2D}}^{(i_z)}, \tag{26}$$

i.e., Hamiltonians that correspond to L^2 mutually uncoupled chains or Hamiltonians that correspond to L mutually uncoupled two-dimensional systems. We further assume that the individual chains are governed by the same one-dimensional Hamiltonian $\hat{H}_{\mathrm{1D}}$ and will give numerical examples for the one-dimensional Heisenberg model and the XY chain.

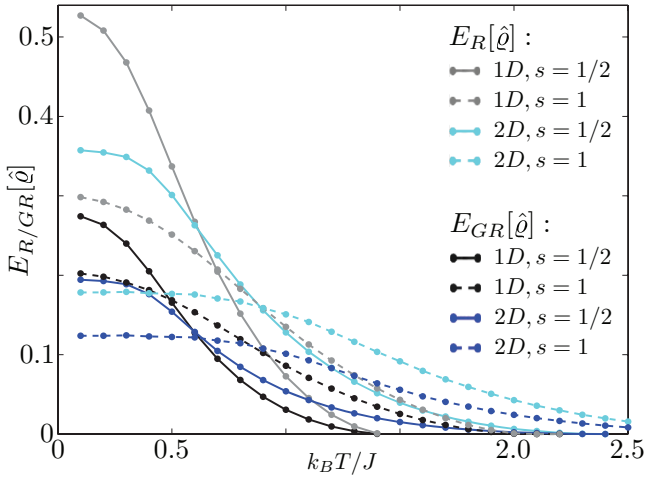


FIG. 4. (Color online) Lower bounds $E_R[\hat{\varrho}]$ and $E_{\mathrm{GR}}[\hat{\varrho}]$ [Eqs. (24) and (21); see the main text for the choice of the set Q] to the robustness measures $\mathcal{E}_R[\hat{\varrho}]$ and $\mathcal{E}_{\mathrm{GR}}[\hat{\varrho}]$ as functions of temperature for thermal states of the quasi-one-dimensional [black, see Eqs. (26) and (27)] and quasi-two-dimensional [blue, see Eq. (27)] Heisenberg models with spin number $s = 1/2$ (solid) and $s = 1$ (dashed). Note that for any state $E_R[\hat{\varrho}] \geqslant E_{\mathrm{GR}}[\hat{\varrho}]$. The lines are guides to the eye and $N = 900$ spins were simulated [56].

Similarly, we assume that the individual two-dimensional systems are governed by the same $\hat{H}_{\mathrm{2D}}$ and provide numerical examples for it being the two-dimensional Heisenberg model.

Results for thermal states are obtained using the loop algorithm of the ALPS quantum Monte Carlo library [50]. For details on the simulation of effective one- and two-dimensional models and the symmetries of the models under consideration see Appendixes B and C.

We start with quasi-one-dimensional models, the first of which is the antiferromagnetic one-dimensional Heisenberg model, i.e., the individual chains are governed by the Hamiltonian

$$\hat{H}_{\mathrm{1D}}^{H} = J \sum_{\langle i,j \rangle} \hat{\boldsymbol{S}}_i \cdot \hat{\boldsymbol{S}}_j = J \sum_{\langle i,j \rangle} \sum_{\alpha} \hat{S}_i^{\alpha} \hat{S}_j^{\alpha}, \tag{27}$$

where $\langle \cdot,\cdot \rangle$ denotes summation over nearest neighbors. Various materials may approximately be described by such mutually uncoupled chains and have been studied experimentally using neutron scattering; see Table I for some examples. In Fig. 1, we present results for the lower bound $E_{\mathrm{BSA}}[\hat{\varrho}](\boldsymbol{q})$, which, due to symmetries of the considered model, is independent of q_y and q_z (see Appendix C for details).

As a second quasi-one-dimensional example, we consider thermal states $\hat{\varrho} = e^{-\beta \hat{H}}/Z$ of the spin-1/2 XY chain in a transverse magnetic field,

$$\hat{H}_{\mathrm{1D}}^{XY} = \sum_{\langle i,j \rangle} \left[(1+\gamma) \hat{S}_i^x \hat{S}_j^x + (1-\gamma) \hat{S}_i^y \hat{S}_j^y \right] - h \sum_i \hat{S}_i^z, \tag{28}$$

where γ is the anisotropy parameter and h denotes the magnetic field. The system undergoes a quantum phase transition at the critical value $h = 1$ and the ground state factorizes for $\gamma^2 + h^2 = 1$. See Ref. [57] for a comparison of this model to experimental data on Cs_2CoCl_4 and Ref. [58]

TABLE I. Various materials that have been studied using neutron scattering and that may approximately be described by quasi-one- or two-dimensional Heisenberg Hamiltonians.

Compound	Effective D	s	J (K)	Studied at T (K)	Ref.
$CuSO_4 \cdot 5D_2O$	1	1/2	3	0.1	[51]
Cs_2CuCl_4	1	1/2	4	0.06	[52]
$CsNiCl_3$	1	1	17	1.6	[53]
$Cu(DCOO)_2 \cdot 4D_2O$	2	1/2	72	1.5	[54]
La_2CuO_4	2	1/2	1567	337	[40]
$SrCuO_4Cl_2$	2	1/2	1451	10	[41]
K_2NiF_4	2	1	112	4.2	[39]
Rb_2MnF_4	2	5/2	8	10	[55]

for confirmation of the one-dimensional spin-1/2 XY character of the interactions between the pseudospins of the Pr^{3+} ions in $PrCl_3$. The spin-correlation functions for thermal states of this model were extensively studied by Barouch and McCoy in Ref. [59] and may be obtained numerically for very large chain lengths. We present lower bounds to the best separable approximation of thermal states of this model in Fig. 2. The presented results are for chains oriented along the x direction and we maximize the bound $E_{\mathrm{BSA}}[\hat{\varrho}](\boldsymbol{q})$ over all $\boldsymbol{q} \in 2\pi\{0,\ldots,L-1\}^{\times 3}/L$ with $\boldsymbol{q} \neq \boldsymbol{0}$; see Appendix C for details. Further, we use the fact that entanglement properties of the thermal state are invariant under $\gamma \mapsto -\gamma$ (as this may be implemented by local unitaries).

Finally, in Fig. 3, we present results for the quasi-two-dimensional model, in which each two-dimensional subsystem is governed by the Heisenberg model such that the total Hamiltonian reads

$$\hat{H}^H = J \sum_{\langle \boldsymbol{i},\boldsymbol{j}\rangle} \delta_{i_z,j_z} \sum_{\alpha} \hat{S}_{\boldsymbol{i}}^{\alpha} \hat{S}_{\boldsymbol{j}}^{\alpha}, \tag{29}$$

where we recall that $\boldsymbol{i} = (i_x,i_y,i_z) \in \{1,\ldots,L\}^{\times 3}$. Due to the symmetries of this model, the bound $E_{\mathrm{BSA}}[\hat{\varrho}](\boldsymbol{q})$ in Eq. (20) is independent of q_z; see Appendix C for details. For compounds well described by the quasi-two-dimensional Heisenberg model, see Table I.

To present results on the robustness measures $\mathcal{E}_R[\hat{\varrho}]$ and $\mathcal{E}_{\mathrm{GR}}[\hat{\varrho}]$, we need to specify the set of scattering vectors Q appearing in the lower bounds $E_R[\hat{\varrho}]$ and $E_{\mathrm{GR}}[\hat{\varrho}]$ in Eqs. (24) and (21). We use the following choice of scattering vectors:

$$Q(x) = \left\{ \boldsymbol{q} \in \mathcal{Q} \,|\, \sum_{i,j} e^{i\boldsymbol{q}(\boldsymbol{r}_i - \boldsymbol{r}_j)} \sum_{\alpha} \left\langle \hat{S}_i^{\alpha} \hat{S}_j^{\alpha} \right\rangle \geqslant x \right\} \tag{30}$$

and then take Q as the $Q(x)$ that maximizes the lower bound. In Fig. 4, we present results for all the Heisenberg models that we also considered for the best separable approximation.

IV. ANALYTIC EXAMPLES

In this section, we discuss resonating valence bond (RVB) states and the Majumdar-Gosh model, for which an exact expression for the expectation value of $\hat{S}(\boldsymbol{q})$ (and hence for our entanglement bounds) may be obtained. In the context of high-temperature superconductors, resonating valence bond states were introduced by Anderson [60,61]. They are used to describe quantum spin liquids, i.e., states without long-range magnetic order [62], and appear as ground states of frustrated antiferromagnets. Such systems and their description by the RVB model currently receive increased theoretical as well as experimental attention; see, e.g., Refs. [8,9,63,64], and Ref. [65] for a recent neutron scattering investigation of the antiferromagnetic Heisenberg model on a kagome lattice. Besides the characterization of high-T_c superconductors, quantum spin liquids have potential applications for topological quantum computation [66]. The entanglement properties of RVB states have recently been considered using tools from quantum information theory [67,68]. Consider a lattice with N (even) sites and a dimer covering $\Delta = \{(i_1,j_1),\ldots,(i_{N/2},j_{N/2})\}$, i.e., a collection of pairs of lattice sites such that each lattice site belongs to exactly one dimer. To any such dimerization, one may associate a valence bond state $|\psi_\Delta\rangle = \otimes_{(i,j)\in\Delta} |\phi_{i,j}\rangle$. Singlet RVB states are superpositions of such states, $|\psi\rangle = \sum_\Delta c_\Delta |\psi_\Delta\rangle$, where each dimer forms a singlet $|\phi_{i,j}\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle_i|\downarrow\rangle_j - |\downarrow\rangle_i|\uparrow\rangle_j)$. The span of all singlet valence bond states is equal to the singlet sector, i.e., to the spin-zero subspace. For these states, in the limit $\boldsymbol{q} \to \boldsymbol{0}$, we have $E_{\mathrm{BSA}}[|\psi\rangle\langle\psi|](\boldsymbol{q} \to \boldsymbol{0}) \geqslant 1 - \frac{1}{NC_s} \sum_\alpha \langle \hat{S}_\alpha^2 \rangle = 1$, where $\hat{S}_\alpha = \sum_i \hat{S}_i^\alpha$ is the total spin along α, i.e.,

$$E_{\mathrm{BSA}}[|\psi\rangle\langle\psi|](\boldsymbol{q} \to \boldsymbol{0}) = 1, \tag{31}$$

for all $|\psi\rangle = \sum_\Delta c_\Delta |\psi_\Delta\rangle$, i.e., these states maximally violate the lower bound in Eq. (14) and their entanglement as quantified in terms of the best separable approximation is hence optimally quantified by the neutron scattering observable in Eq. (20).

Hamiltonians for which the RVB model may describe the ground state and explain low-lying excitations include examples with frustration due to additional next-nearest-neighbor interaction such as the so-called Klein Hamiltonian [69] on two-dimensional lattices and the Majumdar-Ghosh Hamiltonian in one dimension [70],

$$\hat{H}_{\mathrm{1D}}^{\mathrm{MG}} = 2 \sum_i \hat{\boldsymbol{S}}_i \cdot \hat{\boldsymbol{S}}_{i+1} + \sum_i \hat{\boldsymbol{S}}_i \cdot \hat{\boldsymbol{S}}_{i+2}. \tag{32}$$

In Ref. [71] it was shown that the ratio of nearest-neighbor and next-nearest-neighbor coupling in the quasi-one-dimensional antiferromagnet $CuCrO_4$ is close to 2, putting this magnet in the vicinity of the Majumdar-Ghosh point. Every ground state of $\hat{H}_{\mathrm{1D}}^{\mathrm{MG}}$ is a superposition of two two-periodic states given by products of nearest-neighbor singlets, i.e., a RVB state. The equal-weight ground state may be given explicitly by exploiting its description as a matrix product state [72]. The correlators can be computed exactly and allow for a particularly concise expression of the structure factor in the thermodynamic limit: The correlators for a single chain of length L are given by [72,73]

$$\left\langle \hat{S}_i^\alpha \hat{S}_{i+r}^\alpha \right\rangle = \begin{cases} (-1)^{L/2-1} \frac{(-1)^r}{2^{L/2+1}+4(-1)^{L/2}} & \text{for} \quad r > 1, \\ -\frac{1}{4} \frac{2^{L/2}+4(-1)^{L/2}}{2^{L/2+1}+4(-1)^{L/2}} & \text{for} \quad r = 1. \end{cases} \tag{33}$$

In the thermodynamic limit we find $\langle \hat{S}_i^\alpha \hat{S}_{i+r}^\alpha \rangle = -\frac{\delta_{1,r}}{8}$ for $\alpha = x,y,z$ and $r > 0$, which yields

$$E_{\mathrm{BSA}}[\hat{\varrho}](\boldsymbol{q}) = 2\cos(q_x) - 1 \tag{34}$$

if every one of the mutually uncoupled chains is in this ground state; see the solid line in Fig. 1. With $Q = \{\boldsymbol{q}\}$, i.e., $|Q| = 1$, we find for the robustness bounds in Eq. (24) that, as $N \to \infty$,

$$\begin{aligned} E_R[\hat{\varrho}] &= \frac{1 - 3\cos(q_x)}{N} - 1, \\ E_{\mathrm{GR}}[\hat{\varrho}] &= \frac{3[1 - \cos(q_x)]}{2 + N} - 1, \end{aligned} \tag{35}$$

both of which become trivial if N is too large. Just as for the numerical examples, we see that summation over several scattering vectors is necessary to obtain a nontrivial lower bound: We choose $Q(c) = \{\boldsymbol{q} \in \mathcal{Q} \,|\, \frac{2\pi}{L}\frac{L}{2} - \frac{2\pi}{L}cL < q_x \leqslant \frac{2\pi}{L}\frac{L}{2} + \frac{2\pi}{L}cL\}$, i.e., $|Q(c)| = 2cN$. This choice follows from the form of the structure factor of this model, which has a maximum at π and decreases monotonically towards 0 and 2π. Thus, c parametrizes the set $Q(c)$ as in (30). We may then, for large L, replace the summation of the structure factor over different q_x by an integral according to $\lim_{L\to\infty} \frac{1}{L}\sum_{q=a}^{b} f(\frac{2\pi q}{L}) = \frac{1}{2\pi}\int_{2\pi a/L}^{2\pi b/L} f(q)dq$. By direct computation of the integral over the set $Q(c)$ we obtain lower bounds to the robustness measures for every c. By maximizing over $0 < c < 1/2$, we find that $E_R[\hat{\varrho}] \approx 0.51$ and $E_{\mathrm{GR}}[\hat{\varrho}] \approx 0.23$ in the thermodynamic limit.

V. SUMMARY AND OUTLOOK

We showed how entanglement may be quantified by relying on observables typically obtained in scattering experiments. In particular, these observables can be measured via the scattering cross section in neutron scattering. We showed how such measurements give lower bounds on the entanglement in the sample, bounding the best separable approximation, the robustness of entanglement, and the generalized robustness of entanglement. These bounds rely neither on the knowledge of the systems underlying Hamiltonian nor on any other information about the state of the sample material. The detection can be applied to macroscopic systems, because the experimental effort does not increase with the system size—in stark contrast to quantum state tomography. We showed for several model Hamiltonians, such as the Heisenberg, Majumdar-Gosh, and XY models (for different spin numbers and different spatial geometries), that our method can indeed quantify entanglement in large samples at finite temperature. Interestingly, quantum phase transitions and factorization points are detected by our entanglement bounds. The considered models are well known and applicable to real materials. Therefore our results pave the way for macroscopic entanglement quantification in experiments. This is very important for future applications which utilize entanglement, e.g., in quantum information science. Our method might also be valuable as an alternative way to check the power of a model to describe the sample material, e.g., if a sample is highly entangled, a classical description certainly fails.

ACKNOWLEDGMENTS

We gratefully acknowledge Robert Rosenbach for help with the numerics. The work at Ulm University has been supported by the EU Integrated Projects Q-ESSENCE and SIQS, the EU STREP EQUAM, the BMBF Verbundprojekt QuOReP, a GIF project, and an Alexander von Humboldt Professorship. D.B., M.E., and H.K. acknowledge financial support by the Deutsche Forschungsgemeinschaft (DFG).

APPENDIX A: BOUNDS FOR FULLY SEPARABLE STATES

Let $Q \subset \mathbb{R}^3$. For $\boldsymbol{q} \in Q$, $i = 1, \ldots, N$, and $\alpha = x, y, z$, let $f_{i,\alpha}(\boldsymbol{q}) \in \mathbb{C}$ and $\boldsymbol{r}_i \in \mathbb{R}^3$. Further, for each $\boldsymbol{q} \in Q$ let $M(\boldsymbol{q})$ be a 3×3 Hermitian positive semidefinite matrix with entries $M_{\alpha,\beta}(\boldsymbol{q})$. Consider the observable

$$\hat{S} = \sum_{\boldsymbol{q}\in Q}\sum_{\alpha,\beta}\sum_{i,j} M_{\alpha,\beta}(\boldsymbol{q}) f^*_{i,\alpha}(\boldsymbol{q}) f_{j,\beta}(\boldsymbol{q}) e^{i\boldsymbol{q}(\boldsymbol{r}_i - \boldsymbol{r}_j)} \hat{S}_i^{\alpha} \hat{S}_j^{\beta}, \tag{A1}$$

which is positive semidefinite: Denoting $\hat{S}_\alpha(\boldsymbol{q}) = \sum_i f_{i,\alpha}(\boldsymbol{q}) e^{-i\boldsymbol{q}\boldsymbol{r}_i} \hat{S}_i^{\alpha}$, we have

$$\hat{S} = \sum_{\boldsymbol{q}\in Q}\sum_{\alpha,\beta} M_{\alpha,\beta}(\boldsymbol{q}) \hat{S}_\alpha(\boldsymbol{q})^\dagger \hat{S}_\beta(\boldsymbol{q}), \tag{A2}$$

which is positive semidefinite as the 3×3 matrices $M(\boldsymbol{q})$ are and as for every $\boldsymbol{q}$ and every state vector $|\psi\rangle$ the 3×3 matrix with entries $\langle\psi|\hat{S}_\alpha(\boldsymbol{q})^\dagger \hat{S}_\beta(\boldsymbol{q})|\psi\rangle$ is positive semidefinite [for every $z \in \mathbb{C}^3$, one has $\sum_{\alpha,\beta} z^*_\alpha \langle\psi|\hat{S}_\alpha(\boldsymbol{q})^\dagger \hat{S}_\beta(\boldsymbol{q})|\psi\rangle z_\beta = \langle\psi|[\sum_\alpha z_\alpha \hat{S}_\alpha(\boldsymbol{q})]^\dagger[\sum_\beta z_\beta \hat{S}_\beta(\boldsymbol{q})]|\psi\rangle \geqslant 0$].

For each $i = 1, \ldots, N$ define the 3×3 matrix $M^{(i)}$ with entries

$$M^{(i)}_{\alpha,\beta} = \sum_{\boldsymbol{q}\in Q} f^*_{i,\alpha}(\boldsymbol{q}) f_{i,\beta}(\boldsymbol{q}) M_{\alpha,\beta}(\boldsymbol{q}). \tag{A3}$$

We assume that these matrices are real symmetric. This is fulfilled, e.g., if $f_{i,\alpha}(\boldsymbol{q}) = F_i(\boldsymbol{q}) g_{i,\alpha}$ with $F_i(\boldsymbol{q}) \in \mathbb{C}$ and $g_{i,\alpha} \in \mathbb{R}$. We further note that these $M^{(i)}$ are positive semidefinite as we assumed that the $M(\boldsymbol{q})$ are positive semidefinite: Let $z \in \mathbb{C}^3$. Then

$$\begin{aligned} z^\dagger M^{(i)} z &= \sum_{\alpha,\beta} z^*_\alpha M^{(i)}_{\alpha,\beta} z_\beta \\ &= \sum_{\boldsymbol{q}\in Q} \left[\sum_\alpha z_\alpha f_{i,\alpha}(\boldsymbol{q})\right]^\dagger M_{\alpha,\beta}(\boldsymbol{q}) \\ &\quad \times \left[\sum_\beta z_\beta f_{i,\beta}(\boldsymbol{q})\right] \geqslant 0. \end{aligned} \tag{A4}$$

We set out to derive upper and lower bounds on the expectation of $\hat{S}$ for product states $|\psi\rangle = \otimes_i |\psi_i\rangle$. The same bounds then also hold for fully separable states $\hat{\varrho} = \sum_n p_n \otimes_i \hat{\varrho}_i^{(n)}$ by convexity. For product states, we have that for all $i \neq j$ the equality $\langle \hat{S}_i^\alpha \hat{S}_j^\beta \rangle = \langle \hat{S}_i^\alpha \rangle \langle \hat{S}_j^\beta \rangle$ holds. Hence,

$$\begin{aligned} \langle\hat{S}\rangle &= \sum_i \sum_{\alpha,\beta} M^{(i)}_{\alpha,\beta} \langle \hat{S}_i^\alpha \hat{S}_i^\beta \rangle - \sum_i \sum_{\alpha,\beta} M^{(i)}_{\alpha,\beta} \langle \hat{S}_i^\alpha \rangle \langle \hat{S}_i^\beta \rangle \\ &\quad + \sum_{\boldsymbol{q}\in Q}\sum_{\alpha,\beta}\sum_{i,j} M_{\alpha,\beta}(\boldsymbol{q}) f^*_{i,\alpha}(\boldsymbol{q}) f_{j,\beta}(\boldsymbol{q}) e^{i\boldsymbol{q}(\boldsymbol{r}_i - \boldsymbol{r}_j)} \langle \hat{S}_i^\alpha \rangle \langle \hat{S}_j^\beta \rangle \\ &=: A - B + C. \end{aligned} \tag{A5}$$

1. Lower bound

The third term C in Eq. (A5) is non-negative as for each $\boldsymbol{q}$ the matrix $M(\boldsymbol{q})$ is positive semidefinite. Hence we have the lower bound

$$\langle \hat{S} \rangle \geqslant A - B = \sum_i \sum_{\alpha,\beta} M^{(i)}_{\alpha,\beta} \big(\langle \hat{S}^\alpha_i \hat{S}^\beta_i \rangle - \langle \hat{S}^\alpha_i \rangle \langle \hat{S}^\beta_i \rangle \big). \tag{A6}$$

As we assumed that for each i the $M^{(i)}$ are real symmetric, there are mutually orthonormal real eigenvectors $\boldsymbol{m}^{(i)}_\gamma$ with corresponding eigenvalues $m^{(i)}_\gamma$ and there is a unitary $\hat{U}_i$ such that $\sum_\alpha [\boldsymbol{m}^{(i)}_\gamma]_\alpha \hat{S}^\alpha_i = \hat{U}^\dagger_i \hat{S}^\gamma_i \hat{U}_i$ for all γ. Thus

$$\begin{aligned} &\sum_{\alpha,\beta} M^{(i)}_{\alpha,\beta} \big(\langle \psi_i | \hat{S}^\alpha_i \hat{S}^\beta_i | \psi_i \rangle - \langle \psi_i | \hat{S}^\alpha_i | \psi_i \rangle \langle \psi_i | \hat{S}^\beta_i | \psi_i \rangle \big) \\ &\quad = \sum_\gamma m^{(i)}_\gamma \big(\langle \psi_i | \hat{U}^\dagger_i \big(\hat{S}^\gamma_i \big)^2 \hat{U}_i | \psi_i \rangle - \langle \psi_i | \hat{U}^\dagger_i \hat{S}^\gamma_i \hat{U}_i | \psi_i \rangle^2 \big) \\ &\quad \geqslant \min_{\substack{|\psi\rangle \in \mathbb{C}^{2s+1} \\ \langle \psi | \psi \rangle = 1}} \sum_\gamma m^{(i)}_\gamma \big(\langle \psi | \big(\hat{S}^\gamma_i \big)^2 | \psi \rangle - \langle \psi | \hat{S}^\gamma_i | \psi \rangle^2 \big), \end{aligned} \tag{A7}$$

which is $c_{\min}$ presented in the main text.

2. Upper bound

We first bound, as above,

$$\begin{aligned} A &= \sum_i \sum_{\alpha,\beta} M^{(i)}_{\alpha,\beta} \langle \psi_i | \hat{S}^\alpha_i \hat{S}^\beta_i | \psi_i \rangle \\ &= \sum_i \sum_\gamma m^{(i)}_\gamma \langle \psi_i | \hat{U}^\dagger_i \big(\hat{S}^\gamma_i \big)^2 \hat{U}_i | \psi_i \rangle \leqslant \sum_i \left\| \sum_\gamma m^{(i)}_\gamma \big(\hat{S}^\gamma_i \big)^2 \right\|, \end{aligned} \tag{A8}$$

where $\| \cdot \|$ denotes the operator norm. Now denote by $\mathcal{M}$ the Hermitian $3N \times 3N$ matrix with entries

$$\mathcal{M}_{i,\alpha;j,\beta} = \sum_{\boldsymbol{q} \in Q} M_{\alpha,\beta}(\boldsymbol{q}) f^*_{i,\alpha}(\boldsymbol{q}) f_{j,\beta}(\boldsymbol{q}) (e^{i \boldsymbol{q} (\boldsymbol{r}_i - \boldsymbol{r}_j)} - \delta_{i,j}). \tag{A9}$$

This matrix has $\mathrm{tr}[\mathcal{M}] = 0$, i.e., its largest eigenvalue $\lambda_{\max}$ is non-negative and therefore

$$C - B = \sum_{\alpha,\beta} \sum_{i,j} \mathcal{M}_{i,\alpha;j,\beta} \langle \hat{S}^\alpha_i \rangle \langle \hat{S}^\beta_j \rangle \leqslant \lambda_{\max} N s^2. \tag{A10}$$

Hence, we have the bound

$$A - B + C \leqslant \sum_i \left\| \sum_\gamma m^{(i)}_\gamma \big(\hat{S}^\gamma_i \big)^2 \right\| + \lambda_{\max} N s^2. \tag{A11}$$

This constitutes our general result for $c_{\max}$. To compute it, one needs to find the maximum eigenvalue of the $3N \times 3N$ matrix $\mathcal{M}$ and, for each $i = 1, \ldots, N$, the eigenvalues of the 3×3 matrix $M^{(i)}$. We now discuss a geometry for which this may be made more explicit.

Let the positions of the ith spin be $\boldsymbol{r}_i = \boldsymbol{r}_{k,l} = \boldsymbol{R}_k + \boldsymbol{x}_l$, where $k = 1, \ldots, N_c$ and $l = 1, \ldots, n$ such that $N = n N_c$. Further we let the lattice sites $k = 1, \ldots, N_c$, with $N_c = N^c_1 N^c_2 N^c_3$, be the sites of a finite Bravais lattice with primitive vectors $\boldsymbol{a}_d$, $d = 1,2,3$, such that $\boldsymbol{R}_k = \sum_{d=1}^3 k_d \boldsymbol{a}_d$ with $k_d \in \{1, \ldots, N^c_d\}$. Note that this is more general than in the main text as we allow for n spins in each unit cell. We now assume that $f_{i,\alpha}(\boldsymbol{q}) = f_{k,l,\alpha}(\boldsymbol{q}) = f_{l,\alpha}(\boldsymbol{q})$, i.e., it depends only on l. Further we assume that

$$Q \subset \left\{ \sum_{d=1}^3 q_d \boldsymbol{b}_d \,\middle|\, q_d = \frac{i-1}{N^c_d},\ i \in \{1, \ldots, N^c_d\} \right\} =: \mathcal{Q}, \tag{A12}$$

where the $\boldsymbol{b}_d$ are reciprocal primitive vectors corresponding to the $\boldsymbol{a}_d$. We then have $\frac{1}{N_c} \sum_{\boldsymbol{p} \in \mathcal{Q}} e^{i \boldsymbol{p} (\boldsymbol{R}_k - \boldsymbol{R}_{k'})} = \delta_{k,k'}$, which yields

$$\begin{aligned} \mathcal{M}_{\alpha,k,l;\beta,k',l'} &= \sum_{\boldsymbol{q} \in Q} M_{\alpha,\beta}(\boldsymbol{q}) f^*_{l,\alpha}(\boldsymbol{q}) f_{l',\beta}(\boldsymbol{q}) (e^{i \boldsymbol{q} (\boldsymbol{R}_k - \boldsymbol{R}_{k'})} e^{i \boldsymbol{q} (\boldsymbol{x}_l - \boldsymbol{x}_{l'})} - \delta_{k,k'} \delta_{l,l'}) \\ &=: \sum_{\boldsymbol{q} \in Q} M'_{\alpha,l;\beta,l'}(\boldsymbol{q}) (e^{i \boldsymbol{q} (\boldsymbol{R}_k - \boldsymbol{R}_{k'})} - \delta_{k,k'} \delta_{l,l'}) \\ &= \sum_{\boldsymbol{q} \in Q} M'_{\alpha,l;\beta,l'}(\boldsymbol{q}) \left(e^{i \boldsymbol{q} (\boldsymbol{R}_k - \boldsymbol{R}_{k'})} - \delta_{l,l'} \frac{1}{N_c} \sum_{\boldsymbol{p} \in \mathcal{Q}} e^{i \boldsymbol{p} (\boldsymbol{R}_k - \boldsymbol{R}_{k'})} \right) \\ &= \sum_{\boldsymbol{q} \in Q} M'_{\alpha,l;\beta,l'}(\boldsymbol{q}) \sum_{\boldsymbol{p} \in \mathcal{Q}} \left(\delta_{\boldsymbol{p},\boldsymbol{q}} - \delta_{l,l'} \frac{1}{N_c} \right) e^{i \boldsymbol{p} (\boldsymbol{R}_k - \boldsymbol{R}_{k'})} \\ &=: \sum_{\boldsymbol{p} \in \mathcal{Q}} M''_{\alpha,l;\beta,l'}(\boldsymbol{p}) e^{i \boldsymbol{p} (\boldsymbol{R}_k - \boldsymbol{R}_{k'})} \\ &=: \sum_{\boldsymbol{p} \in \mathcal{Q}} [M''(\boldsymbol{p}) \otimes \boldsymbol{e}_{\boldsymbol{p}} \boldsymbol{e}^\dagger_{\boldsymbol{p}}]_{\alpha,l,k;\beta,l',k'} \end{aligned} \tag{A13}$$

and thus $\lambda_{\max} = N_c \max_{\boldsymbol{p}\in Q} \lambda_{\max}[M''(\boldsymbol{p})] = N_c \max_{\boldsymbol{p}\in Q} \lambda_{\max}[M''(\boldsymbol{p})]$, where

$$M''_{\alpha,l;\beta,l'}(\boldsymbol{p}) = \sum_{\boldsymbol{q}\in Q} M_{\alpha,\beta}(\boldsymbol{q}) f^*_{l,\alpha}(\boldsymbol{q}) f_{l',\beta}(\boldsymbol{q}) e^{i\boldsymbol{q}(\boldsymbol{x}_l - \boldsymbol{x}_{l'})} \left(\delta_{\boldsymbol{p},\boldsymbol{q}} - \delta_{l,l'} \frac{1}{N_c}\right). \tag{A14}$$

Further,

$$M^{(i)}_{\alpha,\beta} = M^{(k,l)}_{\alpha,\beta} = M^{(l)}_{\alpha,\beta} = \sum_{\boldsymbol{q}\in Q} f^*_{l,\alpha}(\boldsymbol{q}) f_{l,\beta}(\boldsymbol{q}) M_{\alpha,\beta}(\boldsymbol{q}) \tag{A15}$$

with eigenvalues $m^{(l)}_\gamma$. We hence have the bound

$$A - B + C \leqslant N_c \sum_{l=1}^{n} \left\| \sum_\gamma m^{(l)}_\gamma \left(\hat{S}^\gamma_i\right)^2 \right\| + N s^2 N_c \max_{\boldsymbol{p}\in Q} \lambda_{\max}[M''(\boldsymbol{p})]. \tag{A16}$$

Comparing this $c_{\max}$ to the general bound above, one now must, for each $\boldsymbol{q} \in Q$, find the maximum eigenvalue of a $3n \times 3n$ matrix (where we recall that n is the number of spins in each unit cell) and, for each $l = 1, \ldots, n$, find the eigenvalues of the 3×3 matrix $M^{(l)}$.

If $f_l(\boldsymbol{q}) = f(\boldsymbol{q})$ and $M_{\alpha,\beta}(\boldsymbol{q}) = \delta_{\alpha,\beta}/|f(\boldsymbol{q})|^2$, we have

$$M''_{\alpha,l;\beta,l'}(\boldsymbol{p}) = \delta_{\alpha,\beta} \sum_{\boldsymbol{q}\in Q} e^{i\boldsymbol{q}(\boldsymbol{x}_l - \boldsymbol{x}_{l'})} \left(\delta_{\boldsymbol{p},\boldsymbol{q}} - \delta_{l,l'} \frac{1}{N_c}\right) = \delta_{\alpha,\beta} e^{i\,\boldsymbol{p}(\boldsymbol{x}_l - \boldsymbol{x}_{l'})} - \delta_{\alpha,\beta}\delta_{l,l'} \frac{|Q|}{N_c} \tag{A17}$$

and $M^{(l)}_{\alpha,\beta} = |Q|\delta_{\alpha,\beta}$, i.e., the bound simplifies to

$$A - B + C \leqslant N|Q|s + N^2 s^2, \tag{A18}$$

which is $c_{\max}$ in the main text.

APPENDIX B: SIMULATION DETAILS: EFFECTIVE ONE- AND TWO-DIMENSIONAL SYSTEMS

Consider

$$\hat{S}_{\alpha,\beta}(\boldsymbol{q}) = \sum_{\boldsymbol{i},\boldsymbol{j}} e^{i\boldsymbol{q}(\boldsymbol{i}-\boldsymbol{j})} \hat{S}^\alpha_{\boldsymbol{i}} \hat{S}^\beta_{\boldsymbol{j}}. \tag{B1}$$

We write $\boldsymbol{i} = (i_x\, i_y\, i_z) \in \{1, \ldots, L\}^{\times 3}$, $\boldsymbol{q} = (q_x\, q_y\, q_z)$, $\tilde{\boldsymbol{i}} = (i_x\, i_y)$, $\tilde{\boldsymbol{q}} = (q_x\, q_y)$. If the system consists of mutually uncoupled (in the z direction) two-dimensional systems, we have $\langle \hat{S}^\alpha_{\boldsymbol{i}} \hat{S}^\beta_{\boldsymbol{j}} \rangle = \langle \hat{S}^\alpha_{\boldsymbol{i}} \rangle \langle \hat{S}^\beta_{\boldsymbol{j}} \rangle$ whenever $i_z \neq j_z$, i.e.,

$$\begin{aligned}
\langle \hat{S}_{\alpha,\beta}(\boldsymbol{q}) \rangle &= \sum_{\substack{\boldsymbol{i},\boldsymbol{j} \\ i_z = j_z}} e^{i\tilde{\boldsymbol{q}}\cdot(\tilde{\boldsymbol{i}}-\tilde{\boldsymbol{j}})} \langle \hat{S}^\alpha_{\boldsymbol{i}} \hat{S}^\beta_{\boldsymbol{j}} \rangle \\
&\quad + \sum_{\substack{\boldsymbol{i},\boldsymbol{j} \\ i_z \neq j_z}} e^{i\boldsymbol{q}\cdot(\boldsymbol{i}-\boldsymbol{j})} \langle \hat{S}^\alpha_{\boldsymbol{i}} \rangle \langle \hat{S}^\beta_{\boldsymbol{j}} \rangle \\
&= \sum_{\substack{\boldsymbol{i},\boldsymbol{j} \\ i_z = j_z}} e^{i\tilde{\boldsymbol{q}}\cdot(\tilde{\boldsymbol{i}}-\tilde{\boldsymbol{j}})} \left(\langle \hat{S}^\alpha_{\boldsymbol{i}} \hat{S}^\beta_{\boldsymbol{j}} \rangle - \langle \hat{S}^\alpha_{\boldsymbol{i}} \rangle \langle \hat{S}^\beta_{\boldsymbol{j}} \rangle \right) \\
&\quad + \left(\sum_{\boldsymbol{i}} e^{i\boldsymbol{q}\cdot\boldsymbol{i}} \langle \hat{S}^\alpha_{\boldsymbol{i}} \rangle \right) \left(\sum_{\boldsymbol{i}} e^{i\boldsymbol{q}\cdot\boldsymbol{i}} \langle \hat{S}^\beta_{\boldsymbol{i}} \rangle \right)^* \\
&=: S_{\alpha,\beta}(\tilde{\boldsymbol{q}}) + M_\alpha(\boldsymbol{q}) M^*_\beta(\boldsymbol{q}).
\end{aligned}$$

Now let the two-dimensional subsystems be equal. Then, any thermal state of the system is of the form $\hat{\varrho} = \otimes_{i_z} \hat{\varrho}_{i_z}$, where the $\hat{\varrho}_{i_z}$ are equal and each describes a two-dimensional layer at z coordinate i_z. Hence,

$$\langle \hat{S}^\alpha_{\boldsymbol{i}} \rangle = \mathrm{tr}\left[\hat{S}^\alpha_{\boldsymbol{i}} \hat{\varrho}\right] = \mathrm{tr}\left[\hat{S}^\alpha_{\boldsymbol{i}} \hat{\varrho}_{i_z}\right] =: \langle \hat{S}^\alpha_{\tilde{\boldsymbol{i}}} \rangle_{\mathrm{2D}}, \tag{B2}$$

which does not depend on i_z. Similarly, for $i_z = j_z$,

$$\langle \hat{S}^\alpha_{\boldsymbol{i}} \hat{S}^\beta_{\boldsymbol{j}} \rangle = \mathrm{tr}\left[\hat{S}^\alpha_{\boldsymbol{i}} \hat{S}^\beta_{\boldsymbol{j}} \hat{\varrho}\right] = \mathrm{tr}\left[\hat{S}^\alpha_{\boldsymbol{i}} \hat{S}^\beta_{\boldsymbol{j}} \hat{\varrho}_{i_z}\right] =: \langle \hat{S}^\alpha_{\tilde{\boldsymbol{i}}} \hat{S}^\beta_{\tilde{\boldsymbol{j}}} \rangle_{\mathrm{2D}}, \tag{B3}$$

which does not depend on i_z. Hence,

$$\frac{S_{\alpha,\beta}(\tilde{\boldsymbol{q}})}{L} = \sum_{\substack{i_x,i_y, \\ j_x,j_y}} e^{i\tilde{\boldsymbol{q}}\cdot(\tilde{\boldsymbol{i}}-\tilde{\boldsymbol{j}})} \left(\langle \hat{S}^\alpha_{\tilde{\boldsymbol{i}}} \hat{S}^\beta_{\tilde{\boldsymbol{j}}} \rangle_{\mathrm{2D}} - \langle \hat{S}^\alpha_{\tilde{\boldsymbol{i}}} \rangle_{\mathrm{2D}} \langle \hat{S}^\beta_{\tilde{\boldsymbol{j}}} \rangle_{\mathrm{2D}} \right),$$

which does not depend on q_z, and

$$M_\alpha(\boldsymbol{q}) = \sum_{\tilde{\boldsymbol{i}}} e^{i\tilde{\boldsymbol{q}}\cdot\tilde{\boldsymbol{i}}} \langle \hat{S}^\alpha_{\tilde{\boldsymbol{i}}} \rangle_{\mathrm{2D}} \sum_{i_z} e^{iq_z i_z} = L\delta_{q_z,0} \sum_{\tilde{\boldsymbol{i}}} e^{i\tilde{\boldsymbol{q}}\cdot\tilde{\boldsymbol{i}}} \langle \hat{S}^\alpha_{\tilde{\boldsymbol{i}}} \rangle_{\mathrm{2D}}, \tag{B4}$$

where we used that $q_z = 2\pi \frac{i}{L}$ for $i \in \{0, \ldots, L-1\}$. Similarly, if the system is quasi-one-dimensional with $\hat{\varrho} = \otimes_{i_z,i_y} \hat{\varrho}_{i_z,i_y}$ and all the $\hat{\varrho}_{i_z,i_y}$ equal, we have

$$\langle \hat{S}_{\alpha,\beta}(\boldsymbol{q}) \rangle = S_{\alpha,\beta}(q_x) + M_\alpha(\boldsymbol{q}) M_\beta(\boldsymbol{q})^*,$$

where

$$\begin{aligned}
\frac{S_{\alpha,\beta}(q)}{L^2} &= \sum_{i_x,j_x} e^{iq(i_x - j_x)} \left(\langle \hat{S}^\alpha_{i_x} \hat{S}^\beta_{j_x} \rangle_{\mathrm{1D}} - \langle \hat{S}^\alpha_{i_x} \rangle_{\mathrm{1D}} \langle \hat{S}^\beta_{j_x} \rangle_{\mathrm{1D}} \right), \\
\frac{M_\alpha(\boldsymbol{q})}{L^2} &= \delta_{q_z,0}\delta_{q_y,0} \sum_{i_x} e^{iq_x i_x} \langle \hat{S}^\alpha_{i_x} \rangle_{\mathrm{1D}}.
\end{aligned}$$

APPENDIX C: SYMMETRIES

1. Heisenberg models

For all the considered Heisenberg models, we have $\hat{H} = (\bigotimes_{\boldsymbol{i}} \hat{U}_{\boldsymbol{i}}) \hat{H} (\bigotimes_{\boldsymbol{i}} \hat{U}_{\boldsymbol{i}})$, where all the $\hat{U}_{\boldsymbol{i}}$ implement the same

spin rotation. This implies $\langle \hat{S}_{\boldsymbol{i}}^{\alpha} \rangle = 0$ and $\langle \hat{S}_{\boldsymbol{i}}^{\alpha} \hat{S}_{\boldsymbol{j}}^{\beta} \rangle = \delta_{\alpha,\beta} \langle \hat{S}_{\boldsymbol{i}}^{z} \hat{S}_{\boldsymbol{j}}^{z} \rangle$. Hence,

$$E_{\mathrm{BSA}}(\boldsymbol{q}) = 1 - \sum_{\alpha,\beta} \frac{\delta_{\alpha,\beta} - \bar{q}_{\alpha}\bar{q}_{\beta}}{NC_s} \sum_{\boldsymbol{i},\boldsymbol{j}} e^{i\boldsymbol{q}(\boldsymbol{i}-\boldsymbol{j})} \langle \hat{S}_{\boldsymbol{i}}^{\alpha} \hat{S}_{\boldsymbol{j}}^{\beta} \rangle = 1 - \frac{2}{NC_s} \sum_{\boldsymbol{i},\boldsymbol{j}} e^{i\boldsymbol{q}(\boldsymbol{i}-\boldsymbol{j})} \langle \hat{S}_{\boldsymbol{i}}^{z} \hat{S}_{\boldsymbol{j}}^{z} \rangle. \tag{C1}$$

For the quasi-one- and two-dimensional systems we have

$$E_{\mathrm{BSA}}(\boldsymbol{q}) = 1 - \frac{2}{LC_s} \sum_{i_x,j_x} e^{iq_x(i_x-j_x)} \langle \hat{S}_{i_x}^{z} \hat{S}_{j_x}^{z} \rangle_{\mathrm{1D}} \tag{C2}$$

and

$$E_{\mathrm{BSA}}(\boldsymbol{q}) = 1 - \frac{2}{L^2C_s} \sum_{\tilde{\boldsymbol{i}},\tilde{\boldsymbol{j}}} e^{i\tilde{\boldsymbol{q}}\cdot(\tilde{\boldsymbol{i}}-\tilde{\boldsymbol{j}})} \langle \hat{S}_{\tilde{\boldsymbol{i}}}^{\alpha} \hat{S}_{\tilde{\boldsymbol{j}}}^{\beta} \rangle_{\mathrm{2D}}, \tag{C3}$$

respectively. To obtain expressions for the robustness measures, one proceeds analogously.

2. *XY* model

The Hamiltonian of the quasi-one-dimensional *XY* model (with the chains along the x direction),

$$\hat{H} = \sum_{\langle \boldsymbol{i},\boldsymbol{j} \rangle} \delta_{i_y,j_y}\delta_{i_z,j_z} \left[(1+\gamma) \hat{S}_{\boldsymbol{i}}^{x} \hat{S}_{\boldsymbol{j}}^{x} + (1-\gamma) \hat{S}_{\boldsymbol{i}}^{y} \hat{S}_{\boldsymbol{j}}^{y} \right] - h \sum_{\boldsymbol{i}} \hat{S}_{\boldsymbol{i}}^{z}, \tag{C4}$$

is invariant under simultaneous rotation of all the spins around their z axis by π (which takes $\hat{S}_{\boldsymbol{i}}^{x}$ to $-\hat{S}_{\boldsymbol{i}}^{x}$ and $\hat{S}_{\boldsymbol{i}}^{y}$ to $-\hat{S}_{\boldsymbol{i}}^{y}$, and leaves $\hat{S}_{\boldsymbol{i}}^{z}$ invariant). Further, the Hamiltonian is a real matrix. For thermal states $\hat{\varrho} = e^{-\beta\hat{H}}/Z$, these properties of the Hamiltonian imply $\langle \hat{S}_{\boldsymbol{i}}^{x} \rangle = \langle \hat{S}_{\boldsymbol{i}}^{y} \rangle = \langle \hat{S}_{\boldsymbol{i}}^{z} \hat{S}_{\boldsymbol{j}}^{x} \rangle = \langle \hat{S}_{\boldsymbol{i}}^{z} \hat{S}_{\boldsymbol{j}}^{y} \rangle = 0$, and $\langle \hat{S}_{\boldsymbol{i}}^{y} \hat{S}_{\boldsymbol{j}}^{x} \rangle = 0$ (note that, in experimental reality, symmetries are not respected and these expectation values may be finite). Hence,

$$E_{\mathrm{BSA}}(\boldsymbol{q}) = 1 - \sum_{\alpha,\beta} \frac{\delta_{\alpha,\beta} - \bar{q}_{\alpha}\bar{q}_{\beta}}{NC_s} \langle \hat{S}_{\alpha,\beta}(\boldsymbol{q}) \rangle = 1 - \frac{1}{NC_s} \sum_{\alpha} \left(1 - \bar{q}_{\alpha}^2\right) \langle \hat{S}_{\alpha,\alpha}(\boldsymbol{q}) \rangle, \tag{C5}$$

where, assuming $\boldsymbol{q} \neq \boldsymbol{0}$ and using translational invariance (such that we may write $s_z = \langle \hat{S}_{\boldsymbol{i}}^{z} \rangle$),

$$\begin{aligned}
\langle \hat{S}_{\alpha,\alpha}(\boldsymbol{q}) \rangle &= \sum_{\boldsymbol{i},\boldsymbol{j}} e^{i\boldsymbol{q}\cdot(\boldsymbol{i}-\boldsymbol{j})} \langle \hat{S}_{\boldsymbol{i}}^{\alpha} \hat{S}_{\boldsymbol{j}}^{\alpha} \rangle \\
&= \sum_{\boldsymbol{i},\boldsymbol{j}} e^{i\boldsymbol{q}\cdot(\boldsymbol{i}-\boldsymbol{j})} \left(\langle \hat{S}_{\boldsymbol{i}}^{\alpha} \hat{S}_{\boldsymbol{j}}^{\alpha} \rangle - \langle \hat{S}_{\boldsymbol{i}}^{\alpha} \rangle \langle \hat{S}_{\boldsymbol{j}}^{\alpha} \rangle \right) + \sum_{\boldsymbol{i},\boldsymbol{j}} e^{i\boldsymbol{q}\cdot(\boldsymbol{i}-\boldsymbol{j})} \langle \hat{S}_{\boldsymbol{i}}^{\alpha} \rangle \langle \hat{S}_{\boldsymbol{j}}^{\alpha} \rangle \\
&= \sum_{\boldsymbol{i},\boldsymbol{j}} e^{i\boldsymbol{q}\cdot(\boldsymbol{i}-\boldsymbol{j})} \delta_{i_y,j_y}\delta_{i_z,j_z} \left(\langle \hat{S}_{\boldsymbol{i}}^{\alpha} \hat{S}_{\boldsymbol{j}}^{\alpha} \rangle - \langle \hat{S}_{\boldsymbol{i}}^{\alpha} \rangle \langle \hat{S}_{\boldsymbol{j}}^{\alpha} \rangle \right) + \delta_{\alpha,z} s_z^2 N^2 \delta_{\boldsymbol{q},\boldsymbol{0}} \\
&= \sum_{\boldsymbol{i},\boldsymbol{j}} e^{iq_x(i_x-j_x)} \delta_{i_y,j_y}\delta_{i_z,j_z} \left(\langle \hat{S}_{\boldsymbol{i}}^{\alpha} \hat{S}_{\boldsymbol{j}}^{\alpha} \rangle - \langle \hat{S}_{\boldsymbol{i}}^{\alpha} \rangle \langle \hat{S}_{\boldsymbol{j}}^{\alpha} \rangle \right) \\
&= L^2 \sum_{i,j} e^{iq_x(i-j)} \left(\langle \hat{S}_{i}^{\alpha} \hat{S}_{j}^{\alpha} \rangle_{\mathrm{1D}} - \langle \hat{S}_{i}^{\alpha} \rangle_{\mathrm{1D}} \langle \hat{S}_{j}^{\alpha} \rangle_{\mathrm{1D}} \right) \\
&=: L^2 \sum_{i,j} c_{i-j}^{\alpha}(q_x).
\end{aligned}$$

Due to translational invariance, we have $c_l^{\alpha}(q) = c_{l+L}^{\alpha}(q) = c_{l-L}^{\alpha}(q) = [c_{-l}^{\alpha}(q)]^*$, and hence for L even,

$$\begin{aligned}
\sum_{i,j} c_{i-j}^{\alpha}(q) &= L c_0^{\alpha}(q) + L c_{L/2}^{\alpha}(q) + 2L \sum_{l=1}^{L/2-1} \mathrm{Re}\left[c_l^{\alpha}(q) \right] \\
&= L\left(\frac{1}{4} - \delta_{\alpha,z} s_z^2 \right) + L c_{L/2}^{\alpha}(q) + 2L \sum_{l=1}^{L/2-1} \mathrm{Re}\left[c_l^{\alpha}(q) \right],
\end{aligned} \tag{C6}$$

i.e.,

$$E(\boldsymbol{q}) = -1 + 4s_z^2\left(1 - \bar{q}_z^2\right) - 4 \sum_{\alpha} \left(1 - \bar{q}_{\alpha}^2\right) \left(c_{L/2}^{\alpha}(q_x) + 2 \sum_{l=1}^{L/2-1} \mathrm{Re}\left[c_l^{\alpha}(q_x) \right] \right). \tag{C7}$$

For the correlation functions, we use the results of [59] ($1 \leqslant l \leqslant L/2$),

$$\begin{aligned}
e^{-iql} c_l^{x}(q) &= \frac{1}{4} \begin{vmatrix} G_{-1} & G_{-2} & \cdots & G_{-l} \\ G_0 & G_{-1} & \cdots & G_{-l+1} \\ \vdots & \vdots & \ddots & \vdots \\ G_{l-2} & G_{l-3} & \cdots & G_{-1} \end{vmatrix}, \\
e^{-iql} c_l^{y}(q) &= \frac{1}{4} \begin{vmatrix} G_{1} & G_{0} & \cdots & G_{-l+2} \\ G_{2} & G_{1} & \cdots & G_{-l+3} \\ \vdots & \vdots & \ddots & \vdots \\ G_{l} & G_{l-1} & \cdots & G_{1} \end{vmatrix}, \\
e^{-iql} c_l^{z}(q) &= -\frac{1}{4} G_l G_{-l},
\end{aligned} \tag{C8}$$

where, for $L \to \infty$,

$$\begin{aligned}
s_z &= \frac{1}{2\pi} \int_0^{\pi} d\phi \, \frac{\tanh[\beta\Lambda(\phi)/2]}{\Lambda(\phi)} [h - \cos(\phi)], \\
G_l &= \frac{1}{\pi} \int_0^{\pi} d\phi \, \frac{\tanh[\beta\Lambda(\phi)/2]}{\Lambda(\phi)} \cos(\phi l)[h - \cos(\phi)] + \frac{\gamma}{\pi} \int_0^{\pi} d\phi \, \frac{\tanh[\beta\Lambda(\phi)/2]}{\Lambda(\phi)} \sin(\phi l) \sin(\phi), \\
\Lambda(\phi) &= \sqrt{\gamma^2 \sin^2(\phi) + (h - \cos(\phi))^2}.
\end{aligned} \tag{C9}$$

[1] M. B. Plenio and S. Virmani, Quantum Inf. Comput. **7**, 1 (2007).
[2] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. **81**, 865 (2009).
[3] K. Audenaert, J. Eisert, M. B. Plenio, and R. F. Werner, Phys. Rev. A **66**, 042327 (2002).
[4] T. J. Osborne and M. A. Nielsen, Quantum Inf. Comput. **1**, 45 (2002).
[5] G. Vidal, Phys. Rev. Lett. **91**, 147902 (2003).
[6] M. B. Plenio, J. Eisert, J. Dreissig, and M. Cramer, Phys. Rev. Lett. **94**, 060503 (2005).
[7] J. Eisert, M. Cramer, and M. B. Plenio, Rev. Mod. Phys. **82**, 277 (2010).
[8] H.-C. Jiang, Z. Wang, and L. Balents, Nat. Phys. **8**, 902 (2012).
[9] S. Depenbrock, I. P. McCulloch, and U. Schollwock, Phys. Rev. Lett. **109**, 067201 (2012).
[10] O. Gühne, P. Hyllus, D. Bruß, A. Ekert, M. Lewenstein, C. Macchiavello, and A. Sanpera, Phys. Rev. A **66**, 062305 (2002).
[11] O. Gühne and G. Toth, Phys. Rep. **474**, 1 (2009).
[12] M. Barbieri, F. De Martini, G. Di Nepi, P. Mataloni, G. M. D'Ariano, and C. Macchiavello, Phys. Rev. Lett. **91**, 227901 (2003).
[13] M. Bourennane, M. Eibl, C. Kurtsiefer, S. Gaertner, H. Weinfurter, O. Gühne, P. Hyllus, D. Bruß, M. Lewenstein, and A. Sanpera, Phys. Rev. Lett. **92**, 087902 (2004).
[14] D. Leibfried, E. Knill, S. Seidelin, J. Britton, R. B. Blakestad, J. Chiaverini, D. B. Hume, W. M. Itano, J. D. Jost, C. Langer, R. Ozeri, R. Reichle, and D. J. Wineland, Nature (London) **438**, 639 (2005).
[15] H. Häffner, W. Hänsel, C. F. Roos, J. Benhelm, D. Chek-al-kar, M. Chwalla, T. Körber, U. D. Rapol, M. Riebe, P. O. Schmidt, C. Becher, O. Gühne, W. Dür, and R. Blatt, Nature (London) **438**, 643 (2005).
[16] J. Estève, C. Gross, A. Weller, S. Giovanazzi, and M. K. Oberthaler, Nature (London) **455**, 1216 (2008).
[17] I. D. Leroux, M. H. Schleier-Smith, and V. Vuletić, Phys. Rev. Lett. **104**, 250801 (2010).
[18] M. F. Riedel, P. Böhi, Y. Li, T. W. Hänsch, A. Sinatra, and P. Treutlein, Nature (London) **464**, 1170 (2010).
[19] A. Louchet-Chauvet, J. Appel, J. J. Renema, D. Oblak, N. Kjaergaard, and E. S. Polzik, New J. Phys. **12**, 065032 (2010).
[20] T. Monz, P. Schindler, J. T. Barreiro, M. Chwalla, D. Nigg, W. A. Coish, M. Harlander, W. Hänsel, M. Hennrich, and R. Blatt, Phys. Rev. Lett. **106**, 130506 (2011).
[21] X.-C. Yao, T.-X. Wang, P. Xu, H. Lu, G.-S. Pan, X.-H. Bao, C.-Z. Peng, C.-Y. Lu, Y.-A. Chen, and J.-W. Pan, Nat. Photon. **6**, 225 (2012).
[22] A. Chiuri, G. Vallone, N. Bruno, C. Macchiavello, D. Bruß, and P. Mataloni, Phys. Rev. Lett. **105**, 250501 (2010).
[23] M. Cramer, A. Bernard, N. Fabbri, L. Fallani, C. Fort, S. Rosi, F. Caruso, M. Inguscio, and M. B. Plenio, Nat. Commun. **4**, 2161 (2013).
[24] H. Wunderlich, G. Vallone, P. Mataloni, and M. B. Plenio, New J. Phys. **13**, 033033 (2011).
[25] K. Vogel and H. Risken, Phys. Rev. A **40**, 2847 (1989).
[26] M. Cramer, M. B. Plenio, S. T. Flammia, R. Somma, D. Gross, S. D. Bartlett, O. Landon-Cardinal, D. Poulin, and Y.-K. Liu, Nat. Commun. **1**, 149 (2010).
[27] P. Krammer, H. Kampermann, D. Bruß, R. A. Bertlmann, L. C. Kwek, and C. Macchiavello, Phys. Rev. Lett. **103**, 100502 (2009).
[28] M. Cramer, M. B. Plenio, and H. Wunderlich, Phys. Rev. Lett. **106**, 020401 (2011).
[29] R. Horodecki, M. Horodecki, and P. Horodecki, Phys. Rev. A **59**, 1799 (1999).
[30] F. G. S. L. Brandão, Phys. Rev. A **72**, 022310 (2005).
[31] K. M. R. Audenaert and M. B. Plenio, New J. Phys. **8**, 266 (2006).
[32] O. Gühne, M. Reimpell, and R. F. Werner, Phys. Rev. Lett. **98**, 110502 (2007).
[33] J. Eisert, F. G. S. L. Brandão, and K. M. R. Audenaert, New J. Phys. **9**, 46 (2007).
[34] T. A. Corcovilos, S. K. Baur, J. M. Hitchcock, E. J. Mueller, and R. G. Hulet, Phys. Rev. A **81**, 013415 (2010).
[35] C. Macchiavello and G. Morigi, Phys. Rev. A **87**, 044301 (2013).
[36] I. A. Zaliznyak and S.-H. Lee, in *Modern Techniques for Characterizing Magnetic Materials*, edited by Y. Zhu (Springer, Heidelberg, 2005).
[37] L. Van Hove, Phys. Rev. **95**, 249 (1954).
[38] M. P. Schulhof, P. Heller, R. Nathans, and A. Linz, Phys. Rev. B **1**, 2304 (1970); E. Balcar and S. W. Lovesey, *Theory of Magnetic Neutron and Photon Scattering* (Oxford University Press, New York, 1989), Chap. 1.7.
[39] R. J. Birgeneau, J. Skalyo, and G. Shirane, Phys. Rev. B **3**, 1736 (1971).
[40] R. J. Birgeneau, M. Greven, M. A. Kastner, Y. S. Lee, B. O. Wells, Y. Endoh, K. Yamada, and G. Shirane, Phys. Rev. B **59**, 13788 (1999).
[41] Y. J. Kim, R. J. Birgeneau, F. C. Chou, M. Greven, M. A. Kastner, Y. S. Lee, B. O. Wells, A. Aharony, O. Entin-Wohlman, I. Ya. Korenblit, A. B. Harris, R. W. Erwin, and G. Shirane, Phys. Rev. B **64**, 024435 (2001).
[42] M. Lewenstein and A. Sanpera, Phys. Rev. Lett. **80**, 2261 (1998).
[43] G. Vidal and R. Tarrach, Phys. Rev. A **59**, 141 (1999).
[44] M. Steiner, Phys. Rev. A **67**, 054305 (2003).
[45] G. Toth, C. Knapp, O. Gühne, and H. J. Briegel, Phys. Rev. Lett. **99**, 250405 (2007).
[46] G. Vitagliano, P. Hyllus, I. L. Egusquiza, and G. Toth, Phys. Rev. Lett. **107**, 240502 (2011).
[47] G. Vitagliano, I. Apellaniz, I. L. Egusquiza, and G. Toth, Phys. Rev. A **89**, 032307 (2014).
[48] H. F. Hofmann and S. Takeuchi, Phys. Rev. A **68**, 032103 (2003).
[49] Q. Y. He, Shi-Guo Peng, P. D. Drummond, and M. D. Reid, Phys. Rev. A **84**, 022107 (2011).
[50] A. F. Albuquerque *et al.*, J. Magn. Magn. Mater. **310**, 1187 (2007); http://alps.comp-phys.org; for all numerical results we used 150 000 Monte Carlo steps (after thermalization) ("sweeps") and 15 000 sweeps for thermalization ("thermalization").
[51] M. Mourigal, M. Enderle, A. Klöpperpieper, Jean-Sébastien Caux, Anne Stunault, and H. M. Rønnow, Nat. Phys. **9**, 435 (2013).
[52] R. Coldea, D. A. Tennant, R. A. Cowley, D. F. McMorrow, B. Dorner, and Z. Tylczynski, Phys. Rev. Lett. **79**, 151 (1997).
[53] M. Steiner, K. Kakurai, J. K. Kjems, D. Petitgrand, and R. Pynn, J. Appl. Phys. **61**, 3953 (1987).

[54] N. B. Christensen, H. M. Rønnow, D. F. McMorrow, A. Harrison, T. G. Perring, M. Enderle, R. Coldea, L. P. Regnault, and G. Aeppli, Proc. Natl. Acad. Sci. USA **104**, 15264 (2007).
[55] Y. S. Lee, M. Greven, B. O. Wells, R. J. Birgeneau, and G. Shirane, Eur. Phys. J. B **5**, 15 (1998).
[56] We have studied systems with total number of spins varying between 100 and 2500 and found no noticeable finite-size effects (differences between the bounds obtained were smaller than 0.01).
[57] R. Basak and I. Chatterjee, Phys. Rev. B **40**, 4627 (1989).
[58] E. Goovaerts, H. DeRaedt, and D. Schoemaker, Phys. Rev. Lett. **52**, 1649 (1984).
[59] E. Barouch and B. M. McCoy, Phys. Rev. A **3**, 786 (1971).
[60] P. W. Anderson, Mater. Res. Bull. **8**, 153 (1973).
[61] P. W. Anderson, Science **235**, 1196 (1987).
[62] L. Balents, Nature (London) **464**, 199 (2010).
[63] S. Yan, D. A. Huse, and S. R. White, Science **332**, 1173 (2011).
[64] N. Schuch, D. Poilblanc, J. I. Cirac, and D. Perez-Garcia, Phys. Rev. B **86**, 115108 (2012).
[65] T.-H. Han, J. S. Helton, S. Chu, D. G. Nocera, J. A. Rodriguez-Rivera, C. Broholm, and Y. S. Lee, Nature (London) **492**, 406 (2012).
[66] A. Y. Kitaev, Ann. Phys. (NY) **303**, 2 (2003).
[67] A. Chandran, D. Kaszlikowski, A. Sen(De), U. Sen, and V. Vedral, Phys. Rev. Lett. **99**, 170502 (2007).
[68] D. Poilblanc, N. Schuch, D. Perez-Garcia, and J. I. Cirac, Phys. Rev. B **86**, 014404 (2012).
[69] J. D. Klein, J. Phys. A **15**, 661 (1982).
[70] C. K. Majumdar and D. K. Ghosh, J. Math. Phys. **10**, 1388 (1969).
[71] J. M. Law, P. Reuvekamp, R. Glaum, C. Lee, J. Kang, M.-H. Whangbo, and R. K. Kremer, Phys. Rev. B **84**, 014426 (2011).
[72] D. Perez-Garcia, F. Verstraete, M. M. Wolf, and J. I. Cirac, Quantum Inf. Comput. **7**, 401 (2007).
[73] M. Asoudeh, V. Karimipour, and A. Sadrolashrafi, Phys. Rev. B **76**, 064433 (2007); V. Karimipour and L. Memarzadeh, *ibid.* **77**, 094416 (2008).

C

Designing Bell Inequalities from a Tsirelson Bound

Title:	Designing Bell Inequalities from a Tsirelson Bound
Authors:	M.E., Hermann Kampermann, and Dagmar Bruß
Journal:	Physical Review Letters
Impact factor:	7.512
Date of submission:	19 June 2013
Publication status:	Published
Contribution by M.E.:	First author (input approx. 80%)
Results:	Derivation of a simple Tsirelson bound, description of a geometrical picture, and application to dimension witnesses.

Designing Bell Inequalities from a Tsirelson Bound

Michael Epping,* Hermann Kampermann, and Dagmar Bruß
Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, Universitätsstrasse 1, D-40225 Düsseldorf, Germany
(Received 19 June 2013; published 11 December 2013)

We present a simple analytic bound on the quantum value of general correlation type Bell inequalities, similar to Tsirelson's bound. It is based on the maximal singular value of the coefficient matrix associated with the inequality. We provide a criterion for tightness of the bound and show that the class of inequalities where our bound is tight covers many famous examples from the literature. We describe how this bound helps to construct Bell inequalities, in particular inequalities that witness the dimension of the measured observables.

DOI: 10.1103/PhysRevLett.111.240404 PACS numbers: 03.65.Ud, 03.67.Mn

An interesting feature of quantum theory is correlations between outcomes of spatially separated measurements that contradict predictions of all theories based on common-sense assumptions called locality, reality, and free will [1,2]. This contradiction is shown by the violation of Bell inequalities. A famous version of them was derived by Clauser, Horne, Shimony, and Holt (CHSH) [3] and many generalizations followed [4–10]. In addition to ruling out local hidden variable theories, several other applications of Bell-type inequalities are known [11–15].

Regarding such applications one is interested in the maximal value of the Bell expression predicted by quantum theory and the corresponding measurements to achieve this optimum. Bounds on this quantum value were first derived by Tsirelson [16,17]. For general CHSH-type Bell inequalities (which will be defined later on), similar bounds can be derived. To this aim, approaches based on different physical principles have been developed, under them information causality [18–20], macroscopic reality [21], uncertainty principles [22], and exclusivity [23]. Furthermore, methods based on semidefinite programming are known [24–27]. In contrast here we present an analytical method to find a quantum bound, which makes use of standard tools of linear algebra only.

Our bound is related to the optimization of Ref. [24] with relaxed boundary conditions, which implies that our bound is not necessarily reachable. However, the class of Bell inequalities reaching our bound contains most examples from the literature. We introduce a constructive method to determine whether the bound is tight, which provides a geometric picture that allows us to construct new Bell inequalities. We exemplify this by constructing dimension witnessing Bell inequalities, analogous to the ones discussed in Refs. [7,28–31]. Different techniques to witness the dimension of a quantum system are described in Refs. [32,33]. Our construction of new Bell inequalities differs from known methods based on the correlation polytope [34,35] and variable elimination [36,37].

We start with considering general bipartite correlation type inequalities, where the two parties $i = 1, 2$ measure M_i different two-outcome observables $\mathcal{A}_i(x_i)$, with $x_i = 1, 2, \ldots, M_i$, on their part of the shared quantum state ρ (see Ref. [35] for an overview). The principal setup of an experiment associated with such an inequality is visualized in Fig. 1. The expectation value of the product of the measurement results of both parties in setting x_1 of party 1 and setting x_2 of party 2 is denoted by $E(x_1, x_2)$. In any local and realistic theory the inequality

$$\sum_{x_1=1}^{M_1}\sum_{x_2=1}^{M_2} g_{x_1,x_2} E_{\mathrm{lr}}(x_1, x_2) \leq B \tag{1}$$

holds, where g_{x_1,x_2} are real coefficients of a matrix g and B is the corresponding local hidden variable bound. It can be obtained by maximizing over all possible local realistic expectation values $E_{\mathrm{lr}}(x_1, x_2) = a_1(x_1)a_2(x_2)$, where $a_i(x_i) = \pm 1$ is the measurement result in setting x_i of party i. Throughout this Letter we are interested in similar bounds T on the quantum value Q,

$$Q := \max_{\rho,\mathcal{A}_1,\mathcal{A}_2} \sum_{x_1=1}^{M_1}\sum_{x_2=1}^{M_2} g_{x_1,x_2} E(x_1, x_2) \leq T, \tag{2}$$

where $E(x_1, x_2) = \mathrm{tr}((\rho\, \mathcal{A}_1(x_1) \otimes \mathcal{A}_2(x_2))$ is the expectation value predicted by quantum theory. If the quantum value Q violates inequality (1), i.e., $Q > B$, we call

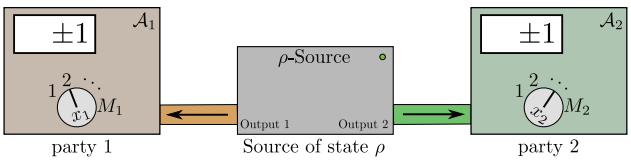


FIG. 1 (color online). Illustration of a bipartite Bell experiment. The source prepares the state ρ and distributes one subsystem to each party. Each party i can choose between M_i different measurement settings $[\mathcal{A}_i(x_i), \quad x_i = 1, \ldots, M_i]$. Multiplying the two results of both parties, which are $+1$ or -1, and repeating the experiment many times gives the expectation value $E(x_1, x_2)$. Bounds on linear combinations of $E(x_1, x_2)$ for different x_1 and x_2 are discussed in the text.

inequality (1) a Bell inequality. We now derive an upper bound T on the quantum value Q using the singular value decomposition of the coefficient matrix g [see Eq. (1)]. For any real $M_1 \times M_2$–matrix g we define an orthogonal $M_1 \times M_1$–matrix V, a diagonal $M_1 \times M_2$–matrix S, containing the singular values, and an orthogonal $M_2 \times M_2$–matrix W, such that

$$g = VSW^T. \tag{3}$$

We use the convention of nonincreasing order on the diagonal of S. The matrices V and W are uniquely defined up to unitary operations on spaces associated with degenerate singular values. The maximal singular value S_{11} will be written as $||g||_2$, the spectral norm of g, which is defined as $||g||_2 = \max_{\vec{x},|\vec{x}|=1}|g\vec{x}|$. The multiplicity of $||g||_2$, i.e., the dimension of the corresponding space, is denoted by d. We will also use the truncated singular value decomposition associated with the maximal singular value only. In this case the matrices are denoted V^d, S^d, and W^d. See Fig. 2 for an illustration of the dimensions of the involved matrices.

With these definitions we can formulate the quantum bound for inequality (1).

Theorem 1. Let there be two parties, labeled with $i = 1, 2$, sharing a state given by a density matrix ρ, i.e., a positive semidefinite $D \times D$ matrix, $D \in \mathbb{N}$, with $\mathrm{tr}\rho = 1$. Let $\{\mathcal{A}_i(x_i)\colon 1 \le x_i \le M_i\}$ be a set of observables with all eigenvalues in $[-1, 1]$ on the subsystem of party i. The expectation value in setting (x_1, x_2) is

$$E(x_1, x_2) = \mathrm{tr}(\mathcal{A}_1(x_1) \otimes \mathcal{A}_2(x_2)\rho). \tag{4}$$

For real coefficients g_{x_1,x_2} the bound

$$\sum_{x_1=1}^{M_1}\sum_{x_2=1}^{M_2} g_{x_1,x_2}E(x_1, x_2) \le \sqrt{M_1 M_2}||g||_2 =: T \tag{5}$$

holds, where $\|g\|_2$ is the maximal singular value of g.

Proof.—As the maximal value of the Bell inequality is achieved by a pure state, it is sufficient to focus on these. The basic idea is to use a well-known result of Tsirelson [16] to map physical observables to real vectors and bound the resulting expression using their length and the maximal singular value of g. In order to prevent confusion, the notation of Tsirelson's theorem is adopted to the one used here.

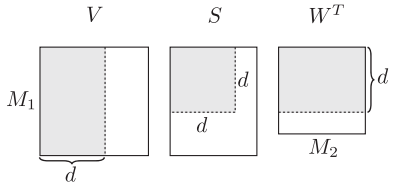


FIG. 2. The dimensions of the matrices V, S and W. The shaded parts belong to the truncated singular value decomposition (V^d, S^d and W^d) for the maximal singular value.

Theorem (Tsirelson [16]). Given sets of observables $\mathcal{A}_1(1), \ldots, \mathcal{A}_1(M_1)$ and $\mathcal{A}_2(1), \ldots, \mathcal{A}_2(M_2)$, whose eigenvalues lie in $[-1, 1]$, and an arbitrary bipartite state $|\psi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$, there exist real unit vectors $\vec{v}_1, \ldots, \vec{v}_{M_1}, \vec{w}_1, \ldots, \vec{w}_{M_2} \in \mathbb{R}^{M_1+M_2}$ such that for all settings $x_1 \in \{1, \ldots, M_1\}$ and $x_2 \in \{1, \ldots, M_2\}$ the expectation value can be written as

$$E(x_1, x_2) = \langle\psi|\mathcal{A}_1(x_1) \otimes \mathcal{A}_2(x_2)|\psi\rangle = \vec{v}_{x_1}^T \vec{w}_{x_2}. \tag{6}$$

This theorem ensures one can write

$$\sum_{x_1=1}^{M_1}\sum_{x_2=1}^{M_2} g_{x_1,x_2}E(x_1, x_2) = \vec{V}^T(g \otimes \mathbb{1}^{M_1+M_2})\vec{W}, \tag{7}$$

where we introduced the vectors

$$\vec{V} = \begin{pmatrix} \vec{v}_1 \\ \vdots \\ \vec{v}_{M_1} \end{pmatrix} \quad \text{and} \quad \vec{W} = \begin{pmatrix} \vec{w}_1 \\ \vdots \\ \vec{w}_{M_2} \end{pmatrix}. \tag{8}$$

The relation between these vectors and the matrices V and W from the singular value decomposition of g will become clear in Theorem 2. From Eq. (7) we see that Q can be bounded by use of the maximal singular value of $(g \otimes \mathbb{1}^{M_1+M_2})$, which is the same as the maximal singular value of g, and the length of $\vec{V}$ and $\vec{W}$. Because the $\vec{v}_i$ and $\vec{w}_j$ are normalized vectors, the lengths of $\vec{V}$ and $\vec{W}$ are $\sqrt{M_1}$ and $\sqrt{M_2}$, respectively. This finishes the proof.

The bound in Theorem 1 holds for any inequality given by an arbitrary real matrix g. But so far we did not discuss the quality of the bound and indeed not for all matrices g is the bound achievable (see example 6 in the Supplemental Material [38]). In the next theorem we give a necessary and sufficient condition for tightness of our bound.

Theorem 2.—For a given real $M_1 \times M_2$–matrix g and the corresponding matrices V^d and W^d (see Fig. 2), the bound (5) can be reached with observables, which are linked via Eq. (6) to $d' \le d$-dimensional real vectors $\vec{v}_i$ and $\vec{w}_j$ given by

$$\vec{v}_i = \alpha^T V^d_{i,*}, \tag{9}$$

$$\vec{w}_j = \sqrt{\frac{M_2}{M_1}}\,\alpha^T W^d_{j,*}, \tag{10}$$

if and only if the system of equations

$$\|\alpha^T V^d_{i,*}\|^2 = 1, \quad \forall\ i \in \{1, 2, \ldots, M_1\} \tag{11}$$

$$\|\alpha^T W^d_{j,*}\|^2 = \frac{M_1}{M_2}, \quad \forall\ j \in \{1, 2, \ldots, M_2\} \tag{12}$$

is solvable. Here the $d \times d'$–matrix α is the unknown and $V^d_{i,*}$ and $W^d_{j,*}$ denote column vectors containing the

elements of the ith row of V^d and the jth row of W^d, respectively.

The proof is given in the Supplemental Material [38]. The main idea of the proof is, that the bound is reachable, if and only if there exist singular vectors to the maximal singular value of $g \otimes \mathbb{1}^{M_1+M_2}$, $\vec{V}$, and $\vec{W}$ [see Eq. (8)], where the vectors $\vec{v}_i$ and $\vec{w}_j$ are unit vectors [see Tsirelson's theorem in Eq. (6)].

Note that all vectors that fulfill Eq. (11) lie on the surface of a d-dimensional origin-centered ellipsoid (see Fig. 3). If the vectors $V^d_{i,*}$ and $W^d_{j,*}$ permit us to find an ellipsoid such that they all lie on it's surface, then the bound is tight. If semiaxes are infinite, e.g., if the ellipsoid is not uniquely defined, then $d' < d$ and the corresponding α does not have full rank. In particular $d' = 1$ implies, that one-dimensional vectors reach the bound, the inequality (1) cannot be violated and thus it is no Bell inequality [see Fig. 3(b)]. An algorithm solving Eqs. (11) and (12) in $\mathcal{O}((M_1 + M_2)^3)$ is described in the Supplemental Material [38]. From the real vectors $\vec{v}_i$ and $\vec{w}_j$ the observables can be obtained using representants of a Clifford algebra; see Ref. [17].

In the following we provide two sufficient criteria for inequality (5) being tight.

Corollary 1.—If

$$\|V^d_{i,*}\| = \sqrt{\frac{d}{M_1}}, \quad \forall\ i \in \{1, 2, \ldots, M_1\}, \tag{13}$$

and

$$\|W^d_{j,*}\| = \sqrt{\frac{d}{M_2}}, \quad \forall\ j \in \{1, 2, \ldots, M_2\}, \tag{14}$$

then the bound is tight.

Proof.—The matrix $\alpha = (M_1/d)\mathbb{1}^d$ solves the system of equations (11) and (12).

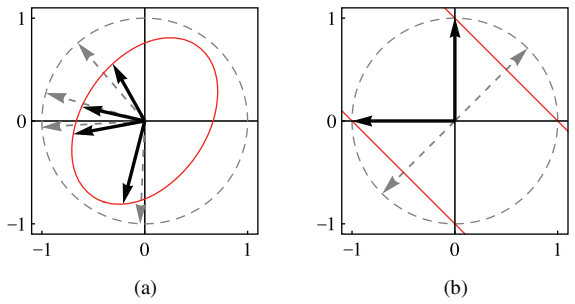


FIG. 3 (color online). The vectors $V^d_{i,*}$, $i = 1, 2, \ldots, M_1$ (black) can be normalized by applying the matrix α^T, if they lie on an origin-centered ellipsoid (red), i.e., the vectors $\vec{v}_i = \alpha^T V^d_{i,*}$ lie on the unit sphere (dashed). An analogous picture could be drawn for $\vec{w}_j$, $j = 1, 2, \ldots, M_2$. (a) In this example $d = 2$ and $M_1 = 4$. The four vectors uniquely define an ellipse. (b) In this example $d = 2$ and $M_1 = 2$. This ellipse is not uniquely defined by the vectors $V^d_{i,*}$. The one shown has one infinite semiaxis.

A second corollary treats the special case when g is a square matrix and all singular values are the same.

Corollary 2.—If $d = M_1 = M_2$, then inequality (5) is tight.

Proof.—Due to the orthogonality of V and W, $\alpha = \mathbb{1}^d$ solves the system of equations (11) and (12).

An application of this corollary is illustrated in the following example.

Example 1.—Inequalities with coefficients

$$g = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}^{\otimes k} \tag{15}$$

are considered in Ref. [39], where for $k = 2$ an upper bound of $4\sqrt{10}$ for the quantum value is given. Inequality (5) improves this bound to $T = 8$, which coincides with the local realistic bound B. Note that Corollary 2 states that the bound $T(k) = 2^{3k/2}$ is tight for all k. It can be easily seen, that for all even k, the classical value coincides with the quantum bound; i.e., the inequality is no Bell inequality. For odd k numerical evidence indicates that the violation vanishes. Therefore we do not expect the violation to reach $Q/B = \sqrt{3}$ in the limit of large k, different to the conjecture in Ref. [39]. A value of $Q/B = \sqrt{3}$ would be near the maximal violation (Grothendieck's constant) for any bipartite full correlation Bell experiment [40]. Please note that the well-known CHSH inequality is incorporated as the special case with $k = 1$.

Several more examples are given in the Supplemental Material [38], amongst them the famous CHSH inequality [3] (example 5) and inequalities by Braunstein and Caves [5] (example 8), Vertesi and Pál [7] (example 7), Gisin [9] (example 9), and Fishburn and Reeds [40] (example 10).

The presented method can be generalized to more than two parties. All n-party Bell inequalities considered here are of the form

$$\sum_{x_1,\ldots,x_n=1}^{M_1,\ldots,M_n} g(x_1, \ldots, x_n) E_{\mathrm{lr}}(x_1, \ldots, x_n) \leq B. \tag{16}$$

Each party i receives a subsystem from the source and measures it in a setting $x_i \in \{1, 2, \ldots, M_i\}$. Suppose a time order such that all but the first two parties do this before party 1 and 2. Then the setup is exactly the same as considered before, where the bipartite state is obtained by tracing out parties 3 to n. Formalizing this one sees that

$$\sum_{x_1,\ldots,x_n=1}^{M_1,\ldots,M_n} g(x_1, \ldots, x_n) E(x_1, \ldots, x_n) \leq T \tag{17}$$

with

$$T = \sqrt{M_1 M_2} \sum_{x_3,\ldots,x_n}^{M_3,\ldots,M_n} \|g_{*,*,x_3,\ldots,x_n}\|_2. \tag{18}$$

Here $g_{*,*,x_3,\ldots,x_n}$ denotes the matrix found in the nth-order tensor g by fixing all but the first two indices. In general

labeling different parties as 1 and 2 leads to different values of the bound.

Example 2 (Mermin inequality). The Mermin inequality is given by coefficients

$$g(x_1, \ldots, x_n) = \cos\left(\frac{\pi}{2}(x_1 + x_2 + \cdots + x_n)\right). \quad (19)$$

Equation (18) gives the bound

$$T = 2 \sum_{x_3,\ldots,x_n} \underbrace{\|g_{*,*,x_3,\ldots,x_n}\|_2}_{=1} = 2^{n-1}, \quad (20)$$

which is achievable with a GHZ state [4]. Thus the bound is tight for this family of inequalities.

The insights on the mathematical structure gained above help to construct new Bell inequalities. We focus on the minimal dimension of the involved observables required for the maximal violation. The dimension d of the real vectors $\vec{v}_i$ and $\vec{w}_j$ is linked to the dimension of the corresponding observables D. Due to the explicit construction of observables in Ref. [17], we know that

$$D \leq 2^{\lfloor d/2 \rfloor} \quad (21)$$

is possible, while it is also known [28] that

$$D \geq \left\lceil \frac{d+1}{2} \right\rceil \quad (22)$$

is necessary. We construct g such that Eqs. (11) and (12) are fulfilled for some matrix α with rank d. This implies that the maximal violation can be achieved using d-dimensional real vectors $\vec{v}_i$ and $\vec{w}_j$. If in some experiment only qubits ($D = 2$) are available, then one can construct Bell inequalities with $d \leq 3$, ensuring that the maximal violation is within the scope of this experiment. This can be done by explicitly constructing the singular value decomposition of g, e.g.,

$$g = V \mathrm{diag}\{2, 2, 2, 1, \ldots, 1\} W^T, \quad (23)$$

where V and W are unitary matrices, such that the conditions of Theorem 2, Corollary 1, or Corollary 2 are fulfilled.

Example 3 (Inequality for qubits). Consider the Bell inequality corresponding to a matrix g given by Eq. (23) for

$$V = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}^{\otimes 2}, \quad (24)$$

and

$$W = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \otimes \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}. \quad (25)$$

By construction, the maximal quantum value is $Q = 8$, while $B = 4\sqrt{2}$ is the maximum achievable value within local hidden variable theories. From Eq. (23) we know that $d = 3$ and the maximal violation is achievable with qubits. Note that the singular value $S_{44} = 1$ needs only to be smaller than $||g||_2 = 2$; i.e., it can also be chosen to be 0.

Furthermore one might be interested in constructing Bell inequalities that cannot be violated by systems with dimension smaller than some chosen dimension. Such Bell inequalities are a recent development called dimension witnesses [7,28–33]. Here the unitary matrices V and W are constructed such that a rank d solution α exists, but not a rank $d-1$ solution. We can assume α to be a symmetric $d \times d$ matrix (see the Supplemental Material [38]), i.e., α contains $d(d+1)/2$ degrees of freedom. Therefore $d(d+1)/2$ vectors, that lie on a d-dimensional ellipsoid with finite semiaxes and lead to independent equations (11) or (12), determine α and thus also its rank to be d. Note that the rows of both V^d and W^d form this set of vectors. The following simple construction illustrates this method.

Example 4 (Random dimension witness) Given $d \in \mathbb{N}$ greater or equal two, let $k = \lfloor (d-1)/2 \rfloor + 1$ and U_i, $i \in \{1, \ldots, k\}$, be random unitary $d \times d$ matrices. The inequality with coefficients given by the following $kd \times d$ matrix

$$g = \begin{pmatrix} U_1 \\ U_2 \\ \vdots \\ U_k \end{pmatrix} \quad (26)$$

corresponds to a Bell inequality. Note that the truncated singular value decomposition of g can be read from Eq. (26) as $V^d = (1/\sqrt{k})g$, $S^d = \sqrt{k}\mathbb{1}^d$, $W^d = \mathbb{1}^d$. The maximal quantum value $Q = kd$ is achievable (Corollary 1). With probability one, the kd measurement directions of party 1 and the d measurement directions of party 2 uniquely define a d-dimensional ellipsoid. Note that due to the orthogonality of U_i, more than $d(d+1)/2$ measurement directions are used. Observables corresponding to real vectors spanning a space with dimension smaller than d do not suffice to observe a maximal violation of such a Bell inequality and therefore it can be used as a dimension witness. The number of measurement settings needed to witness dimension d with this method is only $\mathcal{O}(d^2)$, while it is $\mathcal{O}(2^d)$ for the witness proposed in Ref. [7]; see example 7 in the Supplemental Material [38].

In conclusion we introduced an approach for calculating upper bounds on the quantum value of correlation type Bell inequalities. Computing the bound only requires the principal singular value of the coefficient matrix. We described how the tightness of the bound can be tested. If the bound is reachable, which we find in several important examples, this method leads to optimal observables in a natural way. Reversely, we showed how understanding the optimality conditions for our bound allows us to construct Bell inequalities with chosen properties, in particular properties of optimal observables, including their dimension. The tools developed here may be useful to construct Bell

inequalities with stronger violations than the known inequalities for this scenario. Amongst other advantages, this may help to close the detection loophole in Bell test experiments. Furthermore, an improved generalization of the bound for three and more parties is possibly of avail.

We thank Costantino Budroni, Otfried Gühne, and Tobias Moroder for helpful discussions. M. E. is supported by Deutsche Forschungsgemeinschaft (DFG).

*epping@thphy.uni-duesseldorf.de

[1] J. S. Bell, Physics (N.Y.) **1**, 195 (1964).
[2] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **81**, 5039 (1998).
[3] J. Clauser, M. Horne, A. Shimony, and R. Holt, Phys. Rev. Lett. **23**, 880 (1969).
[4] N. D. Mermin, Phys. Rev. Lett. **65**, 1838 (1990).
[5] S. Braunstein and C. Caves, Ann. Phys. (N.Y.) **202**, 22 (1990).
[6] E. G. Cavalcanti, C. J. Foster, M. D. Reid, and P. D. Drummond, Phys. Rev. Lett. **99**, 210405 (2007).
[7] T. Vértesi and K. F. Pál, Phys. Rev. A **77**, 042106 (2008).
[8] I. Pitowsky and K. Svozil, Phys. Rev. A **64**, 014102 (2001).
[9] N. Gisin, Phys. Lett. A **260**, 1 (1999).
[10] W. Laskowski, T. Paterek, M. Zukowski, and C. Brukner, Phys. Rev. Lett. **93**, 200401 (2004).
[11] C. Brukner, M. Zukowski, J.-W. Pan, and A. Zeilinger, Phys. Rev. Lett. **92**, 127901 (2004).
[12] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[13] J. Barrett, L. Hardy, and A. Kent, Phys. Rev. Lett. **95**, 010503 (2005).
[14] S. Pironio, A. Acín, S. Massar, A. de la Giroday, D. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. Manning, and C. Monroe, Nature (London) **464**, 1021 (2010).
[15] D. Mayers and A. C.-C. Yao, Quantum Inf. Comput. **4**, 273 (2004).
[16] B. Tsirelson, Lett. Math. Phys. **4**, 93 (1980).
[17] B. Tsirelson, Hadronic J. **8**, 329 (1993), http://www.tau.ac.il/~tsirel/download/hadron.html.
[18] J. Allcock, N. Brunner, M. Pawlowski, and V. Scarani, Phys. Rev. A **80**, 040103 (2009).
[19] M. Pawlowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, and M. Zukowski, Nature (London) **461**, 1101 (2009).
[20] R. Gallego, L. E. Würflinger, A. Acín, and M. Navascués, Phys. Rev. Lett. **107**, 210403 (2011).
[21] M. Navascués and H. Wunderlich, Proc. Phys. Soc. London Sect. A **466**, 881 (2009).
[22] J. Oppenheim and S. Wehner, Science **330**, 1072 (2010).
[23] A. Cabello, Phys. Rev. Lett. **110**, 060402 (2013).
[24] S. Wehner, Phys. Rev. A **73**, 022110 (2006).
[25] M. Navascués, S. Pironio, and A. Acin, Phys. Rev. Lett. **98**, 010401 (2007).
[26] M. Navascués, S. Pironio, and A. Acín, New J. Phys. **10**, 073013 (2008).
[27] A. C. Doherty, Y.-C. Liang, B. Toner, and S. Wehner, P. IEEE CCC **08**, 199 (2008).
[28] T. Vértesi and K. F. Pál, Phys. Rev. A **79**, 042106 (2009).
[29] N. Brunner, S. Pironio, A. Acin, N. Gisin, A. A. Méthot, and V. Scarani, Phys. Rev. Lett. **100**, 210503 (2008).
[30] R. Gallego, N. Brunner, C. Hadley, and A. Acín, Phys. Rev. Lett. **105**, 230501 (2010).
[31] T. Moroder, J.-D. Bancal, Y.-C. Liang, M. Hofmann, and O. Gühne, Phys. Rev. Lett. **111**, 030501 (2013).
[32] M. M. Wolf and D. Perez-Garcia, Phys. Rev. Lett. **102**, 190504 (2009).
[33] S. Wehner, M. Christandl, and A. C. Doherty, Phys. Rev. A **78**, 062112 (2008).
[34] I. Pitowsky, J. Math. Phys. (N.Y.) **27**, 1556 (1986).
[35] A. Peres, Found. Phys. **29**, 589 (1999).
[36] D. Avis, H. Imai, T. Ito, and Y. Sasaki, arXiv:quant-ph/0404014v3.
[37] C. Budroni and A. Cabello, J. Phys. A **45**, 385304 (2012).
[38] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.111.240404 for the proof of Theorem 2, the mentioned algorithm, and several examples.
[39] H. Heydari, J. Phys. A **39**, 1 (2006).
[40] P. Fishburn and J. Reeds, SIAM J. Discrete Math. **7**, 48 (1994).

Supplemental Material for Epping et al. "Designing Bell inequalities from a Tsirelson bound"

A. PROOF OF THEOREM 2

From the proof of Theorem 1 we know that

$$\sum_{x_1=1}^{M_1}\sum_{x_2=1}^{M_2} g_{x_1,x_2}E(x_1,x_2) = \vec{V}^T(g\otimes \mathbb{1}^{M_1+M_2})\vec{W} \tag{26}$$

where the real vectors $\vec{V}$ and $\vec{W}$ are defined in Eq. (8). From this we see, that the bound is reached, if and only if $\vec{V}$ and $\vec{W}$ are "matching" singular vectors to the maximal singular value, i.e. $(g\otimes \mathbb{1}^{M_1+M_2})\vec{W} = \sqrt{M_2/M_1}||g||_2\vec{V}$, while at the same time the respective vectors $\vec{v}_i$ and $\vec{w}_j$ are unit vectors. The normalization of $\vec{v}_i$ and $\vec{w}_j$ is required by Tsirelson's theorem. General singular vectors to the maximal singular value can be written as

$$\vec{V} = \sum_{l_1=1}^{d}\sum_{l_2=1}^{M_1+M_2} \alpha_{l_1,l_2}V_{*,l_1}\otimes \mathbb{1}^{M_1+M_2}_{*,l_2}, \tag{27}$$

$$\vec{W} = \sum_{l_1=1}^{d}\sum_{l_2=1}^{M_1+M_2} \beta_{l_1,l_2}W_{*,l_1}\otimes \mathbb{1}^{M_1+M_2}_{*,l_2}, \tag{28}$$

where V_{*,l_1} denotes the l_1-th row of the matrix V as a column vector and $\mathbb{1}^{M_1+M_2}_{*,l_2}$ denotes the l_2-th canonical basis vector. The fact that $\vec{V}$ matches $\vec{W}$ becomes manifest in

$$\alpha_{l_1,l_2} = \sqrt{\frac{M_1}{M_2}}\beta_{l_1,l_2}. \tag{29}$$

We are interested in the components α_{l_1,l_2} introduced in Eqs. (27) and (28). They are restricted by the norm conditions for $\vec{v}_i$ and $\vec{w}_j$, which read

$$1 = ||\vec{v}_i||^2 = ||\alpha^T V^d_{i,*}||^2 \tag{30}$$

$$\text{and } 1 = ||\vec{w}_i||^2 = \sqrt{\frac{M_2}{M_1}}||\alpha^T W^d_{i,*}||^2. \tag{31}$$

Therefore the bound is tight, if and only if this system of equations is solvable. We conclude by showing, how the number of columns of α is related to the dimension of the measurement vectors. If and only if the bound is reachable with d'-dimensional vectors $\vec{v}_i$, $\vec{w}_j$, the system of equations is solvable by a $d\times d'$-matrix α, where $d'\leq d$.

"⇐": If α is a $d\times d'$-matrix that solves the system of equations, then

$$d' \geq \operatorname{rank}\alpha \geq \dim \operatorname{span}\{v_i, w_j\}, \tag{32}$$

where the last $\geq$-sign holds because $\vec{v}_i = \alpha^T V^d_{i*}$ and $\vec{w}_i = \sqrt{\frac{M_2}{M_1}}\alpha^T W^d_{i*}$, i.e. $\vec{v}_i$ and $\vec{w}_j$ lie in the image of α^T. The result $\dim\operatorname{span}\{v_i,w_j\}\leq d'$ implies, that after some appropriate rotation, $(\vec{v}_i)_k = 0$ and $(\vec{w}_j)_l = 0$ for $k,l>d'$ and all i,j. Therefore $\vec{v}_i$ and $\vec{w}_j$ can be considered to be elements of $\mathbb{R}^{d'}$. Observables associated with these d'-dimensional vectors permit maximal violation.

"⇒": If the bound is reachable with d'-dimensional vectors $\vec{v}_i$, $\vec{w}_j$, then all vectors $\vec{v}_i$ and $\vec{w}_j$ lie on a d'-dimensional unit sphere. Without affecting the mapping of the $\vec{v}_i$ and $\vec{w}_j$, the image of α can be chosen to coincide with the d' dimensional subspace spanned by $\vec{v}_i$ and $\vec{w}_j$, so the rank of α can be chosen to be d'. The rank is equal to the number of nonzero singular values. The truncated singular value decomposition associated with all nonzero singular values equals α. Let us call it $\alpha = \tilde{V}\tilde{S}\tilde{W}^T$, so $\alpha\alpha^T = \tilde{V}\tilde{S}\tilde{W}^T\tilde{W}\tilde{S}\tilde{V}^T = \tilde{V}\tilde{S}\tilde{S}\tilde{V}^T$, therefore $\alpha' = \tilde{V}\tilde{S}$ is a $d\times d'$-matrix solving the system of equations.

B. ALGORITHM TO FIND α

We want to find the solution α to the system of equations

$$||\alpha^T V^d_{i,*}||^2 = 1 \qquad \forall i \in \{1, 2, ..., M_1\} \tag{33}$$

$$||\alpha^T W^d_{j,*}||^2 = \frac{M_1}{M_2} \qquad \forall j \in \{1, 2, ..., M_2\}. \tag{34}$$

It is convenient to rewrite these equations as

$$A^T_{i,*} X A_{i,*} = 1 \qquad \forall i \in \{1, 2, ..., M_1 + M_2\} \tag{35}$$

where $X = \alpha\alpha^T$ is unknown and

$$A = \begin{pmatrix} V^d \\ \sqrt{\frac{M_2}{M_1}} W^d \end{pmatrix} \tag{36}$$

is a $(M_1 + M_2) \times d$ matrix containing all the vectors $A_{i,*}$ which will be normalized after application of α^T (if possible). Eq. (35) restricts X on the space spanned by these vectors. Unaffected by their linear dependence, the unknown X in Eq. (35) can be defined via it's action on these vectors,

$$X A_{i,*} = \sum_k \tilde{c}_{i,k} A_{k,*}, \tag{37}$$

where $\tilde{c}_{i,k}$ is real. If $A_{i,*}$ and $A_{k,*}$ are perpendicular, then we can choose $\tilde{c}_{i,k} = 0$. Thus we use the form

$$\tilde{c}_{i,k} = A^T_{k,*} A_{i,*} c_{i,k} \tag{38}$$

and Eq. (37) becomes

$$X A_{i,*} = \sum_k c_{i,k} A^T_{k,*} A_{i,*} A_{k,*} \tag{39}$$

$$= \underbrace{\sum_k c_{i,k} A_{k,*} A^T_{k,*}}_{X} A_{i,*}, \tag{40}$$

from which we can read X. This has to be the same X for every equation in the system of equations (35), i.e. $c_{i,k} = c_k$. We have

$$X = \sum_{k=1}^{M_1+M_2} c_k A_{k,*} A^T_{k,*} \tag{41}$$

$$= A^T \operatorname{diag}(c_1, ..., c_{M_1+M_2}) A. \tag{42}$$

Inserting this into Eq. (35) gives for all i

$$1 = (AXA^T)_{ii} \tag{43}$$

$$= (P \operatorname{diag}(c_1, ..., c_{M_1+M_2}) P)_{ii} \tag{44}$$

$$= \sum_{k=1}^{M_1+M_2} c_k P^2_{ik}. \tag{45}$$

Here we introduced the projector $P = AA^T$. We also introduce the matrix Q, which is P componentwise squared, i.e. $Q_{ij} = P^2_{ij}$, and the vector $\vec{1}$, where every component is one. Then Eq. (45) can be written as

$$Q\vec{c} = \vec{1} \tag{46}$$

This equation is solvable if and only if

$$\vec{1} = QQ^- \vec{1}, \tag{47}$$

where Q^- is the pseudoinverse of Q. Then all solutions to this equation are given by

$$\vec{c} = \underbrace{Q^- \vec{1}}_{\vec{c}_0} + \underbrace{(\mathbb{1} - Q^- Q)\vec{y}}_{\vec{c}_y}, \tag{48}$$

with $\vec{y} \in \mathbb{R}^{M_1+M_2}$. Here we marked the y-independent and y-dependent part of $\vec{c}$. Inserting into Eq. (42) gives a y-independent part and a y-dependent part of X, i.e.

$$X = X_0 + X_y. \tag{49}$$

The vector $\vec{c}_y = (\mathbb{1} - Q^- Q)\vec{y}$ lies in the kernel of Q. Therefore for all $i \leq M_1 + M_2$

$$0 = \sum_{k=1}^{M_1+M_2} Q_{ik}(c_y)_k \tag{50}$$

$$= \sum_{l_1,l_2=1}^{d} A_{il_1} A_{il_2} \underbrace{\sum_{k=1}^{M_1+M_2} A_{kl_1} A_{kl_2} (c_y)_k}_{(X_y)_{l_1,l_2}} \tag{51}$$

$$= A^T_{i,*} X_y A_{i,*}. \tag{52}$$

This implies that $X_y = 0$ and thus $X = X_0$ is uniquely defined by Eq. (35) and Eq. (38). We obtain a solution α with $\alpha\alpha^T = X$ via

$$\alpha = \sqrt{X}. \tag{53}$$

It is possible, that X is not semipositive, in which case there is no real solution α.
The described algorithm contains a singular value decomposition, the calculation of a pseudoinverse and a square root of a matrix, as well as several matrix multiplications. The runtime complexities of all of these operations are asymptotically upper bounded by the matrix dimension to the power of three [1]. Therefore the runtime complexity of this algorithm is $\mathcal{O}((M_1 + M_2)^3)$.
A summarized pseudo code version of the described algorithm follows.

procedure AlphaMatrix(g)
  $(V, S, W) \leftarrow \mathrm{SVD}(g)$ ▷ singular value decomposition of g
  $d \leftarrow \max_{i:S_{ii}=S_{11}} i$ ▷ degeneracy of maximal singular value
  $V^d \leftarrow V$ with columns $d+1$ to M_1 dropped ▷ truncated SVD
  $W^d \leftarrow W$ with columns $d+1$ to M_2 dropped
  $A \leftarrow \begin{pmatrix} V^d \\ \sqrt{\frac{M_2}{M_1}} W^d \end{pmatrix}$ ▷ the set of vectors on ellipsoid
  $P \leftarrow AA^T$
  for all $i, j \in \{1, 2, ..., M_1 + M_2\}$ **do**
    $Q_{i,j} \leftarrow P^2_{i,j}$
  end for
  $\vec{c} \leftarrow Q^- \vec{1}$ ▷ apply pseudoinverse
  if $Q\vec{c} = \vec{1}$ **then** ▷ solution exists
    $X \leftarrow A^T \,\mathrm{diag}\,(\vec{c}) A$
    $\alpha \leftarrow \sqrt{X}$
    if $\mathrm{Im}(\alpha)$=0 **then**
      return α
    else ▷ X is not semipositive
      return 0 ▷ only complex solutions
    end if
  else
    return 0 ▷ equation not solvable
  end if
end procedure

C. A COLLECTION OF INSTRUCTIVE EXAMPLES

This section contains more examples.

Example 5 (CHSH inequality)**.** The original Clauser-Horne-Shimony-Holt(CHSH) inequality [2] is given by

$$g = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{54}$$

As g is symmetric, the singular values are given by the absolute values of it's eigenvalues, which is $\sqrt{2}$. Since all singular values are equal, the bound in Ineq. (5) is tight (Corollary 2, see also Fig. 4(a)). It is the well-known upper bound of $T = Q = 2\sqrt{2}$ for the quantum value of the CHSH-inequality derived by Tsirelson [3].

Example 6. Consider the coefficients

$$g = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \tag{55}$$

where the bound gives $T = 1 + \sqrt{5}$, but obviously only 3 can be reached in any theory. Therefore the bound is not tight for this instance of g.

Example 7 (Binary digits)**.** In Ref. [4] a bipartite Bell inequality given by coefficients

$$g_{x_1,x_2} = 1 - 2(\lfloor 2^{1-x_2}(x_1 - 1)\rfloor \bmod 2) \tag{56}$$

is discussed, which resembles a list of binary numbers. The number of measurement settings is given by $M_1 = 2^{M_2-1}$. It can be used to witness observables referring to $d = M_2$ dimensional real vectors. Thus the number of measurement settings $M_1 + M_2$ is $\mathcal{O}(2^d)$. Bounds on the value of the Bell inequality are given in the reference.
It can be shown, that all singular values of g are equal to $\sqrt{M_1} = \sqrt{2^{M_2-1}}$. A singular value decomposition of g then is

$$g = \underbrace{\frac{1}{\sqrt{M_1}}}_{V} g \underbrace{\sqrt{M_1}\mathbb{1}^{M_2}}_{S} \underbrace{\mathbb{1}^{M_2}}_{W^T}. \tag{57}$$

From this the diagonal solution $\alpha_i = \sqrt{M_1}M_2$ can be read. This implies, that the bound $T = M_1\sqrt{M_2}$ is tight.

Example 8 (Braunstein-Caves inequalities)**.** The Braunstein-Caves inequalities [5] are given by

$$g_{x_1,x_2} = \begin{cases} 1 & \text{if } 0 \le x_1 - x_2 \le 1 \\ -1 & \text{if } x_1 = 1 \text{ and } x_2 = M \\ 0 & \text{else} \end{cases}, \tag{58}$$

where $M = M_1 = M_2$. It can be shown that the maximal singular value of g is $2\cos(\pi/(2M))$ and twofold degenerate. The bound reads $T = 2M\cos(\pi/(2M))$, which is achievable [5, 6]. See also Fig. 4(b).

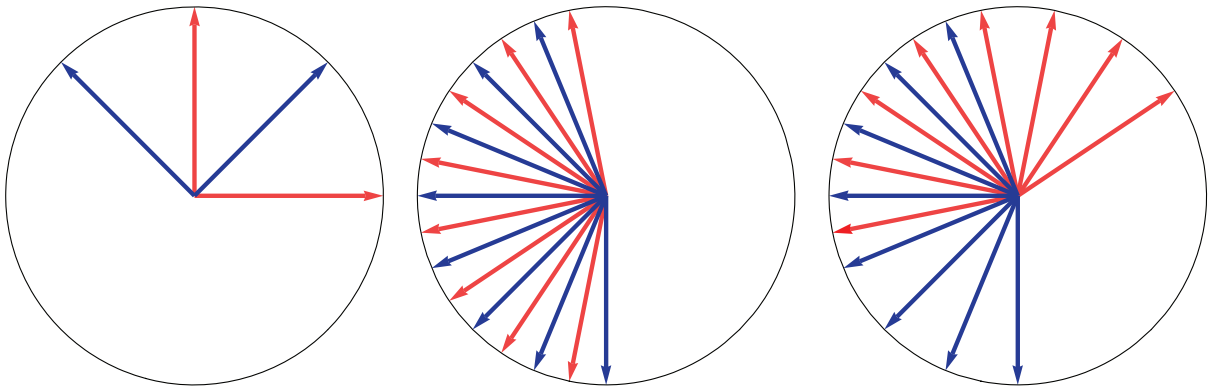
Example 9 (Greater Equal Function)**.** The greater-equal-function is related to a Bell inequality with coefficients

$$g_{x_1,x_2} = \begin{cases} 1 & \text{if } x_1 \ge x_2 \\ -1 & \text{else} \end{cases}, \tag{59}$$

where $1 \le x_1, x_2 \le M_1 = M_2 = M$ [7]. The maximal singular value of g, $\csc(\pi/(2M))$, is twofold degenerate. The quantum bound $T = M\csc(\pi/(2M)$ is tight (Corollary 1, see also Fig. 4(c)) and strictly larger than the local hidden variable bound $B = \lceil M^2/2\rceil$. The violation Q/B in the limit of large M is $4/\pi$ [7].

Example 10 (Fishburn-Reeds)**.** The highest violation of an explicit bipartite correlation type Bell inequality known to the authors is given by Fishburn and Reeds in [8]. They describe a series of Bell inequalities, which is constructed as follows. Construct a $k(k-1)\times k$-matrix F_k, which rows constitute all vectors of the form $(0, ..., 0, -1, 0, ..., 0, 1, 0, ..., 0)$ and $(0, ..., 0, 1, 0, ..., 0, 1, 0, ..., 0)$. The Bell inequality is given by coefficients

$$g = F_k F_k^T - \frac{4}{3}\mathbb{1}. \tag{60}$$



(a)CHSH Inequality (Ex. 5) (b)BC Inequality (Ex. 8) (c)Gisin's Inequality (Ex. 9)

FIG. 4. If and only if the bound is tight, the vectors $V^d_{i,*}$ (blue) and $\sqrt{\frac{M_2}{M_1}}W^d_{j,*}$ (red) lie on the surface of an origin-centered Ellipsoid.

By construction, $g' = F_k F_k^T$ fulfills the conditions of Corollary 1. The diagonal modification changes the singular values, without changing their order. Therefore also g fulfills the conditions of Corollary 1. Because the maximal singular value is $2(k-1)-4/3$, the maximal quantum value is $Q = T = (2(k-1)-4/3)k(k-1)$, which is the value derived in the reference. The first k for which $Q/B > \sqrt{2}$ is $k = 5$, where $Q/B = \frac{10}{7} \approx 1.42857$. For $k = 5$, the explicit form of g is

$$g = \begin{pmatrix}
\frac{2}{3} & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\
1 & \frac{2}{3} & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & -1 & 0 & 0 & 1 & 1 & 0 \\
1 & 1 & \frac{2}{3} & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & -1 & 0 & -1 & 0 & 1 \\
1 & 1 & 1 & \frac{2}{3} & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & -1 & 0 & -1 & -1 \\
1 & 1 & 0 & 0 & \frac{2}{3} & 1 & 1 & 1 & 1 & 0 & -1 & -1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\
1 & 0 & 1 & 0 & 1 & \frac{2}{3} & 1 & 1 & 0 & 1 & -1 & 0 & -1 & 0 & 1 & 0 & 1 & -1 & 0 & 1 \\
1 & 0 & 0 & 1 & 1 & 1 & \frac{2}{3} & 0 & 1 & 1 & -1 & 0 & 0 & -1 & 1 & 1 & 0 & 0 & -1 & -1 \\
0 & 1 & 1 & 0 & 1 & 1 & 0 & \frac{2}{3} & 1 & 1 & 0 & -1 & -1 & 0 & -1 & -1 & 0 & 0 & 1 & 1 \\
0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & \frac{2}{3} & 1 & 0 & -1 & 0 & -1 & -1 & 0 & -1 & 1 & 0 & -1 \\
0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & \frac{2}{3} & 0 & 0 & -1 & -1 & 0 & -1 & -1 & -1 & -1 & 0 \\
0 & 1 & 1 & 1 & -1 & -1 & -1 & 0 & 0 & 0 & \frac{2}{3} & 1 & 1 & 1 & -1 & -1 & -1 & 0 & 0 & 0 \\
1 & 0 & 1 & 1 & -1 & 0 & 0 & -1 & -1 & 0 & 1 & \frac{2}{3} & 1 & 1 & 1 & 0 & 0 & -1 & -1 & 0 \\
1 & 1 & 0 & 1 & 0 & -1 & 0 & -1 & 0 & -1 & 1 & 1 & \frac{2}{3} & 1 & 0 & 1 & 0 & 1 & 0 & -1 \\
1 & 1 & 1 & 0 & 0 & 0 & -1 & 0 & -1 & -1 & 1 & 1 & 1 & \frac{2}{3} & 0 & 0 & 1 & 0 & 1 & 1 \\
1 & -1 & 0 & 0 & 0 & 1 & 1 & -1 & -1 & 0 & -1 & 1 & 0 & 0 & \frac{2}{3} & 1 & 1 & -1 & -1 & 0 \\
1 & 0 & -1 & 0 & 1 & 0 & 1 & -1 & 0 & -1 & -1 & 0 & 1 & 0 & 1 & \frac{2}{3} & 1 & 1 & 0 & -1 \\
1 & 0 & 0 & -1 & 1 & 1 & 0 & 0 & -1 & -1 & -1 & 0 & 0 & 1 & 1 & 1 & \frac{2}{3} & 0 & 1 & 1 \\
0 & 1 & -1 & 0 & 1 & -1 & 0 & 0 & 1 & -1 & 0 & -1 & 1 & 0 & -1 & 1 & 0 & \frac{2}{3} & 1 & -1 \\
0 & 1 & 0 & -1 & 1 & 0 & -1 & 1 & 0 & -1 & 0 & -1 & 0 & 1 & -1 & 0 & 1 & 1 & \frac{2}{3} & 1 \\
0 & 0 & 1 & -1 & 0 & 1 & -1 & 1 & -1 & 0 & 0 & 0 & -1 & 1 & 0 & -1 & 1 & -1 & 1 & \frac{2}{3}
\end{pmatrix}. \tag{61}$$

[1] Gene H. Golub and Charles F. Van Loan. *Matrix Computations*. The Johns Hopkins University Press, Baltimore, 4th edition, 2013.

[2] JF Clauser, MA Horne, A Shimony, and RA Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23(15):880–884, 1969.

[3] BS Tsirelson. Quantum generalizations of Bell's inequality. *Lett. Math. Phys.*, 4:93–100, 1980.

[4] T Vértesi and KF Pál. Generalized Clauser-Horne-Shimony-Holt inequalities maximally violated by higher-dimensional systems. *Phys. Rev. A*, 77:042106, 2008.

[5] SL Braunstein and CM Caves. Wringing out better Bell inequalities. *Ann. Phys.-NY*, 202(1):22–56, 1990.

[6] Adán Cabello, Jan-Åke Larsson, and David Rodríguez. Minimum detection efficiency required for a loophole-free violation of the Braunstein-Caves chained Bell inequalities. *Phys. Rev. A*, 79, Jun 2009.

[7] N Gisin. Bell inequality for arbitrary many settings of the analyzers. *Phys. Lett. A*, 260(September):8–10, 1999.
[8] PC Fishburn and JA Reeds. Bell inequalities, Grothendieck's constant, and root two. *SIAM J. Discrete Math.*, 7(1):48–56, 1994.

D

Optimization of Bell inequalities with invariant Tsirelson bound

Title:	Optimization of Bell inequalities with invariant Tsirelson bound
Authors:	M.E., Hermann Kampermann, and Dagmar Bruß
Journal:	Journal of Physics A: Mathematical and Theoretical
Impact factor:	1.583
Date of submission:	3 February 2014
Publication status:	Published
Contribution by M.E.:	First author (input approx. 80%)
Results:	Description of all manipulations that leave the singular value based Tsirelson bound invariant. Application of these operations to Bell Experiments without common alignment and optimization of Bell inequalities w.r.t. the violation.

Optimization of Bell inequalities with invariant Tsirelson bound

IOP Publishing Journal of Physics A: Mathematical and Theoretical
J. Phys. A: Math. Theor. **47** (2014) 424015 (10pp) doi:10.1088/1751-8113/47/42/424015

Optimization of Bell inequalities with invariant Tsirelson bound

M Epping, H Kampermann and D Bruß

Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, Universitätsstrasse 1, D-40225 Düsseldorf, Germany

E-mail: epping@hhu.de

Received 3 February 2014, revised 1 April 2014
Accepted for publication 1 April 2014
Published 8 October 2014

Abstract

We consider a subclass of bipartite CHSH-type Bell inequalities. We investigate operations which leave their Tsirelson bound invariant, but change their classical bound. The optimal observables are unaffected except for a relative rotation of the two laboratories. We illustrate the utility of these operations by giving explicit examples. We prove that, for a fixed quantum state and fixed measurement setup except for a relative rotation of the two laboratories, there is a Bell inequality that is maximally violated for this rotation, and we optimize some Bell inequalities with respect to the maximal violation. Finally, we optimize the qutrit to qubit ratio of some dimension witnessing Bell inequalities.

This article is part of a special issue of *Journal of Physics A: Mathematical and Theoretical* devoted to '50 years of Bell's theorem'.

Keywords: Bell inequality, Tsirelson bound, optimization of violation
PACS number: 03.65.Ud

S Online supplementary data available from stacks.iop.org/JPhysA/47/424015/mmedia

(Some figures may appear in colour only in the online journal)

1. Introduction

Originally, John S Bell introduced what we now call Bell inequalities in order to show that the ideas of locality and realism are incompatible with statistical predictions of quantum theory [1]. Thus, the question whether a completion of quantum theory obeying these axioms exists, as proposed by Einstein *et al* [2], was brought to an experimentally testable level. Now, 50 years later, there is very strong experimental evidence that Bell inequalities can be violated by nature [3–10], which implies that not all axioms in the derivation of Bell inequalities are followed by nature. Nevertheless Bell inequalities are not water under the bridge yet. This is amongst other reasons due to several interesting applications, like quantum key distribution, where the

violation of Bell inequalities is a test for eavesdropping [11]. Here and in other applications, the amount of violation becomes important and a stronger violation of the inequality is usually beneficial (e.g. noise is less corruptive or the gap between classical and quantum performance increases).

In the present paper, we discuss two methods to modify Bell inequalities, which change the classical bound but leave the maximal value achievable in quantum theory unchanged. These methods can be used to optimize Bell inequalities with respect to the possible amount of violation. Various research on Bell inequalities with a large amount of violation has been carried out [12–15], but literature on the specific problem investigated in this paper is less extensive [16, 17].

We specify the Bell inequalities under consideration in the following section 2. Then we formulate the above-mentioned methods as a corollary in section 3 and give examples for their utility in section 4. Section 5 concludes this paper.

2. A subclass of CHSH-type Bell inequalities

We consider bipartite full correlation Bell inequalities (CHSH-type Bell inequalities [18, 19]) with M_i measurement settings at the site of party i. These settings are labelled $x_i = 1, 2, \ldots, M_i$. Such Bell inequalities can be written in the form

$$\sum_{x_1,x_2=1}^{M_1,M_2} g_{x_1,x_2} E(x_1, x_2) \leqslant B, \tag{1}$$

where $E(x_1, x_2)$ is the expectation value for setting x_1 at Alice's site and x_2 at Bob's site and g is a real $M_1 \times M_2$-matrix of coefficients. Measurement outcomes are required to be in the interval $[-1, 1]$. The local hidden variable bound B holds for all values achievable in local hidden variable theories, i.e.

$$\max_{a_1,a_2} \sum_{x_1,x_2=1}^{M_1,M_2} g_{x_1,x_2} a_1(x_1) a_2(x_2) \leqslant B. \tag{2}$$

B can be calculated by performing this maximization over all possible (deterministically) predefined measurement outcomes $a_1(x_1) = \pm 1$ and $a_2(x_2) = \pm 1$. Due to the assumption of locality, a_1 (a_2) does not depend on x_2 (x_1). The use of unmeasured outcomes is motivated by the assumption of realism. See [20] for a more thorough analysis. For some g, inequality (2) can be violated within quantum theory.

Similarly, one can write down bounds for expectation values predicted by quantum theory [21]. The analogue of inequality (1) reads

$$\sum_{x_1,x_2=1}^{M_1,M_2} g_{x_1,x_2} E(x_1, x_2) \leqslant T, \tag{3}$$

where T is a Tsirelson bound, which holds for all quantum states given by a density matrix ρ and all observables $\mathcal{A}_1(x_1)$ and $\mathcal{A}_2(x_2)$, i.e.

$$\max_{\mathcal{A}_1,\mathcal{A}_2,\rho} \sum_{x_1,x_2=1}^{M_1,M_2} g_{x_1,x_2} \operatorname{tr}(\rho \mathcal{A}_1(x_1) \otimes \mathcal{A}_2(x_2)) \leqslant T. \tag{4}$$

We do not restrict the dimension of the Hilbert space. In [22] we showed that a quantum bound for inequality (3) is given by

$$T(g) = ||g||_2 \sqrt{M_1 M_2}, \tag{5}$$

where $||g||_2$ is the largest singular value of g. However, this bound T is not always tight. It is not always possible to achieve equality in inequality (4). Nevertheless it is tight for a subclass of Bell inequalities, which contains many well-known Bell inequalities. In this paper we will restrict ourselves to this class of Bell inequalities, for which T in equation (5) is achievable for some states and observables. In this case the violation of the Bell inequality, which is the ratio of the quantum and the classical value, is

$$v = \frac{T}{B}. \tag{6}$$

According to a theorem by Tsirelson [23], there exist real vectors $\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_{M_1}$ and $\vec{w}_1, \vec{w}_2, \ldots, \vec{w}_{M_2}$, such that the quantum mechanical expectation value can be written as

$$E(x_1, x_2) = \vec{v}_{x_1}^T \vec{w}_{x_2}. \tag{7}$$

In the present context, it is usually more convenient to use these vectors instead of the observables. Let g be a real $M_1 \times M_2$-matrix and V, S, W be a singular value decomposition of g, i.e. $g = VSW^T$ with diagonal S and V, W being orthogonal. We denote the dimension of the space of the largest singular value $||g||_2$ as d, i.e. this is the degeneracy of the largest singular value. The corresponding matrices of the truncated singular value decomposition associated with $||g||_2$ contain the first d columns (the singular vectors) of V and W, respectively.

Theorem 1 (Tightness of T [22])**.** *For any real $M_1 \times M_2$-matrix g, let V^d, $||g||_2 \mathbb{1}^d$, W^d be a truncated singular value decomposition of g associated with $||g||_2$, where d is the degeneracy of $||g||_2$. The bound $T = ||g||_2\sqrt{M_1 M_2}$ can be reached with observables, which are linked via $E(i, j) = \vec{v}_i^T \vec{w}_j$ to $d' \leqslant d$-dimensional real vectors $\vec{v}_i$ and $\vec{w}_j$ given by*

$$\vec{v}_i = \alpha^T V^d_{i,*} \tag{8}$$

and

$$\vec{w}_j = \sqrt{\frac{M_2}{M_1}}\alpha^T W^d_{j,*}, \tag{9}$$

if and only if there exists a $d \times d'$-matrix α, such that these vectors are normalized. Here $V^d_{i,*}$ and $W^d_{j,*}$ denote column vectors containing the elements of the ith row of V^d and the jth row of W^d, respectively.

There is a geometric interpretation of the norm conditions: the bound T is tight for observables corresponding to d'-dimensional real vectors $\vec{v}_i$ and $\vec{w}_j$ if and only if the vectors $V^d_{i,*}$ and $\sqrt{\frac{M_2}{M_1}}W^d_{j,*}$ lie on the surface of an origin-centred ellipsoid with no more than d' finite semi-axes [22]. We call this object a d'-dimensional ellipsoid.

3. Modifying Bell inequalities inside this class

We aim at modifying Bell inequalities inside the class described in the previous section, i.e. those where the quantum bound given in equation (5) is tight. In particular, we are interested in operations that do not change the value of T given in equation (5). However, in general these operations do change the classical bound of the Bell inequality, i.e. the modification's effect on the quantum and the classical value are qualitatively and quantitatively different. This is in contrast to arbitrary modifications of the coefficients, where both values are simultaneously affected. We will exemplify later that such modifications can be a useful tool, e.g. for optimizing Bell inequalities. The following corollary gives modifications with the properties we are seeking.

Corollary 1. *Let g be a $M_1 \times M_2$ real matrix with singular value decomposition V, S, W, i.e. $g = VSW^T$, such that $T(g)$ is achievable. The multiplicity of $||g||_2$ is denoted by d, the length of the diagonal of S is $s = \min(M_1, M_2)$. The following modifications of g lead to achievable bounds $T(g')$ (primed symbols correspond to the modified coefficients g').*

(i) 'Twisting' of singular vectors.
For

$$g' = V \begin{pmatrix} R_1 & 0 \\ 0 & R_2 \end{pmatrix} S \begin{pmatrix} \mathbb{1}^d & 0 \\ 0 & R_3 \end{pmatrix} W^T, \tag{10}$$

where R_1 is a $d \times d$ orthogonal matrix commuting with α (see equation (8)) and R_2 and R_3 are orthogonal matrices of dimension $(M_1 - d)$ and $(M_2 - d)$, respectively, $T(g') = T(g)$ is achievable.

(ii) Modification of singular values.
For real numbers $\lambda_1, \lambda_{d+1}, \lambda_{d+2}, \ldots, \lambda_s$ fulfilling

$$|\lambda_i + S_{i,i}| < |\,||g||_2 + \lambda_1| \quad \text{for all} \quad i > d \tag{11}$$

the modified coefficients $g' = VS'W^T$ with

$$S' = diag(S_{1,1} + \lambda_1, \ldots, S_{d,d} + \lambda_1, S_{d+1,d+1} + \lambda_{d+1}, \ldots, S_{s,s} + \lambda_s) \tag{12}$$

correspond to an inequality with achievable $T(g') = \frac{||g||_2 + \lambda_1}{||g||_2} T(g)$.

Proof.

(i) R_1 can be considered as a rotation of the singular vectors, i.e. the singular values in S are not affected. If R_1 and the $d \times d$-matrix α commute, then

$$\left|\left|\alpha^T \left(R_1^T V_{i,*}^d\right)\right|\right| = \left|\left|R_1^T \alpha^T V_{i,*}^d\right|\right| = \left|\left|\alpha^T V_{i,*}^d\right|\right|, \tag{13}$$

i.e. the conditions of theorem 1 are not affected. R_2 and R_3 merely rotate the singular vectors outside the space associated with $||g||_2$, which neither affects the tightness nor the value of the bound.

(ii) The conditions for tightness according to theorem 1 and the value of T are not affected by modification of non-maximal singular values, as long as they do not become maximal. Adding the same value to all largest singular values is only a scaling of T (as long as they remain maximal). A negative diagonal entry induces a sign change of the elements of the corresponding singular vector. □

Please note that the condition of (i) is fulfilled if there exists a solution $\alpha \propto \mathbb{1}$.

We remark that (ii) is a generalization of the diagonal modification in [16]. There, $V = W$ and $g' = g + \lambda \mathbb{1}$, which corresponds to $\lambda_i = \lambda$. The condition of equation (11) on the λ_i can be ignored, if one assures tightness according to theorem 1. For example, depending on the particular form of V and W, the bound might be tight for different values of d. In particular, T is tight, if the new singular values are all equal. Furthermore (ii) includes the special case, where $g' = rg$ for any $r \in \mathbb{R}$.

4. Using these modifications as a method

In this section, the modifications described in corollary 1 are applied to specific examples of coefficient matrices g.

4.1. Maximally violated Bell inequality for relative rotation of laboratories

We start with the modification (i), i.e. the twisting of the singular vectors. First we note that R_1 is a relative rotation of the two parties in the sense, that the real vectors $\vec{v}_{x_1}$, which define optimal observables for party one, are rotated by R_1. For $d' = 3$, one can interpret $\vec{v}_{x_1}$ as a Bloch-vector, i.e. $\mathcal{A}(x_1) = \vec{v}_{x_1}^T \vec{\sigma}$, where $\vec{\sigma}$ denotes the vector containing the three Pauli matrices. In this way we see that the rotation R_1 corresponds to a relative rotation of the two laboratories in the usual sense.

This motivates us to prove the following statement.

Example 1. For every relative rotation between the laboratories of party one and party two, there exists a Bell inequality that is maximally violated for exactly this rotation. We require that the experimental setup is fixed up to the relative rotation, i.e. the measurement directions in the local coordinate systems and the shared state (e.g. $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$) do not depend on the rotation angle. Consider the Bell inequalities given via the coefficient matrix

$$g = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & 0 \\ -\frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} \end{pmatrix} R(\Phi, \Theta, \Psi), \tag{14}$$

where

$$\begin{aligned} R(\Phi, \Theta, \Psi) = & \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(\Phi) & \sin(\Phi) \\ 0 & -\sin(\Phi) & \cos(\Phi) \end{pmatrix} \\ & \times \begin{pmatrix} \cos(\Theta) & 0 & -\sin(\Theta) \\ 0 & 1 & 0 \\ \sin(\Theta) & 0 & \cos(\Theta) \end{pmatrix} \begin{pmatrix} \cos(\Psi) & \sin(\Psi) & 0 \\ -\sin(\Psi) & \cos(\Psi) & 0 \\ 0 & 0 & 1 \end{pmatrix} \end{aligned} \tag{15}$$

is a general rotation given by the roll-pitch-yaw angle. From equation (14) one can read the truncated singular value decomposition associated with the threefold ($d = 3$) degenerate maximal singular value 1: i.e. the first factor is V^d, $S^d = \mathbb{1}$ and $W^T = R(\Phi, \Theta, \Psi)$. From this we already know that $T(g) = \sqrt{M_1 M_2} = 3\sqrt{2}$ for all angles. This bound is achievable, because $\alpha = \sqrt{2}\mathbb{1}^3$ is a solution (see theorem 1). The vectors $V^d_{1,*}$, $V^d_{2,*}$, $V^d_{4,*}$, $V^d_{5,*}$ force the rank of α to be at least two (two or more semi-axes of the corresponding ellipsoid are finite). Therefore, the inequality associated with g is really a Bell inequality, i.e. it can be violated. The bound is achieved for the state $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ with observables

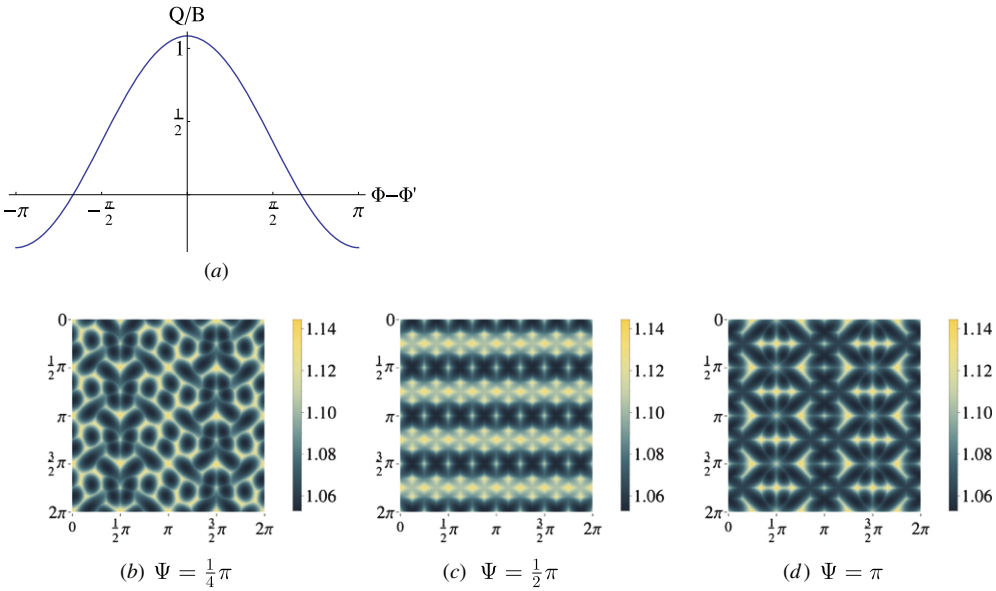
$$\mathcal{A}(x_1) = \vec{v}_{x_1}^T \vec{\sigma}, \tag{16}$$

$$\mathcal{A}(x_2) = \left(\vec{w}_{x_2}^T \vec{\sigma}\right)^T. \tag{17}$$

Because

$$\vec{w}_j = \sqrt{\frac{M_2}{M_1}} \alpha^T W^d_{j,*} = R(\Phi, \Theta, \Psi)_{j,*}, \tag{18}$$

i.e. the measurement directions of party two are given by the columns of $R^T(\Phi, \Theta, \Psi)$, this Bell inequality is maximally violated for a relative rotation of the laboratories given by the roll-pitch-yaw angle (see figure 1(*a*)). The violation $\frac{T}{B}$ of the inequality given by the coefficients in equation (14) depends on the angles (see figure 1(*b*)–(*d*)).



(*a*)

(*b*) $\Psi = \frac{1}{4}\pi$ (*c*) $\Psi = \frac{1}{2}\pi$ (*d*) $\Psi = \pi$

Figure 1. Violation of the 'rotated' Bell inequality (equation (14)). (*a*) The measured violation (quantum value Q for actual observables divided by local hidden variable value B) of the Bell inequality with coefficients given in equation (14) for optimal angles (Φ, Θ, Ψ) depending on the yaw angle Φ' of the actual observables. Φ, Θ and Ψ are fixed to arbitrary values. The same plot can be drawn for Θ and Ψ. (*b*)–(*d*) The maximal violation of Bell inequalities given by different angles, see equation (14), where Ψ is fixed.

4.2. Optimization of Bell inequalities for fixed measurement directions

In several applications a large violation is desirable. Given the experimental measurement setup used to evaluate a given Bell inequality, there might be different inequalities that lead to a higher violation. In that sense, they are 'better' inequalities. Finding an optimal inequality seems to be a difficult task. In some cases the methods above (corollary 1 (i) and (ii)) might give an intuition how to improve a given matrix of coefficients g without changing the involved measurements.

There is another possible motivation for restricting the observables in the optimization of the violation: it turns out that the average violation of Bell inequalities inside this restricted parameter space is larger than the one for the whole parameter space. Figure 2 shows the probability of an amount of violation for completely random coefficients and rotated versions (corollary 1 (i)) of

$$g = \begin{pmatrix} 1 & -1 & -1 \\ 1 & 1 & -1 \\ 1 & 1 & 1 \end{pmatrix}. \tag{19}$$

Example 2. The coefficients of Gisin's inequality [24] for $M_1 = M_2 = 6$ read

$$g = \begin{pmatrix} 1 & -1 & -1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 & -1 & -1 \\ 1 & 1 & 1 & 1 & 1 & -1 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}. \tag{20}$$

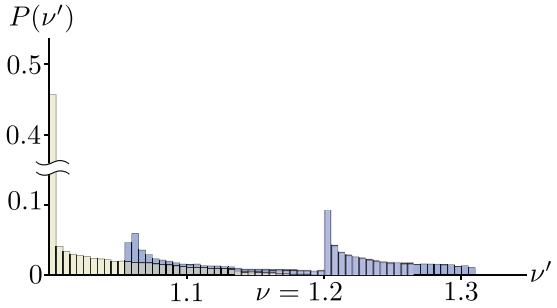


Figure 2. A histogram of the maximal violation ν' of a random Bell inequality (light) and a 'twisted' version of Gisin's inequality [24] (dark). The size of the matrices is 3×3. The random inequality has equally distributed coefficients in $[-1, 1]$. For the other inequality, the rotation angles are equally distributed. The probability of a given violation is estimated from samples of 50 000 inequalities each. The violation of the original inequality by Gisin is $\nu = 1.2$.

This inequality has $B = 18$, as one can easily see when the first two rows get multiplied with -1. The quantum value is $T = M/\sin(\pi/(2M)) = 12\sqrt{2+\sqrt{3}} \approx 23.1822$. Using corollary 1 (ii) we can optimize the coefficients numerically, and obtain

$$\begin{aligned} g' &= V\,\mathrm{diag}\,(||g||_2, ||g||_2, ||g||_2, ||g||_2, -||g||_2, -||g||_2)W^T \\ &= (1+\sqrt{3}) \begin{pmatrix} 0 & 0 & -1 & 0 & 0 & -1 \\ 1 & 0 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & -1 & 0 \\ 0 & 0 & 1 & 0 & 0 & -1 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}, \end{aligned} \tag{21}$$

which is equivalent to the CHSH inequality. This implies a violation of $\nu' = \sqrt{2}$ and $B(g') = 6(1+\sqrt{3}) \approx 16.3923$. Here we ignored the condition in equation (11) of corollary 1 (ii) as tightness of T is ensured by the fact that all singular values are equal. One would obtain the same result, when considering $g' = V\,\mathrm{diag}\,(||g||_2, ||g||_2, ||g||_2 - \varepsilon, ||g||_2 - \varepsilon, -||g||_2 + \varepsilon, -||g||_2 + \varepsilon)W^T$ for a very small positive ε. In this way the degeneracy remains $d' = 2$ and the condition of equation (11) is fulfilled. The matrix g' constitutes a local optimum, i.e. small modifications of the singular values lead to a smaller violation.

Example 3 (Fishburn–Reeds inequalities [16])**.** In [16], the authors construct a series of inequalities with increasing number of measurement settings. For $d \in \mathbb{N}$ greater or equal two,

$$g = V^d (V^d)^T - \tfrac{4}{3}\mathbb{1}, \tag{22}$$

where V^d is a $(d-1)d \times d$-matrix containing all rows of the form $(0, \ldots, 0, -1, 0, \ldots, 0, 1, 0, \ldots, 0)$ and $(0, \ldots, 0, 1, 0, \ldots, 0, 1, 0, \ldots, 0)$. The columns of V^d are orthogonal and thus $\frac{1}{\sqrt{2(d-1)}}V^d$, $(2(d-1) - 4/3)\mathbb{1}^d$ and $\frac{1}{\sqrt{2(d-1)}}V^d$ form a truncated singular value decomposition of g. Therefore, the optimal measurement settings for party one and party two are identical. Intuitively, this choice of settings seems to be not optimal with respect to the amount of violation. We searched numerically for inequalities with a larger violation using methods (i) and (ii) of corollary 1. We give improved violations for $d = 2, \ldots, 5$ in table 1. Due to the computational complexity of determining B, it is likely that the given values are not the maximal ones achievable with these methods.

Table 1. Optimized violations of the first four inequalities by Fishburn and Reeds [16], T/B', compared to the original violation T/B. The explicit coefficients of the corresponding matrix g' are given in the supplemental material (available at stacks.iop.org/JPhysA/47/424015/mmedia). Note that the given values for ν' are not necessarily maximal.

d	$\nu = T/B$	$\nu' = T/B'$
2	1	$\sqrt{2} \approx 1.414\,21$
3	$4/3 \approx 1.333\,33$	$1.341\,63$
4	$7/5 = 1.4$	$\sqrt{2} \approx 1.414\,21$
5	$10/7 \approx 1.428\,57$	$1.428\,60$

4.3. Optimization of dimension witnessing Bell inequalities

The minimal d' for a solution α is a lower bound on the length of the vectors $\vec{v}_i$ and $\vec{w}_j$, which is linked to the dimension of the observables. For example, if this minimal d' is larger than three, the maximal quantum value of the inequality cannot be reached using qubits. Let us denote the bound for d'-dimensional real vectors by $T_{d'}$. Please note that $B = T_1$.

In the previous section, we aimed at increasing the ratio T/T_1 by decreasing T_1. The same optimizations can be performed for any other value d' with $T_{d'} < T$.

To calculate the bound $T_{d'}$, we are interested in the optimal strategy (optimal 'observables') achieving this bound. We note that the optimal observables of party two are fixed by the ones of party one. The maximum in equation (4) using equation (7) is achieved, if for all x_2 (each column), the vector $\vec{w}_{x_2}$ is parallel to $\sum_{x_1} g_{x_1,x_2}\vec{v}_{x_1}$, i.e.

$$\vec{w}_{x_2} = \frac{1}{||\sum g_{x_1,x_2}\vec{v}_{x_1}||}\sum g_{x_1,x_2}\vec{v}_{x_1}, \tag{23}$$

so the bound simplifies to

$$T_{d'}(g) = \max_{\vec{v}_{x_1}\in\mathbb{R}^{d'},||\vec{v}_{x_1}||=1}\sum_{x_2=1}^{M_2}\left|\left|\sum_{x_1=1}^{M_1} g_{x_1,x_2}\vec{v}_{x_1}\right|\right|. \tag{24}$$

As $T_{d'}(g) = T_{d'}(g^T)$, we can assume that $M_1 \leqslant M_2$ without loss of generality. We give an example for such optimizations.

Example 4. We optimize inequality $D6_1$ in [25]. It is the skew left circulant matrix given by the first row $(1 \quad 0 \quad 1 \quad 0 \quad 1 \quad 1)$, i.e.

$$D6_1 = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & -1 \\ 1 & 0 & 1 & 1 & -1 & 0 \\ 0 & 1 & 1 & -1 & 0 & -1 \\ 1 & 1 & -1 & 0 & -1 & 0 \\ 1 & -1 & 0 & -1 & 0 & -1 \end{pmatrix}. \tag{25}$$

A solution α of theorem 1 is $\alpha = \sqrt{\frac{M}{d}}\mathbb{1}^d$, as it is the case for many circulant (left, right, skew left, skew right) matrices. See [26] for the singular value decomposition of circulant matrices. This Bell inequality has $T_2 = T_3 = T$, which can be proved using a 4×2-matrix α in theorem 1. Therefore it is no dimension witness. We applied modifications (i) and (ii) of corollary 1. We started with a global random search to find good starting points, which we further optimized by a local optimization. Both algorithms are numerical. The software implementation of the maximization in equation (24) does not guarantee that the found value

is a global maximum, which implies that the calculated values for the violation are in principle only upper bounds. However since we used many different starting points and random seeds we are confident that the given digits also present the actual value of the violation. Using the described methods we arrived at the matrix

$$g' = \begin{pmatrix} -0.350\,174 & 0.323\,788 & 0.344\,416 & -0.368\,076 & -0.299\,221 & 0.314\,04 \\ -0.472\,675 & -0.357\,842 & -0.182\,589 & -0.317\,64 & -0.377\,403 & 0.215\,713 \\ -0.218\,507 & -0.300\,642 & -0.525\,576 & -0.185\,735 & 0.389\,52 & 0.279\,595 \\ 0.394\,05 & 0.286\,377 & -0.315\,566 & -0.315\,986 & 0.296\,399 & 0.391\,561 \\ 0.303\,896 & 0.375\,89 & -0.193\,803 & -0.514\,786 & -0.310\,722 & -0.200\,436 \\ 0.190\,791 & -0.355\,309 & -0.321\,679 & -0.184\,563 & -0.326\,631 & -0.511\,833 \end{pmatrix}, \tag{26}$$

which corresponds to an inequality with a qutrit to qubit ratio of $T/T_3 \approx 1.026\,22$. This seems to be small. However, we do not know of a higher ratio than 1.035 28 with few settings (see $\mathcal{B}_{X4}$ in [27], with $8 + 4$ settings). More settings allow for larger qudit to qubit ratios [27, 28].

5. Conclusions

We presented two modifications of the coefficients of bipartite CHSH-type Bell inequalities, which preserve tightness of the Tsirelson bound T given in [22]. These are rotations of the singular vectors on the subspace of the maximal singular value and the subspace of the non-maximal singular values as well as changes of non-maximal singular values. Physically, they do not affect the optimal observables (up to a relative rotation of the two laboratories).

We applied this method to show that for any relative rotation of the two laboratories, there is a Bell inequality that is maximally violated for this rotation and a fixed shared quantum state. Furthermore we optimized Bell inequalities with respect to the ratio of the quantum value and the local hidden variable bound (the violation). In particular, we did this for Bell inequalities from a series of Fishburn and Reeds [16]. The violation of the fourth Bell inequality from that series could be improved to 1.428 60.

Finally, we showed how our method can be used to optimize dimension witnessing Bell inequalities, i.e. Bell inequalities, where the maximal quantum value is not achievable with two qubits. We present an explicit example with six settings per party where the qutrit to qubit ratio is 1.026 22.

Acknowledgments

We thank N Gisin for discussions on [24]. This project was supported by the DFG, BMBF and SFF of Heinrich-Heine-University Düsseldorf.

References

[1] Bell J S 1964 On the Einstein Podolski Rosen paradox *Physics* **1** 195–200
[2] Einstein A, Podolsky B and Rosen N 1935 Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.* **47** 777–80
[3] Aspect A, Grangier P and Roger G 1982 Experimental realization of Einstein–Podolsky–Rosen–Bohm *Gedankenexperiment*: a new violation of Bell's inequalities *Phys. Rev. Lett.* **49** 91–4
[4] Weihs G, Jennewein T, Simon C, Weinfurter H and Zeilinger A 1998 Violation of Bell's inequality under strict Einstein locality conditions *Phys. Rev. Lett.* **81** 5039–43
[5] Rowe M A, Kielpinski D, Meyer V, Sackett C A, Itano W M, Monroe C and Wineland D J 2001 Experimental violation of a Bell's inequality with efficient detection *Nature* **409** 791–4

[6] Ansmann M *et al* 2009 Violation of Bell's inequality in Josephson phase qubits *Nature* **461** 504–6
[7] Christensen B G *et al* 2013 Detection-loophole-free test of quantum nonlocality, and applications *Phys. Rev. Lett.* **111** 130406
[8] Shadbolt P, Vértesi T, Liang Y-C, Branciard C, Brunner N and O'Brien J L 2012 Guaranteed violation of a Bell inequality without aligned reference frames or calibrated devices *Sci. Rep.* **2** 470
[9] Erven C *et al* 2013 Experimental three-particle quantum nonlocality under strict locality conditions arXiv:1309.1379
[10] Lanyon B P, Zwerger M, Jurcevic P, Hempel C, Dür W, Briegel H J, Blatt R and Roos C F 2013 Experimental violation of multipartite Bell inequalities with trapped ions *Phys. Rev. Lett.* **112** 100403
[11] Ekert A 1991 Quantum cryptography based on Bell's theorem *Phys. Rev. Lett.* **67** 661–3
[12] Buhrman H, Regev O, Scarpa G and de Wolf R 2010 Near-optimal and explicit Bell inequality violations arXiv:1012.5043
[13] Junge M and Palazuelos C 2011 Large violation of Bell inequalities with low entanglement *Commun. Math. Phys.* **306** 695–746
[14] He Q Y, Cavalcanti E G, Reid M D and Drummond P D 2009 Testing for multipartite quantum nonlocality using functional Bell inequalities *Phys. Rev. Lett.* **103** 180402
[15] Gao W-B, Yao X-C, Xu P, Lu H, Gühne O, Cabello A, Lu C-Y, Yang T, Chen Z-B and Pan J-W 2010 Bell inequality tests of four-photon six-qubit graph states *Phys. Rev.* A **82** 042334
[16] Fishburn P C and Reeds J A 1994 Bell inequalities, Grothendieck's constant, and root two *SIAM J. Discrete Math.* **7** 48–56
[17] Gühne O and Cabello A 2008 Generalized Ardehali–Bell inequalities for graph states *Phys. Rev.* A **77** 032108
[18] Clauser J F, Horne M A, Shimony A and Holt R A 1969 Proposed experiment to test local hidden-variable theories *Phys. Rev. Lett.* **23** 880–4
[19] Werner R F and Wolf M M 2001 Bell inequalities and entanglement *Quantum Inform. Comput.* **1** 1–25
[20] Peres A 1986 Existence of a free will as a problem of physics *Found. Phys.* **16** 573–84
[21] Cirel'son B S 1980 Quantum generalizations of Bell's inequality *Lett. Math. Phys.* **4** 93–100
[22] Epping M, Kampermann H and Bruß D 2013 Designing Bell inequalities from a Tsirelson bound *Phys. Rev. Lett.* **111** 240404
[23] Tsirelson B S 1993 Some results and problems on quantum Bell-type inequalities *Hadronic J.* **8** 329–45
[24] Gisin N 1999 Bell inequality for arbitrary many settings of the analyzers *Phys. Lett.* A **260** 8–10
[25] Gisin N 2009 Bell inequalities: many questions, a few answers *Essays in Honour of Abner Shimony (The Western Ontario Series in Philosophy of Science)* ed W C Myrvold and J Christian pp 125–40
[26] Karner H, Schneid J and Ueberhuber C W 2003 Spectral decomposition of real circulant matrices *Linear Algebra Appl.* **367** 301–11
[27] Vértesi T and Pál K 2009 Bounding the dimension of bipartite quantum systems *Phys. Rev.* A **79** 042106
[28] Briët J, Buhrman H and Toner B 2009 A generalized Grothendieck inequality and entanglement in XOR games arXiv:0901.2009

E

A quantum mechanical bound for CHSH-type Bell inequalities

Title:	A quantum mechanical bound for CHSH-type Bell inequalities
Authors:	M.E., Hermann Kampermann, and Dagmar Bruß
In:	"Quantum [Un]Speakables II" edited by Reinhold Bertlmann and Anton Zeilinger
Publisher:	Springer
Date of submission:	7 January 2015
Publication status:	Invited contribution, to be published
Contribution by M.E.:	First author (input approx. 80%)
Results:	Less technical description of the results of Appendix C and D. New example for a Bell experiment without alignment.

A quantum mechanical bound for CHSH-type Bell inequalities

Michael Epping, Hermann Kampermann and Dagmar Bruß

Abstract Many typical Bell experiments can be described as follows. A source repeatedly distributes particles among two spacelike separated observers. Each of them makes a measurement, using an observable randomly chosen out of several possible ones, leading to one of two possible outcomes. After collecting a sufficient amount of data one calculates the value of a so-called Bell expression. An important question in this context is whether the result is compatible with bounds based on the assumptions of locality, realism and freedom of choice. Here we are interested in bounds on the obtained value derived from quantum theory, so-called Tsirelson bounds. We describe a simple Tsirelson bound, which is based on a singular value decomposition. This mathematical result leads to some physical insights. In particular the optimal observables can be obtained. Furthermore statements about the dimension of the underlying Hilbert space are possible. Finally, Bell inequalities can be modified to match rotated measurement settings, e.g. if the two parties do not share a common reference frame.

1 Introduction

Since the advent of quantum theory physicists have been struggling for a deeper understanding of its concepts and implications. One approach to this end is to carve out the differences between quantum theory and "classical" theories, i.e. to explicitly point to the conflicts between quantum theory and popular preconceptions, which evolved in each individual and the scientific community from decoherent macroscopic experiences. Plain formulations of such discrepancies and convincing experimental demonstrations are crucial to internalizing quantum theory and replacing existing misconceptions. For this reason the double-slit-experiments (and similar

Michael Epping · Hermann Kampermann · Dagmar Bruß
Heinrich-Heine-University Düsseldorf, Universitätsstr. 1, 40225 Düsseldorf, Germany, e-mail: epping@hhu.de

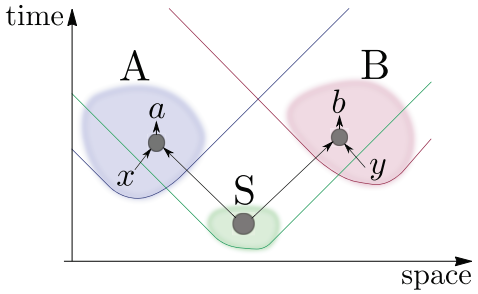


Fig. 1 Two parties, Alice (A) and Bob (B), perform a Bell experiment. Both of them receive parts of a quantum system from the source (S). They randomly choose a measurement setting, denoted by $x = 1, 2, ..., M_1$ and $y = 1, 2, ..., M_2$, and write down their outcomes $a = -1$ or 1 and $b = -1$ or 1, respectively. The experiment is repeated until the accumulated data is analyzed according to the text. Angles of 45 degrees in the space-time-diagram correspond to the speed of light. The future light cones of A, B and S show, that the setting choice and outcome of one party cannot influence the other and that A and B also cannot influence any event inside the source.

experiments with optical gratings) [1, 2, 3, 4, 5], which expose the role of state superpositions in quantum theory, are so very fascinating and famous. Other examples of "eye-openers" are demonstrations of tunneling [6, 7, pp. 33-12], the quantum Zeno effect [8] and variations of the Elitzur-Vaidman-scheme [9, 10, 11], to pick just a few.
Bell experiments [12, 13, 14, 15], which show entanglement in a particularly striking way, belong to this list. Informally, entanglement is the fact that in quantum theory the state of a compound system (e.g. two particles) is not only a collection of the states of the subsystems. This fact can lead to strong correlations between measurements on different subsystems. Before going into more detail here, we would like to note that the described differences between the relatively new quantum theory and our old preconceptions are obvious starting points when to look for innovative technologies which were even unthinkable before. This is in fact a huge motivation for the field of quantum information, where Bell experiments play a central role.

1.1 Bell experiments bring three fundamental common sense assumptions to a test

The idea of Bell was to show that some common sense assumptions lead to predictions of experimental data which contradict the predictions of quantum theory. In the following we employ a black box approach to emphasize that this idea is completely independent of the physical realization of an experiment. For example the measurement apparatuses get some input (an integer number which will in the following be called "setting") and produce some output (the "measurement outcomes"). We refer

readers preferring a more concrete notion to Section 1.2, where physical implementations and concrete measurements are outlined.

In the present paper we consider the following (typical) Bell experiment, see also Figure 1. There are three experimental sites, two of which we call the parties Alice (A) and Bob (B), and the third being a preparation site which we call source (S). Alice and Bob have a spatial separation large enough such that no signal can travel from one party to the other at the speed of light during the execution of our experiment. The source is separated such that no signal can travel from A or B to it at the speed of light before it finishes the state production. The importance of such separations will become clear later.

The source produces a quantum system, and sends one part to Alice and one to Bob. We will exemplify this in Section 1.2. A and B are in possession of measurement apparatuses with a predefined set of different settings. In each run they choose the setting randomly, e.g. they turn a knob located at the outside of the apparatus, measure the system received from the source and list the setting and outcome. In the present paper the measurements are two-valued and the outcomes are denoted by -1 and $+1$. Let M_1 and M_2 be the number of different measurement settings at site A and B, respectively. We label them by $x = 1,2,3,...,M_1$ for Alice and $y = 1,2,3,...,M_2$ for Bob. This preparation and measurement procedure of a quantum system is repeated until the amount of data suffices to estimate the expectation value of the measured observables, up to the statistical accuracy one aims at. The expectation value of an observable is the average of all possible outcomes, here ± 1, weighted with the corresponding probability to get this outcome.

Let us sketch the preconceptions that are *jointly* in conflict with the quantum theoretical predictions for Bell tests. These are mainly three concepts: Locality, realism and freedom of choice. This forces us to question at least one of these ideas, because any interpretation of quantum theory, as well as any "postquantum" theory, cannot obey all of them. We invite the reader to pick one to abandon while reading the following descriptions. Do not be confused by our comparison with the textbook formalism of quantum theory: so far you are free to choose any of them.

Locality is the assumption, that effects only have nearby direct causes, or the other way around: any action can only affect directly nearby objects. If some action here has an impact there, then something traveled from here to there. And, according to special relativity, the speed of this signal is at most the speed of light. In our setup, this means that whatever Alice does cannot have any observable effect at Bob's site. In particular, the measurement outcome at one side cannot depend on the choice of measurement setting at the other site. While the formalism of quantum theory has some "nonlocal features", e.g. a global state, it is strictly local in the above sense, because any local quantum operation on one subsystem does not change expectation values of local observables for a different subsystem.

Realism is the concept of an objective world that exists independently of subjects ("observers"). A stronger form of realism is the "value-definiteness" assumption meaning that the properties of objects always have definite values, also if they are not measured or even unaccessible for any observer. It seems to be against common sense to assume that objects cease to have definite properties if we do not measure

them any longer. In particular the natural sciences were founded on the assumption, that nature and its properties exist independently of the scientist. In our setup realism implies, that the measurement outcomes of unperformed measurements (in unchosen settings) have some value. We do not know them, but we can safely assume that they exist, give them a name and use them as variables. If possible outcomes are -1 and $+1$, for example, we might use that the outcome squared is 1 in any of our calculations. In general the (usual) formalism of quantum theory does not contain definite values for measurement outcomes independent of a measurement.
Freedom of choice, which is also sometimes called the free will assumption, means it is possible to freely choose what experiment to perform and how. Because this idea is elusive, we are content with a decision that is statistically independent of any quantity which is subject of our experiment. The idea of fate seems to be tempting to many people. However, dropping freedom of choice makes science useless. Just imagine you "want" to investigate the question whether a bag contains black balls but your fate is to pick only white balls (and put them back afterwards), even though there are many black balls inside. In our setup, freedom of choice implies, that A's and B's choice of measurement setting does not depend on the other's choice or the outcomes. In quantum theory, there is freedom of choice in the sense that random measurement outcomes of some other process can be used to make decisions.
If you decided that you preferably take leave of locality you are in good company. Many scientists conclude from Bell's theorem, that the locality assumption is not sustainable. This is particularly interesting when you consider the above comparison with the standard textbook formalism of quantum theory, which is apparently not realistic but local in the described sense. The fact that in this context many scientists speak about "quantum nonlocality" thus leads to controversy [16]. We therefore want to stress again, that the experimental contradiction only tells us that at least one of all the assumptions that lead to the predictions needs to be wrong. We cannot decide which assumption is wrong from Bell's theorem alone.
We now focus on a tool to show the contradiction in the described experiment between the above assumptions and quantum theory, the so called Bell inequalities. These are inequalities of measurable quantities which are (mainly) derived from locality, realism and freedom of choice and therefore hold for all theories which obey these principles, while they are violated by the predictions of quantum theory. We consider a special kind of Bell inequalities which are linear combinations of joint expectation values of Alice's and Bob's observables. The joint expectation value of the two observables of Alice and Bob is the expectation value of the product of the measurement outcomes, which again takes values ± 1. It depends on the setting choice x at Alice's site and y at Bob's site and we denote it by $E(x,y)$. If we denote the (real) coefficient in front of the expectation value $E(x,y)$ as $g_{x,y}$, then we can write such Bell inequalities as

$$\sum_{x=1}^{M_1}\sum_{y=1}^{M_2} g_{x,y}E(x,y) \leq B_g, \tag{1}$$

where the bound B_g depends only on the coefficients $g_{x,y}$. These coefficients form a matrix g which has dimension $M_1 \times M_2$. Any real matrix g defines a Bell inequality via Eq. (1). The may be most famous example is the Clauser-Horne-Shimony-Holt (CHSH) [17] inequality, which reads

$$E(1,1)+E(1,2)+E(2,1)-E(2,2) \leq 2. \tag{2}$$

Here the corresponding matrix g is

$$g = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{3}$$

Due to its prominence we call the class of Bell inequalities in the form of Eq. (1) CHSH-type Bell inequalities. For completeness we sketch the derivation of B_g. It turns out that it suffices to consider deterministic outcomes only, as a probabilistic theory, where the outcomes follow some probability distribution, cannot achieve a higher value in Eq. (1): it can be described as a mixture of deterministic theories and the value of Eq. (1) is the sum of the values for the deterministic theories weighted with the corresponding probability in the mixture. For deterministic theories the expectation value is merely the product of the two (possibly unmeasured) outcomes a of Alice and b of Bob, which we are allowed to use when assuming *realism*. Due to *locality* a only depends on the setting x of Alice, which has no further dependence due to *freedom of choice*. Analogously b depends only on the setting y of Bob, which in turn has no further dependence. Thus the expectation value is

$$E(x,y) = a(x)b(y). \tag{4}$$

Now we can calculate B_g by maximizing Eq. (1) over all possible assignments of -1 and $+1$ values to $a(x)$ and $b(y)$. In Eq. (2) the maximal value is $B_g = 2$, which is achieved for $a(1) = a(2) = b(1) = b(2) = 1$, for example. Note that the sign of $E(2,2)$ cannot be changed independently of the other three terms, because $E(1,2)$ and $E(2,1)$ contain $b(2)$ and $a(2)$, respectively.
We point out that any function that maps the probabilities of different measurement outcomes to a real number may be used to derive Bell inequalities, and different types of Bell inequalities can be found in the literature (e.g. [18]). However, here we focus on Bell inequalities of the form of Eq. (1).

1.2 The CHSH inequality can be violated in experiments with entangled photons

We recapitulate some basics of quantum (information) theory. Analogously to a classical bit the quantum bit, or qubit, can be in two states 0 and 1, but additionally in every possible superposition of them. Mathematically this state is a unit vector in

the two-dimensional Hilbert space (a vector space with a scalar product) $\mathbb{C}^2$ spanned by the basis vectors

$$\mathbf{0} := \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ and } \mathbf{1} := \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{5}$$

An example of a superposition of these basis states is $\psi = \frac{1}{\sqrt{2}}(\mathbf{0}+\mathbf{1})$. Any observable on a qubit with outcomes $+1$ and -1 can be written as

$$A = a_x \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}}_{\sigma_x} + a_y \underbrace{\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}}_{\sigma_y} + a_z \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}}_{\sigma_z}, \tag{6}$$

where the vector $\mathbf{a} = (a_x, a_y, a_z)^T$ (here ^{T} denotes transposition) defines the measurement direction and the matrices σ_x, σ_y and σ_z are called Pauli matrices. The expectation value of this observable given any state ψ can be calculated as $E = \psi^\dagger A \psi$ (here † denotes the complex conjugated transpose), which is between -1 and $+1$.
Any quantum mechanical system with (at least) two degrees of freedom can be used as a qubit. In the present context the spin of a spin-$\frac{1}{2}$-particle, two energy levels of an atom and the polarization of a photon are important examples of qubits. The spin measurement can be performed using a Stern-Gerlach-Apparatus [19], the energy level of an atom may be measured using resonant laser light, or the polarization of a photon can be measured using polarization filters or polarizing beam splitters.
The Hilbert space of two qubits is constructed using the tensor product, i.e. $\mathbb{C}^2 \otimes \mathbb{C}^2 = \mathbb{C}^4$. The tensor product of two matrices (of which vectors are a special case) is formed by multiplying each component of the first matrix with the complete second matrix, such that a bigger matrix arises. The state of the composite system of two qubits in states $\phi^A = (\phi_1^A, \phi_2^A)^T$ and $\phi^B = (\phi_1^B, \phi_2^B)^T$ then reads $\phi^{AB} = \phi^A \otimes \phi^B = (\phi_1^A\phi_1^B, \phi_1^A\phi_2^B, \phi_2^A\phi_1^B, \phi_2^A\phi_2^B)^T$. The states of such composite systems might be superposed, which leads to the notion of entanglement.
Out of several physical implementations of the CHSH experiment we sketch the ones with polarization entangled photons (see [20]). We identify $\mathbf{0}$ with the horizontal and $\mathbf{1}$ with the vertical polarization of a photon. Nonlinear processes in special optical elements can be used to create two photons in the state

$$\phi_+ = \frac{1}{\sqrt{2}}(1,0,0,1)^T, \tag{7}$$

i.e. an equal superposition of two horizontally polarized photons and two vertically polarized photons. The measurements of Alice and Bob in setting 1 and 2 are

$$A_1 = \cos(2\times 22.5^\circ)\sigma_x + \sin(2\times 22.5^\circ)\sigma_z, \tag{8}$$
$$A_2 = \cos(-2\times 22.5^\circ)\sigma_x + \sin(-2\times 22.5^\circ)\sigma_z, \tag{9}$$
$$B_1 = \cos(2\times 0^\circ)\sigma_x + \sin(2\times 0^\circ)\sigma_z \tag{10}$$
$$\text{and } B_2 = \cos(2\times 45^\circ)\sigma_x + \sin(2\times 45^\circ)\sigma_z, \tag{11}$$

respectively. Here the angles are the angles of the polarizer and the factor 2 is due to the fact that in contrast to the Stern-Gerlach-Apparatus a rotation of the polarizer of 180° corresponds to the same measurement again. One can now calculate the value of Eq. 2:

$$\begin{aligned} E(1,1)+E(1,2)+E(2,1)-E(2,2) = \quad & \phi_+^\dagger(A_1\otimes B_1)\phi_+ + \phi_+^\dagger(A_1\otimes B_2)\phi_+ \\ & +\phi_+^\dagger(A_2\otimes B_1)\phi_+ - \phi_+^\dagger(A_2\otimes B_2)\phi_+ \\ & = \frac{1}{\sqrt{2}}+\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{2}}-\left(-\frac{1}{\sqrt{2}}\right) \\ & = 2\sqrt{2}. \end{aligned} \tag{12}$$

The value $2\sqrt{2}\approx 2.82$ is larger than 2 and therefore the CHSH inequality is violated. One can ask whether it is possible to achieve an even higher value, e.g. when using higher-dimensional systems than qubits, because at the first glance a value of up to four seems to be possible. This question is addressed in the following sections (the answer, which is negative, is given in Section 2.2).

1.3 The quantum analog to classical bounds on Bell Inequalities are Tsirelson Bounds

Analogously to the "classical" bound one can ask for bounds on the maximal value of a Bell inequality obtainable within quantum theory, so-called Tsirelson bounds [21], and the observables that should be measured to achieve this value. In other words: which observables are best suited to show the contradiction between quantum theory and the conjunction of the three discussed common sense assumptions. This question, which is also of some importance for applications of Bell inequalities, is the main subject of the present essay.

The scientific literature contains several approaches to derive Tsirelson bounds, some of which we want to mention. The problem of finding the Tsirelson bound of Eq. (1) can be formulated as a semidefinite program. Semidefinite programming is a method to obtain the global optimum of functions, under the restriction that the variable is a positive semidefinite matrix (i.e. it has no negative eigenvalues). This implies that well developed (mostly numerical) methods can be applied [22, 23]. The interested reader can find a Matlab code snippet to play around with in the appendix 4. Furthermore there has been some effort to derive Tsirelson bounds from first principles, amongst them the non-signalling principle [24], information causality [25] and the exclusivity principle [26].

The non-signalling principle is satisfied by all theories, that do not allow for faster-than-light communication. Information causality is a generalization of the non-signalling principle, in which the amount of information one party can gain about data of another is restricted by the amount of (classical) communication between

them. The exclusivity principle states, that the probability to see one event out of a set of pairwise exclusive events cannot be larger than one.

2 The singular value bound

Here we will discuss a simple mathematical bound for the maximal quantum value of a CHSH-type Bell inequality defined via a matrix g, which we derived in [27]. While it is not as widely applicable as the semidefinite programming approach, it is an analytical expression which is easy to calculate and it already enables valuable insights. For "simple" Bell inequalities, like the CHSH inequality given above, it is sufficient to use the method of this paper.
We will make use of singular value decompositions of real matrices, a standard tool of linear algebra, which we now shortly recapitulate.

2.1 Any matrix can be written in a singular value decomposition

A singular value decomposition is very similar to an eigenvalue decomposition, in fact the two concepts are strongly related. Any real matrix g of dimension $M_1 \times M_2$ can be written as the product of three matrices V, S, W^T, i.e.

$$g = VSW^T, \tag{13}$$

where these three matrices have special properties. The matrix V is orthogonal, i.e. its columns, which are called left singular vectors, are orthonormal. It has a dimension of $M_1 \times M_1$. The matrix S is a diagonal matrix of dimension $M_1 \times M_2$, which is not necessarily a square matrix. Its diagonal entries are positive and have non-increasing order (from upper left to lower right). They are called singular values of g. The matrix W is again orthogonal. It has dimension $M_2 \times M_2$ and its columns are called right singular vectors.
The largest singular value can appear several times on the diagonal of S. We call the number of appearances the degeneracy d of the maximal singular value. Due to the ordering of S, these are the first d diagonal elements of S. Here we note the concept of a truncated singular value decomposition: instead of using the full decomposition one can approximate g by using only parts of the matrices corresponding to, e.g., the first d singular values (i.e. only the maximal ones). These are the first d left and right singular vectors, and the first part of S, which is just a $d \times d$ identity matrix multiplied by the largest singular value. Since these matrices play an important role in the following analysis we will give them special names: $V^{(d)}$, $S^{(d)}$ and $W^{(d)}$. All these matrices are depicted in Figure 2.
The matrix g maps a vector $\mathbf{v}$ to a vector $g\mathbf{v}$ which, in general, has a different length than $\mathbf{v}$. Here the length is measured by the (usual) Euclidean norm

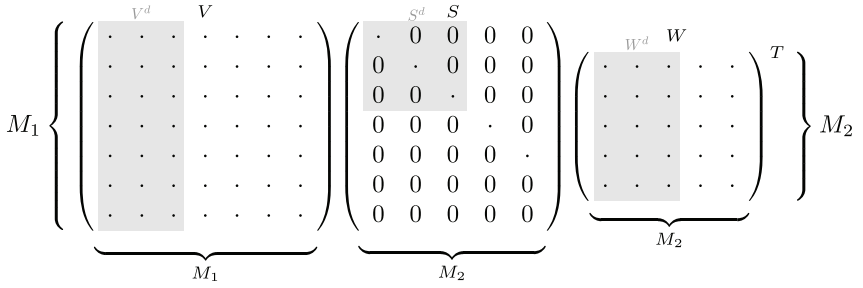


Fig. 2 The matrices involved in the singular value decomposition of a general real $M_1 \times M_2$ matrix g: V and W are orthogonal matrices, S is diagonal. V and W contain the left and right singular vectors, respectively, as columns, and S contains the singular values on its diagonal. The shaded parts belong to a truncated singular value decomposition of g. We denote the parts corresponding to the maximal singular value as $V^{(d)}$, $S^{(d)}$ and $W^{(d)}$.

$||\mathbf{v}||_2 = \sqrt{v_1^2 + v_2^2 + ... + v_{M_2}^2}$. The largest possible stretching factor for all vectors $\mathbf{v}$ is a property of the matrix: its matrix norm induced by the Euclidean norm. The value of this matrix norm coincides with the maximal singular value S_{11}. We can therefore express the maximal singular value using

$$S_{11} = \max_{\mathbf{v} \in \mathbb{R}^{M_2}} \frac{||g\mathbf{v}||_2}{||\mathbf{v}||_2} =: ||g||_2. \tag{14}$$

The notation $||g||_2$ for the maximal singular value of g is more convenient than S_{11}, as it contains the matrix as an argument.

2.2 The singular value bound is a simple Tsirelson bound

It turns out that the matrix norm of g, i.e. its maximal singular value, leads to an upper bound on the quantum value for a Bell inequality, defined by g via Eq. (1). This is the central insight of this essay. It is remarkable that a *mathematical* property, solely due to the rules of linear algebra, leads to a bound for a *physical* theory, here the theory of quantum mechanics. With the definition of the matrix norm given above, we can now write this singular value bound of g, a simple Tsirelson bound [27]. It reads

$$\sum_{x=1}^{M_1} \sum_{y=1}^{M_2} g_{x_1,x_2} E(x_1,x_2) \leq \sqrt{M_1 M_2}\, ||g||_2, \tag{15}$$

where E now denotes the expectation value of a quantum measurement in setting x_1 and x_2. Eq. (15) is the central formula of this essay. Note that this bound is not always tight, i.e. there exist examples where the right hand side cannot be reached

within quantum mechanics. However for many examples it is tight. The proof of this bound is sketched in Appendix 3.
We now calculate this bound for the CHSH inequality given in Eq. (2). We see, that here the matrix of coefficients is

$$g = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \underbrace{\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}}_{V} \underbrace{\begin{pmatrix} \sqrt{2} & 0 \\ 0 & \sqrt{2} \end{pmatrix}}_{S} \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}}_{W^T}. \tag{16}$$

It is easy to check that the given decomposition of g is a singular value decomposition, i.e. V, S and W have the properties described above. From this we read, that the maximal singular value of g is $||g||_2 = \sqrt{2}$. Then Eq. (15) tells us, that the maximal value of the CHSH inequality (Eq. (2)) within quantum theory is not larger than $2\sqrt{2}$, a value which can also be achieved when using appropriate measurements and states (see Section 1.2)

2.3 Tightness of the bound can be checked efficiently

We already mentioned that the inequality (15) is not always tight, i.e. sometimes it is not possible to find observables and a quantum state such that there is equality. From the derivation of Eq. (15) sketched in Appendix 3 one understands, why this is the case. The value $\sqrt{M_1 M_2}||g||_2$ is achieved if and only if there exists a right singular vector $\mathbf{v}$ to the maximal singular value and and a corresponding left singular vector $\mathbf{w}$ which fulfill further normalization constraints.
It is common to denote the element in the i-th row and j-th column of a matrix A as A_{ij}. We will extend this notation to denote the whole i-th row by A_{i*} and the whole j-th column by A_{*j}, i.e. the $*$ stands for "all". For example, the l-th $M_1 + M_2$ dimensional canonical basis vector, with a one at position l and 0 everywhere else, can then be written as $\mathbb{1}_{*,l}^{(M_1+M_2)}$.
With this notation at hand we write down the normalization constraint from above as the system of equations

$$\left\| \alpha^T V_{x*}^{(d)} \right\|^2 = 1 \text{ for } x = 1, 2, ..., M_1 \tag{17}$$

$$\text{and } \left\| \sqrt{\frac{M_2}{M_1}} \alpha^T W_{y*}^{(d)} \right\|^2 = 1 \text{ for } y = 1, 2, ..., M_2, \tag{18}$$

where the $d \times d'$ matrix α is the unknown. The bound in Eq. (15) is tight if and only if such matrix α solving this system of equations can be found. Here d is the degeneracy of the maximal singular value of g and d', the dimension of the vectors $\mathbf{v}_x = \alpha^T V_{x*}^{(d)}$ and $\mathbf{w}_y = \alpha^T V_{y*}^{(d)}$, is a natural number. The steps leading to Eqs. (17) and (18) can be found in the supplemental material of [27]. Because Eqs. (17) and

(18) are quadratic in α it may not be obvious how to solve it. In [27] we described an algorithm to solve the above system of equations in polynomial time with respect to the size of g. The interested reader may also find a Matlab snippet in the Appendix 4. Often the solution α is obvious, e.g. when it is proportional to the identity matrix.

2.4 Optimal measurements are obtained from the SVD

From the previous considerations we understand that the existence of the unit vectors $\mathbf{v}_x = \alpha^T V_{x*}^{(d)}$ and $\mathbf{w}_y = \alpha^T V_{y*}^{(d)}$, i.e. the existence of the matrix α that allows this normalization, is crucial to the satisfiability of the singular value bound. Furthermore they have a physical meaning, because they are related to the observables in the following way.
Let us again consider the example of Eq. (2), with the singular value decomposition

$$g = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \underbrace{\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}}_{V} \underbrace{\begin{pmatrix} \sqrt{2} & 0 \\ 0 & \sqrt{2} \end{pmatrix}}_{S} \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}}_{W^T}. \tag{19}$$

which we repeat from Eq. (16). The multiplicity $d = 2$ of the maximal singular value $\sqrt{2}$ equals the number of measurement settings M_1 and M_2, so each of the rows $V_{x*}^{(d)}$ and $W_{y*}^{(d)}$ are already normalized due to orthogonality of V and W. Therefore we can choose $\alpha = \mathbb{1}^{(2)}$ to solve Eqs. (17) and (18). We then have $\mathbf{v}_1 = (1,1)^T/\sqrt{2}$, $\mathbf{v}_2 = (1,-1)^T/\sqrt{2}$, $\mathbf{w}_1 = (1,0)^T$ and $\mathbf{w}_2 = (0,1)^T$. We are looking for a state and observables such that $E(x,y) = \mathbf{v}_x \cdot \mathbf{w}_y$, which is always possible to find (see Tsirelson's theorem, Appendix 3).
Consider for example two spin-$\frac{1}{2}$ particles in the state $\phi_+ = \frac{1}{\sqrt{2}}(1,0,0,1)^T$. Alice and Bob can measure their particles' spin with Stern-Gerlach apparatuses along any orientation in the x-z-plane. The observable of Alice corresponding to a measurement along the direction $(a_x, a_z)^T$ is

$$A = a_x \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + a_z \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{20}$$

where the matrices are two of the so-called Pauli matrices. Bob's measurement reads analogously. The reader can easily verify that the expectation value of the joint observable $A \otimes B$ is given by

$$\phi_+^\dagger (A \otimes B) \phi_+ = \mathbf{a} \cdot \mathbf{b}. \tag{21}$$

Therefore optimal measurement directions leading to equality in Ineq. (15) are given by $\mathbf{v}_x$ and $\mathbf{w}_y$. For this reason we will call $\mathbf{v}_x$ and $\mathbf{w}_y$ the measurement directions, even though they can have a dimension greater than three for general g.
We note how this construction of observables generalizes: The state can be taken to

be $\phi_+ = \frac{1}{\sqrt{D}} \sum_{i=1}^{D} \mathbf{e}_i \otimes \mathbf{e}_i$ and the observables can be constructed as $A_x = \mathbf{v}_x \cdot \mathbf{X}$ and $B_y = \mathbf{v}_y \cdot \mathbf{X}$, where $\mathbf{X}$ is a vector of matrices X_i generalizing Pauli matrices in some sense (they anticommute, i.e. $X_i X_j + X_j X_i = 0$ for $i \neq j$).

2.5 Bell inequalities allow to lower bound the Hilbert space dimension

In the previous example we chose α to be a square matrix, namely $\alpha = \mathbb{1}^{(2)}$. We will now illustrate the role of the dimension of the measurement directions d' with an example of a trivial Bell inequality, where $d' = 1$ suffices to obtain the Tsirelson bound. For this example the coefficients are $g = \mathbb{1}^{(2)}$. An obvious singular value decomposition of this identity matrix is to choose $V = S = W = \mathbb{1}^{(2)}$. Just as before we can say that $\alpha = \mathbb{1}^{(2)}$ is a solution to Eqs. (17) and (18), thus the bound is achievable with $d' = 2$. But we can also choose $\alpha = (1,1)^T$, which also solves the system of equations. In this case the measurement directions are one-dimensional ($d' = 1$), in fact they are all equal to 1. Then the expectation value given by the scalar product of the measurement directions reduces to the "classical" expectation value of deterministic local and realistic theories given in Eq. (4). Both quantum theory and local realistic theories can achieve the maximal value of two. This inequality is therefore unable to show a contradiction between quantum theory and locality, realism and freedom of choice. You might have expected this, since the matrix of coefficients does not even contain a negative coefficient, which implies that the maximum value is achieved if all outcomes are $+1$.

Let us discuss a more interesting example. It is a special instance of the family of Bell inequalities discussed by Vertési and Pál in [28]. You can also find the following analysis for the whole family in the supplemental material of [27]. The coefficients are

$$g = \begin{pmatrix} 1 & 1 & 1 & 1 \\ -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ -1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 1 \\ -1 & -1 & -1 & 1 \end{pmatrix}. \tag{22}$$

Please note, that the columns of g are orthogonal, thus it is easy to find a truncated singular value decomposition of g: We can choose $V^{(d)} = \frac{1}{2\sqrt{2}} g$, $S^{(d)} = 2\sqrt{2}\mathbb{1}^{(4)}$ and $W = \mathbb{1}^{(4)}$. One can easily check, that $\alpha = \sqrt{2}\mathbb{1}^{(4)}$ is a solution for the $(d \times d')$-matrix α of Eqs. (17) and (18), so the maximal quantum value of 16 (see Eq. (15)) is achievable with $(d' = 4)$-dimensional measurement directions. It turns out, that the system of equations is not solvable if we choose $d' = 3$, i.e. α to be a (4×3)-dimensional matrix. This has some very interesting physical implications. Since

$(d' = 3)$-dimensional measurement directions do not suffice to obtain the maximal value of the Bell inequality, we can conclude from a measured value of $Q = 16$, that our measurement directions were at least four-dimensional. Of course one will never measure this value perfectly in experiment, so what one has to do in practice is to calculate the maximum of the Bell inequality over all three-dimensional measurement directions (this is analog to the calculation of the classical bound B_g described above). If we call this value T_3, then any value between T_3 and 16 witnesses the dimension of the measurement directions to be at least four (see Figure 3).

For spin-$\frac{1}{2}$ particles, there are three orthogonal measurement directions (orienta-

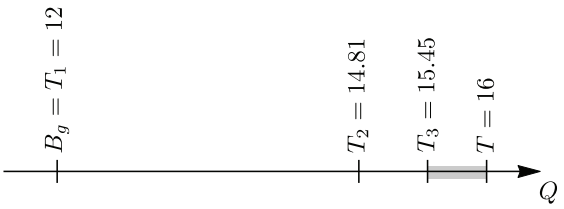


Fig. 3 Depending on the dimension d' of the measurement directions different values $T_{d'}$ are maximal for the Bell inequality given by coefficients in Eq. (22). An experimentally obtained value Q of the Bell inequality inside the shaded area witnesses, that the produced quantum system had a greater Hilbert space dimension than qubits (see text). The values are taken from [28].

tions of the Stern-Gerlach-apparatus), i.e. x-, y- and z-direction, corresponding to the three Pauli matrices (see Eq. (6)) and not more. This holds for all quantum systems with two-dimensional Hilbert space (qubits). Thus if in some Bell experiment the value of the Vertési-Pál-inequality given by the coefficients in Eq. 22 is found to be 16 (or larger than T_3), one can conclude that the produced and measured systems were no qubits. In particular they were not single spin-$\frac{1}{2}$ particles. Please note, that this argument is independent of the physical implementation of the source and the measurement apparatuses. For this reason the concept is often called device independent dimension witness.

2.6 Satisfiability of the bound can be understood geometrically

With $\mathbf{r} = V_{x*}^{(d)}$ Eq. (17) can be written as $\mathbf{r}^T \alpha\alpha^T \mathbf{r} = 1$. This quadratic form defines an ellipsoid with semi-axes $\frac{1}{\sqrt{\lambda_1}}, \frac{1}{\sqrt{\lambda_2}}, ..., \frac{1}{\sqrt{\lambda_d}}$ where $\lambda_1, \lambda_2, ..., \lambda_d$ are the eigenvalues of $\alpha\alpha^T$. Analogously the vectors $\mathbf{r}' = \sqrt{\frac{M_2}{M_1}} W_{y*}^{(d)}$ lie on the same ellipsoid (see Eq. (18)).

We therefore state, that the singular value bound is obtainable if and only if the vec-

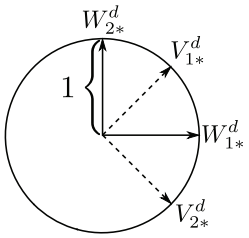


Fig. 4 The singular value bound is achievable if and only if the vectors $V^{(d)}_{x*}$ and $\sqrt{\frac{M_2}{M_1}}W^{(d)}_{y*}$ lie on the surface of an ellipsoid. These vectors and the ellipsoid (here a circle) are shown for the CHSH inequality.

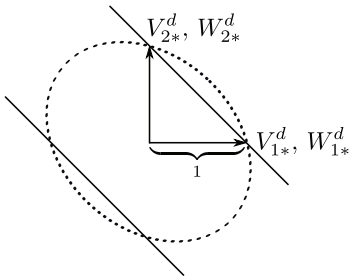


Fig. 5 The vectors $V^{(d)}_{x*}$ and $\sqrt{\frac{M_2}{M_1}}W^{(d)}_{y*}$ of $g = \mathbb{1}^{(2)}$ lie on the dotted ellipse. Increasing the larger semi-axis while keeping the vectors on the ellipse leads to the solid (degenerate) ellipse in the limit. Infinite semi-axes of the ellipsoid imply, that lower dimensional measurement directions (here $d' = 1$) suffice to achieve the Tsirelson bound.

tors $V^{(d)}_{x*}$ and $\sqrt{\frac{M_2}{M_1}}W^{(d)}_{y*}$ lie on an ellipsoid. As we mentioned before, in many cases (e.g. from the literature), α can be chosen to be proportional to the identity matrix. Thus in these cases the vectors lie on a d-dimensional sphere, i.e. for $d = 2$ they are on a circle, which is shown for the CHSH inequality [17] in Fig. 4.
If α is not square or not full rank (i.e. at least one eigenvalue of α is zero), then at least one of the eigenvalues of $\alpha\alpha^T$ is zero, too. We define the corresponding semi-axis to be infinite.
The measurement directions lie in the image of the linear transformation associated with α. Thus the dimension of the measurement directions cannot be larger than the rank of α. For $g = \mathbb{1}$ we show the degenerate ellipsoid with one infinite semi-axis corresponding to the solution $\alpha = (1,1)^T$ (see above) in Fig. 5.

2.7 Changing g without changing the Tsirelson bound

The parts of the SVD of g which do not correspond to the maximal singular value of (i.e. the non-shaded areas in Figure 2) did not appear in our discussion of the Tsirelson bound. Therefore any changes of these singular vectors in V and W and singular values in S will not affect our analysis. The last is, of course, only true as long as these new singular values do not become bigger than the (previously) maximal singular value. While this changes the matrix g, i.e. leads to a new Bell inequality, the quantum bound remains obtainable and its value remains the same.

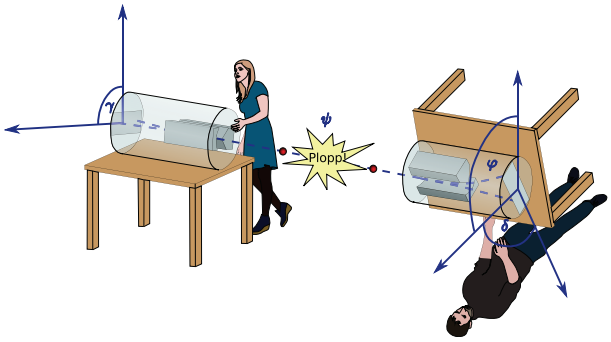


Fig. 6 Alice and Bob share pairs of particles in a spin-entangled state ψ and want to violate a Bell inequality. They each can measure the spin of their particle along transversal axes with different angle relative to the table's up. Unfortunately they were not able to agree on what "up" means, yet, and their local coordinate systems are twisted by a relative angle φ. The text explains that one possibility is to measure using (local) angles $\gamma_1 = 45°$, $\gamma_2 = -45°$, $\gamma_3 = 0°$, $\gamma_4 = 90°$ at Alice's site and $\delta_1 = 0°$ and $\delta_2 = 90°$ at Bob's site and "rotate" the Bell inequality.

From the geometric picture we immediately understand, that rotations of the vectors $V_{x*}^{(d)}$ and $\sqrt{\frac{M_2}{M_1}}W_{y*}^{(d)}$ which keep them on the ellipsoid (see Figs. 4 and 5) also do not change the value and satisfiability of the singular value bound.

We give an example to illustrate that the measurement directions can be rotated without affecting the singular value bound and its tightness. Consider the CHSH test described above, but now Alice and Bob did not agree on a common coordinate system before performing the experiment, see Figure 6. Let us assume for simplicity that their local coordinate systems are only rotated relative to each other by an angle φ around their common y-axis. This angle φ is unknown to Alice and Bob at the time of collecting the measurement data. The quantum state is still $\psi = \frac{1}{\sqrt{2}}(1,0,0,1)^T$, independent of φ.

Let us analyze the effect of the relative rotation on the violation of the CHSH inequality. The first idea might be to measure the observables of Section 2.4 in the local basis and insert the estimated expectation values into the CHSH inequality. For a relative angle $\varphi = 0°$ these observables are optimal, but for an angle of $\varphi = -45°$ Alice and Bob measure in the same direction and their data will not violate the CHSH inequality. From the previous considerations we know that it is also possible to "rotate" the Bell inequality such that the actually performed measurements are optimal for that inequality. This is can be done by applying a rotation matrix to the matrix W. However, twisting the original CHSH inequality by 45° gives $\sqrt{2}\mathbb{1}$ (up to relabeling of the measurement settings), see Figures 4 and 5. And as it is shown in Figure 5 all but one semiaxis of the ellipse associated with α can be chosen to be infinite, which is equivalent to the fact that the classical bound and the quantum bound coincide. This implies that the inequality given by coefficients $g = \sqrt{2}\mathbb{1}$ cannot be violated.

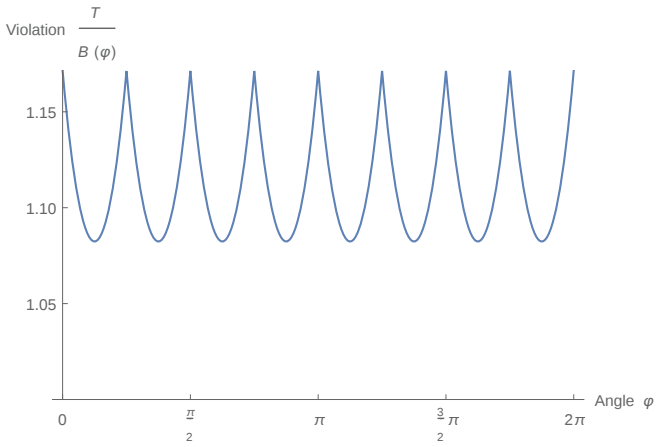


Fig. 7 The ratio of the maximal qauntum and classical value, the violation, is plotted for the Bell inequality given by the coefficients of Eq. (23) as a function of the relative rotation of the two laboratories φ.

The trick is to include more measurement directions. If the measurement directions of Alice already uniquely define the ellipsoid associated with α, then the rotation of the measurement directions of Bob does not change the fact that the Bell inequality can be violated. One obvious possibility to achieve this is to add all settings of Bob to Alice. We do this for the CHSH inequality (see Eq. (16)) and get

$$g(\varphi) = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \cos(\varphi) & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{pmatrix}. \tag{23}$$

If we call the different measurement angles $\gamma_1, \gamma_2, \gamma_3, \gamma_4$ at Alice's site and δ_1, δ_2 at Bob's site we have for $\alpha = \sqrt{2}\mathbb{1}$ that $\gamma_1 = 45°$, $\gamma_2 = -45°$, $\gamma_3 = 0°$, $\gamma_4 = 90°$, $\delta_1 = 0°$ and $\delta_2 = 90°$ are optimal measurement settings. The quantum value $T = 4$ of this inequality does not depend on φ, but the classical bound B does. Figure 7 shows the violation of the Bell inequality depending on the relative rotation φ. As expected it is always strictly larger than one. The maximal violation of $4 - 2\sqrt{2}$ can be obtained for $\varphi = k\frac{\pi}{4}$, where k is an integer number. We remark that if Alice and Bob even do not agree on a common coordinate system for the analysis of the data, they still can maximize the violation over the angle φ.

A similar analysis for a general rotation in three dimensions given by three Euler angles was done in [29]. Different approaches to Bell inequalities without a common coordinate system have been described in the literature. We want to mention the following strategy. Each party measures along random but orthogonal measurement directions. Afterwards the violation of the CHSH inequality is calculated for

all combinations of pairs of measured settings of Alice and Bob. The result is similar to the one in this section: if the parties measure along more than two directions, then one can find a Bell inequality that is violated with certainty [30].
A deeper understanding of the correlations between measurements on separated systems possible according to quantum theory, including the maximal value of Bell inequalities, is an aim of ongoing research in the field of quantum information theory. In this essay we saw how more measurement settings and higher-dimensional quantum systems can lead to stronger violations of Bell inequalities, e.g. in the context of device-independent dimension witnesses or Bell experiments without a shared reference frame. The insights gained from these simple examples may help to find Bell inequalities well suited for different situations and applications.

Acknowledgements We thank Jochen Szangolies and Michaela Stötzel for feedback which helped to improve this manuscript. ME acknowledges financial support of BMBF, network Q.com-Q.

References

[1] T. Young, *A Course of Lectures on Natural Philosophy and the Mechanical Arts* (Taylor and Walton, 1845)
[2] R.P. Feynman, R.B. Leighton, M. Sands, *The Feynman Lectures on Physics*, vol. 3 (Addison Wesley, 1971). URL `http://www.feynmanlectures.caltech.edu/`
[3] R. Bach, D. Pope, S.H. Liou, H. Batelaan, New Journal of Physics **15**(3), 033018 (2013). DOI 10.1088/1367-2630/15/3/033018
[4] B. Brezger, L. Hackermüller, S. Uttenthaler, J. Petschinka, M. Arndt, A. Zeilinger, Phys. Rev. Lett. **88**, 100404 (2002). DOI 10.1103/PhysRevLett.88.100404
[5] M. Arndt, K. Hornberger, Nature Physics **10**, 271 (2014). DOI 10.1038/nphys2863
[6] M. Razavy, *Quantum Theory of Tunneling* (World Scientific Pub Co Inc, 2003)
[7] R.P. Feynman, R.B. Leighton, M. Sands, *The Feynman Lectures on Physics*, vol. 2 (Addison Wesley, 1977). URL `http://www.feynmanlectures.caltech.edu/`
[8] W.M. Itano, D.J. Heinzen, J.J. Bollinger, D.J. Wineland, Phys. Rev. A **41**, 2295 (1990). DOI 10.1103/PhysRevA.41.2295
[9] A.C. Elitzur, L. Vaidman, Foundations of Physics **23**(7), 987 (1993). DOI 10.1007/BF00736012
[10] P.G. Kwiat, A.G. White, J.R. Mitchell, O. Nairz, G. Weihs, H. Weinfurter, A. Zeilinger, Phys. Rev. Lett. **83**, 4725 (1999). DOI 10.1103/PhysRevLett.83.4725
[11] G. Barreto Lemos, V. Borish, G.D. Cole, S. Ramelow, R. Lapkiewicz, A. Zeilinger, Nature pp. 409–412 (2014)

[12] A. Aspect, P. Grangier, G. Roger, Phys. Rev. Lett. **49**, 91 (1982). DOI 10.1103/PhysRevLett.49.91
[13] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, A. Zeilinger, Phys. Rev. Lett. **81**, 5039 (1998). DOI 10.1103/PhysRevLett.81.5039
[14] M.A. Rowel, D. Kielpinski, V. Meyer, C.A. Sackett, W.M. Itano, C. Monroe, D.J. Wineland, Nature **409**, 791 (2001). DOI 10.1038/35057215
[15] J.M.*et. al.*. Martinis, Nature **461**, 504 (2009). DOI 10.1038/nature08363
[16] M. Zukowski, C. Brukner, Journal of Physics A: Mathematical and Theoretical **47**(42), 424009 (2014). DOI 10.1088/1751-8113/47/42/424009
[17] J.F. Clauser, M.A. Horne, A. Shimony, R.A. Holt, Phys. Rev. Lett. **23**, 880 (1969). DOI 10.1103/PhysRevLett.23.880
[18] J.F. Clauser, M.A. Horne, Phys. Rev. D **10**, 526 (1974). DOI 10.1103/PhysRevD.10.526
[19] C. Gerthsen, *Physik* (D. Meschede, 2001)
[20] D. Dehlinger, M.W. Mitchell, Am. J. Phys. **70**, 903 (2002). DOI 10.1119/1.1498860
[21] B. Tsirelson, Lett. Math. Phys. **4**, 93 (1980)
[22] S. Wehner, Phys. Rev. A **73**, 022110 (2006). DOI 10.1103/PhysRevA.73.022110
[23] M. Navascués, S. Pironio, A. Acín, Phys. Rev. Lett. **98**, 010401 (2007). DOI 10.1103/PhysRevLett.98.010401
[24] S. Popescu, D. Rohrlich, Foundations of Physics **24**(3), 379 (1994). DOI 10.1007/BF02058098
[25] M. Pawlowski, T. Paterek, D. Kaslikowski, V. Scarani, A. Winter, M. Zukowski, Nature pp. 1101–1104 (2009). DOI 10.1038/nature08400
[26] A. Cabello, Phys. Rev. Lett. **110**, 060402 (2013). DOI 10.1103/PhysRevLett.110.060402
[27] M. Epping, H. Kampermann, D. Bruß, Phys. Rev. Lett. **111**, 240404 (2013). DOI 10.1103/PhysRevLett.111.240404
[28] T. Vértesi, K.F. Pál, Phys. Rev. A **77**, 042106 (2008). DOI 10.1103/PhysRevA.77.042106
[29] M. Epping, H. Kampermann, D. Bruß, J. Phys. A: Math. Theor. **47**(424015) (2014). DOI 10.1088/1751-8113/47/42/424015
[30] P. Shadbolt, T. Vértesi, Y.C. Liang, C. Branciard, N. Brunner, J.L. O'Brien, Scientific Reports **2**(470) (2012). DOI 10.1038/srep00470
[31] B. Tsirelson, Letters in Mathematical Physics pp. 93–100 (1980)

Appendix

3 Tsirelson's theorem carries the Tsirelson bound to Linear Algebra

We now sketch the derivation of Eq. (15) following [27]. It is strongly based on a theorem by Boris Tsirelson [31]. It links the expectation values of quantum measurements to scalar products of real vectors. While the full theorem shows equivalence of five different ways of expressing the expectation value, we will repeat two of them here.

Remember that in the formalism of quantum theory observables are hermitean operators, i.e. they equal their complex conjugated transpose. And quantum states can be described by density matrices, which are convex mixtures of projectors onto pure quantum states, with the weights being the probability to find the system in the corresponding pure state. This implies that the density matrix is positive and has trace one.

Consider two fixed sets of observables with eigenvalues in $[-1,1]$, $\{A_1, A_2, ..., A_{M_1}\}$ and $\{B_1, B_2, ..., B_{M_2}\}$, and a quantum state given in terms of its density matrix ρ. Then the expectation value of the joint measurement of A_x and B_y, $A_x \otimes B_y$, is $E(x,y) = \mathrm{tr}(A_x \otimes B_y \rho)$ according to quantum theory. Tsirelson's theorem states, that there exist real $M_1 + M_2$ dimensional unit vectors $\{\mathbf{v}_1, \mathbf{v}_2, ..., \mathbf{v}_{M_1}\}$ and $\{\mathbf{w}_1, \mathbf{w}_2, ..., \mathbf{w}_{M_2}\}$ such that all expectation values can be expressed as $E(x,y) = \mathbf{v}_x \cdot \mathbf{w}_y$. This is the direction we need, because it allows us to replace the expectation value in Eq. (1) by the scalar product of some real vectors. Tsirelson also proved the converse direction: given the vectors $\mathbf{v}_1, \mathbf{v}_2, ..., \mathbf{v}_{M_1}$ and $\mathbf{w}_1, \mathbf{w}_2, ..., \mathbf{w}_{M_2}$ there exist observables $A_1, A_2, ..., A_{M_1}$ and $B_1, B_2, ..., B_{M_2}$ and a state ρ such that the expectation value $E(x,y) = \mathrm{tr}(A_x \otimes B_y \rho)$ equals the scalar product $\mathbf{v}_x \cdot \mathbf{w}_y$.

After application of Tsirelson's theorem Eq. (1), i.e. $\sum_{x,y} g_{x,y} E(x,y)$, takes the form

$$\begin{aligned} \sum_{x=1}^{M_1} \sum_{y=1}^{M_2} g_{x,y} \sum_{i=1}^{M_1+M_2} v_{x,i} w_{y,i} &= \sum_{x=1}^{M_1} \sum_{y=1}^{M_2} \sum_{i=1}^{M_1+M_2} \sum_{j=1}^{M_1+M_2} v_{x,i} g_{x,y} \delta_{ij} w_{y,j} \\ &= \mathbf{v}^T (g \otimes \mathbb{1}^{(M_1+M_2)}) \mathbf{w}. \end{aligned} \tag{24}$$

Here we expressed the scalar product as a matrix product using the $M_1 + M_2$ dimensional identity matrix $\mathbb{1}^{(M_1+M_2)}$ and defined the vectors $\mathbf{v}$ and $\mathbf{w}$, which arise if one concatenates all $\mathbf{v}_x$ and $\mathbf{w}_y$, respectively. For the decomposition given in Eq. (16) with $\alpha = \mathbb{1}^{(2)}$, for example, $\mathbf{v}_1 = (\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})^T$ and $\mathbf{v}_2 = (\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}})^T$ and thus $\mathbf{v} = (\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}})^T$. From Eq. (24) we see, that the maximal quantum value of the Bell inequality is given by the maximal singular value (the maximal stretching factor) of $g \otimes \mathbb{1}^{(M_1+M_2)}$ times the length of the vectors $\mathbf{v}$ and $\mathbf{w}$. The matrix $g \otimes \mathbb{1}^{(M_1+M_2)}$ has the same singular values as g, except that each of them appears $M_1 + M_2$ times. Because the $\mathbf{v}_x$ and $\mathbf{w}_y$ constituting $\mathbf{v}$ and $\mathbf{w}$ are all unit vectors, the length of $\mathbf{v}$ is $\sqrt{M_1}$ and the length of $\mathbf{w}$ is $\sqrt{M_2}$. Putting these factors together we

arrive at Eq. (15).

4 MATLAB snippets

```
function [ T ] = singularvaluebound( g )
%SINGULARVALUEBOUND Calculates the SV-bound of g
%    the returned value is a Tsirelson bound for
%    the CHSH-type inequality given by g
T=sqrt(numel(g))*norm(g);
end

function [ a ] = alphamatrix( g )
%ALPHAMATRIX Links SVD to measurement directions
%    see PRL 111, 240404 (2013)
[M1 M2]=size(g);
[V S W]=svd(g);
acc=1E-4; % adjust to numerical precision
d=sum(diag(S)>=S(1,1)-acc);
% the vectors to be normalized by alpha:
A=[V(1:M1,1:d); sqrt(M2/M1)*W(1:M2,1:d)];
Q=(A*A').^2;
c=pinv(Q)*ones(M1+M2,1);
if sum(abs(Q*c-ones(M1+M2,1))>acc)
    error('alphamatrix:nosol','No solution alpha found.');
else
    X=A'*diag(c)*A;
    if eigs(X,1,'sm')<0
        error('alphamatrix:norealsol',
              'No real solution alpha found.');
    end
end
a=X^0.5;
end

function [ T ] = tsirelsonbound( g )
%TSIRELSONBOUND Calculates the Tsirelson bound for g
%    Uses the semidefinite programm described by
%    Stephanie Wehner in PRA 73, 022110 (2006).
[M1 M2]=size(g);
W=[zeros(M1,M1) g; g' zeros(M2,M2)];
G=sdpvar(M1+M2,M1+M2);
obj=trace(G*W)/2;
```

```
F=set(G>0);
for  i=1:M1+M2
     F=F+set(G(i,i) == 1);
end
solvesdp(F,obj,sdpsettings('verbose',0));
T=-double(obj);
end
```

F

Graph state quantum repeater networks

Title:	Graph state quantum repeater networks
Authors:	M.E., Hermann Kampermann, and Dagmar Bruß
Journal:	Physical Review Letters
Impact factor:	7.512
Date of submission:	24 April 2015
Publication status:	Under review
Contribution by M.E.:	First author (input approx. 80%)
Results:	Description of quantum repeaters with encoding in the graph state formalism. Detailed error analysis and improved rates in comparison to the literature. Generalization to networks of quantum repeaters, which distribute a general graph state.

Graph State Quantum Repeater Networks

Michael Epping,* Hermann Kampermann, and Dagmar Bruß
Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, Universitätsstr. 1, D-40225 Düsseldorf, Germany

We show how general graph states, an important resource state for multipartite quantum protocols, can be distributed over large distances using intermediate repeater stations. To this aim we describe a one way quantum repeater scheme using encoding in the language of graph states. For a general Calderbank-Shor-Steane (CSS) code we do a refined error analysis that allows to correct qubit errors and erasures caused by imperfect preparation, gates, transmission, detection, etc.. We analyze the cost and repeater rate for this general scheme. The concept is exemplified by the 7-qubit Steane code and the quantum Golay code. In the considered parameter regime the latter outperforms all known schemes.

PACS numbers: 03.67.Dd,03.67.Bg,03.67.Pp

I. INTRODUCTION TO QUANTUM REPEATERS

Several fascinating aspects of quantum theory can be summed up as its "non-classicality", which is particularly striking in quantum entanglement. The benefit of quantum technology increases with the system size, e.g. when doing quantum computations [1, 2]. Additionally the "non-classicality" of quantum systems increases with the number of spatially separated subsystems. For example the violation of Bell inequalities is known to increase exponentially with the number of parties [3]. several multipartite protocols with quantum advantages are known, e.g. secret sharing or multipartite cryptography [4–8]. They motivate the investigation of the distribution of the required resource states consumed during the execution of the protocols. In the age of the Internet it is not hard to imagine that the parties will be distributed over distances at the global scale and form a two dimensional network in the future. Distribution of entanglement over more than ≈ 200 km requires intermediate quantum repeaters to compensate for losses [9–12].

In this letter we present the generalization of error correction [13–17] based quantum repeaters [18–24] to general networks of such devices that are capable of producing multipartite entangled resource states. This generalization is facilitated by the use of the language of graph states [25–32] that gives a graphic description of the network and the corresponding quantum states. We improve the error analysis compared to the literature by taking many sources of errors into account. There are important parameter regimes for which this protocol is more efficient with respect to the used resources than the previously known ones.

First we explain the basic idea of the repeater for two parties using the stabilizer formalism. We then shift the graph state to a logical graph state via quantum error correction codes and analyze the performance depending on the amount of imperfections and the distance between the repeater stations. Finally we show how this scheme generalizes to networks.

A graph state $|G\rangle$ corresponds to a mathematical graph G consisting of a set V of N vertices and a set of edges $E \subset V \times V$. It can be defined in two equivalent ways. First, $|G\rangle$ is the state that is created from the state $|+\rangle^{\otimes N}$, $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, by applying a controlled-phase gate C_Z on each pair of vertices in E, i.e.

$$|G\rangle = \prod_{(i,j)\in E} C_Z^{(i,j)} |+\rangle^{\otimes N}. \tag{1}$$

Second, $|G\rangle$ is the unique state stabilized by the stabilizer generators

$$g_i = X_i \prod_{\substack{j\in V \\ (i,j)\in E}} Z_j, \tag{2}$$

i.e. $g_i|G\rangle = |G\rangle$, for all $i \in V$. Here X_i and Z_i denote Pauli-operators for the vertex i.

In order to present the main idea we discuss how a simple line graph is produced that consists of an even number N of vertices (see Figure 1). Odd vertex counts lead to an analogous reasoning. This line graph corresponds to a chain of repeaters connecting two parties, Alice (A) and Bob (B). The repeater scheme is one-way, i.e. signals are sent from left to right starting at Alice's site. A qubit in state $|+\rangle$ is produced at each repeater station. This qubit is entangled with the qubit from the previous station by a local C_Z gate and then sent through the channel (see Figure 2). At the next repeater station it is processed by another local C_Z gate and it will be measured at this site. The gates create the edges of the graph state. Note, however, that it is not necessary to store the full graph state, as it is created and measured step by step.

The maximal connectedness of a graph implies that it is possible to turn the quantum state into a maximally entangled state shared by Alice and Bob. This can be formulated in the stabilizer formalism. We number the vertices from left to right, and denote the first qubit by A and the last by B.

* epping@hhu.de

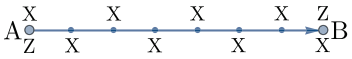


FIG. 1. A line of repeater stations links parties A and B. The operators of the two main stabilizers are shown above and below the graph. X-measurements on the repeater stations (small dots) and application of appropriate byproduct operators projects the state of A and B onto a Bell pair. The arrow indicates the transmission direction.

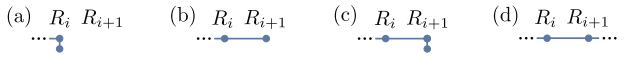


FIG. 2. The operations on repeater stations R_i and R_{i+1}. The preparation and the gate of station R_i (a) and the transmission of the qubit produced at R_i to R_{i+1} (b) creates the edge $(i, i+1)$, where the same procedure is repeated to create the next edge (c,d).

The product of all stabilizer generators centered on odd qubits and the analogous product for the even ones are two stabilizers connecting A and B (see also [33]). We call them the main stabilizers S_A and S_B. All qubits except A and B are measured in the X-basis. This projects the state onto one stabilized by $g_A = X_A \otimes Z_B$ and $g_B = Z_A \otimes X_B$, up to byproduct operators which depend on the measurement outcomes. Afterwards one of four orthogonal Bell states is shared by A and B, where the measurement outcomes determine which one. Any qubit can be measured directly after it has been processed by both gates. This is equivalent to creating the whole graph state, but easier experimentally. If parties A and B want to perform X or Z measurements on the final Bell state, then the byproduct operators can be applied on the measurement outcomes: X flips a Z outcome, Z flips an X outcome and $H = \frac{1}{\sqrt{2}}(X + Z)$ flips the basis label.

The previous considerations must be expanded by an error model (see also [34]). We distinguish two main error types: noticed (losses) and unnoticed ones (noise). Measurement outcomes are 0, 1, and ? (no outcome). Both types of errors, i.e. losses and noise, will be corrected by the same error correction code as discussed later on. In our error model a corrupted qubit is set to a completely mixed state, i.e. all errors are modeled by the depolarizing channel. It is convenient to take the equivalent viewpoint [35] that these imperfections are discrete X and Z errors randomly occurring on the qubits after perfect distribution of the graph state. X and Z errors each occur on this qubit independently with probability $\frac{1}{2}$. We account for spreading of errors by gates. C_Z-gates propagate X-errors to Z-errors while they do not propagate Z-errors. Thus in the present circuit (see Figure 3), errors only propagate to neighboring qubits. X-(Z-)errors before a Z-(X-)measurement flip measurement outcomes. The probability for wrong outcomes on "inner" qubits (i.e. all qubits except A and B) is f_q. Any process acting on a physical qubit can lead to an error.

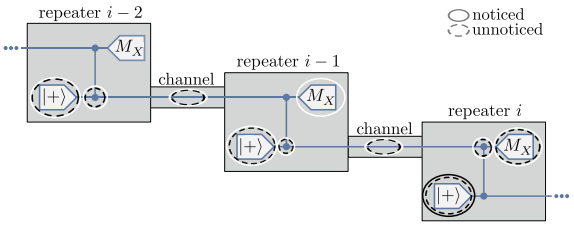


FIG. 3. Encircled processes in this circuit diagram can lead to an error on the qubit measured at repeater i. Solid and dashed lines denote unnoticed and noticed errors, respectively. Black circle errors lead to a flip of the measurement outcome. The outcome will be marked as ? if any white circle error occurred.

We include the failure rates f_P (preparation), f_G (gates), f_T (transmission), and f_M (measurements).
Because the losses will be dominated by the transmission, we mark the outcome of repeater i as ? whenever the qubit $i-1$ got lost.
There are nine sources of unnoticed phase-flip errors on an inner physical qubit i: three preparations, three gates, two transmissions and one measurement (see black circles in Figure 3). All lie in between repeater stations $i-2$ and i, because errors only propagate to neighboring qubits. Thus, for inner physical qubits the probability of phase-flip errors reads

$$\begin{aligned} f_q = & P_{\text{odd}}\left(\left(P_{\text{odd}}\left(\frac{f_{P,u}}{2}, 2\right), \frac{f_{P,n}+f_{P,u}}{2},\right.\right. \\ & \left.\left. P_{\text{odd}}\left(\frac{f_{G,u}}{2}, 3\right), P_{\text{odd}}\left(\frac{f_{T,u}}{2}, 2\right), \frac{f_{M,u}}{2}\right)\right), \end{aligned} \tag{3}$$

where $P_{\text{odd}}(p, n)$ denotes the probability that in n tosses of a coin the side appearing with probability p occurs an odd number of times and $P_{\text{odd}}(\vec{p})$ is used when the probabilities pooled in $\vec{p}$ may be different for each toss (see [36]). The index distinguishes noticed and unnoticed errors. We assume that the single qubit errors are independent and identically distributed. Physical qubits may get lost in any process. Thus the effective probability for a ?-outcome is (see white circles in Fig 3)

$$f_l = 1-(1-f_{P,n})^2(1-f_{G,n})^3(1-f_{T,n})^2(1-f_{M,n})^2. \tag{4}$$

Typical losses for optical fibers are

$$f_{T,n} = 1-(1-f_{C,n})e^{-L_0/L_{\text{att}}}, \tag{5}$$

where $f_{C,n}$ is a coupling failure probability, L_0 is the repeater distance and $L_{\text{att}} \approx 20$ km defines the attenuation of the fiber.
Errors on inner qubits propagate to A or B via the application of the byproduct operators. Additionally processing A and B can directly lead to errors. We denote these error probabilities f_A and f_B. In a prepare-and-measure scenario of a quantum key distribution protocol, which is equivalent to producing the entangled state and A is measured in X or Z basis, qubit 2 is prepared in $|0\rangle, |1\rangle, |+\rangle$,

or $|-\rangle$ and qubit $N-1$ is measured, i.e. $f_A = f_B = 0$. Even numbers of errors on the same main stabilizer cancel each other. We denote the resulting error rate of the main stabilizer S_A by e_A and for S_B by e_B: With probability e_A (e_B) the produced state is stabilized by $-g_A$ ($-g_B$) instead of g_A (g_B). We estimate these error rates by

$$\begin{aligned} e_A =& P_{\text{odd}}\left(\left(P_{\text{odd}}\left(\bar{f}_q, \left\lceil\frac{N-2}{2}\right\rceil\right), f_A, f_B\right)\right) \\ \text{and } e_B =& P_{\text{odd}}\left(\left(P_{\text{odd}}\left(\bar{f}_q, \left\lfloor\frac{N-2}{2}\right\rfloor\right), f_A, f_B\right)\right), \end{aligned} \tag{6}$$

where the logical error probability $\bar{f}_q$ at the moment equals the physical error rate f_q. We come back to this point later.

We focus on the application to quantum key distribution, where the crucial quantity is the secret fraction r_∞, i.e. the number of secret bits per Bell pair that result after the data post-processing. For the BB84 protocol it solely depends on the error rates e_A and e_B and is given by [37]

$$r_\infty = \max\{1 - h(e_A) - h(e_B), 0\}, \tag{7}$$

with the binary entropy $h(p) = -p\log_2(p) - (1-p)\log_2(1-p)$. We have discussed how a Bell pair is gained from the graph state. In the following we describe how our scheme can be used to decrease the error rates.

To tackle imperfections we use error correction codes, i.e. we now use several physical qubits to encode the logical qubit corresponding to a vertex. This leads to a logical graph state. The operators in the graph state stabilizers are replaced by logical operators, which we denote (like all logical quantities) with a bar. The idea of creating a Bell state from the main stabilizers transfers to the logical level.

We focus on Calderbank-Shor-Steane (CSS) codes. Transversal (i.e. qubitwise) implementations of controlled-NOT gates are valid in all CSS codes [17]. We use two codes, the code $\mathcal{C}$ and the code $\mathcal{C}'$, which arises from $\mathcal{C}$ by exchanging the role of the $\bar{X}$ and $\bar{Z}$. Even numbered logical qubits are encoded using $\mathcal{C}$, the odd ones using $\mathcal{C}'$. This way the transversal application of the controlled-NOT gates acts like a logical controlled-Phase gate and we can stick to the notation of graph states. The error analysis is analogous for both codes. We elaborate on the analysis for $\mathcal{C}$.

We assume, that the $\bar{X}_i$-operator consists exclusively of single qubit X-operators. Hence the measurement outcome of $\bar{X}_i$ is affected by phase flip errors (Z). Due to the transversal implementation the physical error rate remains as before.

An $[[n,k,d]]$ quantum code encodes k logical qubits into n physical ones, such that $t = \lfloor\frac{d-1}{2}\rfloor$ single qubit errors can be corrected. The graph state repeater simultaneously creates k Bell pairs. The code space stabilizers containing X and $\mathbb{1}$ operators correspond to the rows of a parity check matrix H_X. Thus in absence of any errors the X measurement outcomes are valid codewords of the corresponding linear code. Decoder for common codes and their error rates are known [13, 38]. An $\bar{X}$-error remains, if the outcomes are decoded to a wrong parity codeword. This leads to the logical error rate $\bar{f}_q$. If specific loss patterns occurred, e.g. more than d losses in one block, we may choose to abort the protocol. The effective secret fraction

$$R = P_{\text{succ}} r_\infty \tag{8}$$

then decreases by a factor P_{succ}. In our analysis $\bar{f}_q$ and P_{succ} are the only quantities that explicitly depend on the employed code (in practice f_P will also strongly depend on the code).

TABLE I. Example values of n (number of qubits per station), w (number of stations), and L (total distance between A and B) that lead to a nonzero secret key rate R. Unmentioned errors are neglected for this calculation.

Code	n	w	L in km	R in %	errors
7-qubit code	7	750	500	0.1	$f_G = 10^{-4}$
		650	200	35.7	
Golay code	23	800	1000	79.7	
		525	1000	4.7	
		2500	1000	28.4	$f_G = f_P = 10^{-3}$, $f_C = f_D = 10^{-2}$
		180	180	54.4	

A popular example of a CSS code is the [[7,1,3]] Steane code [15]. It is symmetric in X and Z, thus we can simply use one code and transversal C_Z-gates. The stabilizers can be read from the parity check matrix of the (7,4)-Hamming code [13]. We choose to abort if we notice three losses. The logical error rate $\bar{f}_q$ and success rate P_{succ} for this code and choice of fatal errors is given in the supplemental material [36]. From these quantities the effective secret fraction can be calculated using Eq. (7) and Eq. (8). Example values can be found in Table I.

To tolerate more errors, e.g. for increased repeater distances or to relax the requirements for the gates, larger codes are required. We discuss an application of the [[23,1,7]] Golay code using a decoding described in [39]. We take the word error rate p_w, i.e. the probability of recovering to a wrong codeword, from that reference. Half of the 4096 codewords correspond to a $+1$ and -1 outcome of $\bar{X}$, respectively. We thus assume $\bar{f}_q \approx p_w/2$. Fault tolerant preparation schemes have been investigated in [40]. Table I lists values for the Golay code.

To compare different codes we use a cost function C' [24] as figure of merit. It is the number of qubits per station n (neglecting preparation overhead) times the number of repeater stations w divided by the total distance L and the rate R, i.e. $C' = \frac{nw}{LR}$. We optimized C' over w for different L for several codes, see Figure 4. The optimal separation distance of the repeater stations decreases with increasing total distance.

This quantity also allows comparison with other repeater schemes, e.g. the analysis in [24] of the quantum

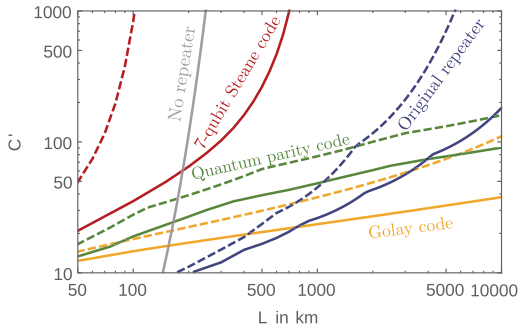


FIG. 4. The cost for different schemes with gate failure rates $f_G = 10^{-3}$ (dashed) and $f_G = 10^{-4}$ (solid): The presented repeater using the Seven-Qubit Steane code (red) and the quantum Golay code (yellow), the quantum parity code of [24] (green) and the original (distillation based) scheme [9, 12] (blue). The gray line corresponds to using no repeaters.

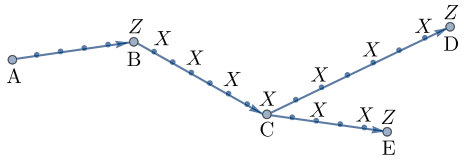


FIG. 5. The graph state of the large vertices is obtained, when all repeater stations (small vertices) are measured in the X-basis. The shown operators form the main stabilizer centered on C.

parity code (QPC, a generalization of the Shor code with special abortion strategy [41]), when one pays attention to the fact that the authors considered less errors than Eq. (3).

Figure 4 gives the comparison to the original distillation based protocol without encoding [9]. Note that this comparison strongly depends on the assumed time for local operations (here 10 μs), since this is the only limiting factor in the case of forward error correction, while the rate of the two-way protocol is restricted by the classical communication time [12]. We point out that the repeater with Golay code outperforms the original repeater already at shorter distaces than the quantum parity code. See [34] for details.

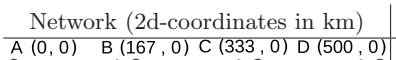
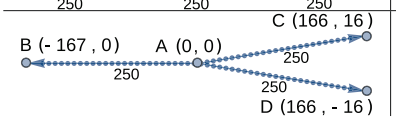
We considered a repeater setup corresponding to the generation of a line graph to distribute a Bell pair. For more than two parties it is possible to distribute other more complex and highly entangled states based on other graphs. We generalize the idea of main stabilizers to general graphs.

In order to distribute the graph state $|G\rangle$ the edges of G are replaced by line graphs with repeater stations as discussed above (see Figure 5). Let the number of repeater stations w_{ij} on all these transmission lines $(i,j) \in E$ be even for simplicity. The main stabilizers S_i are the stabilizer generators g_i of $|G\rangle$ connected by chains of X-operators on every second repeater station (see also [33]). Measuring these intermediate qubits in the X-basis projects the state onto one stabilized by the generators of $|G\rangle$ up to byproduct operators, i.e. this procedure can be used to create $|G\rangle$. Cycles in a graph may increase the storage time of some qubits, since their measurement can be performed only after all incoming neighbors gates acted. Note that the distribution of a state $|G'\rangle$ which is local-unitary-equivalent to $|G\rangle$ can be less demanding [42, 43]. The performance analysis of the previous paragraphs can be transferred to networks. Analogous to Eq. (6) one can calculate the error probability

$$e_i = P_{\text{odd}}\left(\bar{f}_q, \frac{1}{2}\sum_j w_{ij}\right) \tag{9}$$

for all main stabilizers S_i. Table II lists these values for examples of two small networks, a line and a star graph. The in-degree of a vertex corresponding to a party influences the noticed and unnoticed error rates at this position (compare to Eqs. (3) and (4)) and the out-degree will in practice influence the preparation error in a prepare-and-measure-scenario. The last is due to the fact that an (nn_o)-qubit state is sent, where n is the number of qubits of one block and n_o is the out-degree. However, the performance mainly depends on the error rates at the repeater stations (assuming that there are few parties and many repeater stations).

TABLE II. The error rates for two small networks using the Seven Qubit Steane Code with $f_G = 10^{-4}$.

Network (2d-coordinates in km)	e_A	e_B	e_C	e_D
	0.02	0.04	0.04	0.02
	0.06	0.02	0.02	0.02

Thus in conclusion we described how any multipartite graph state can be distributed via repeater stations. The procedure can be understood as the creation of a large graph state followed by a projection onto the desired state by local measurements on the repeater stations. Operational errors and channel erasures are treated equally. CSS codes have been employed to tackle these imperfections. In particular the 23-qubit Golay code turns out to be remarkably efficient in the considered scenario of losses and noise. General graph states can be distributed with effort, rate and quality comparable to the distribution of a single Bell pair by error correction based repeaters.

ACKNOWLEDGMENTS

M.E. acknowledges helpful discussions with S. Muralidharan and financial support by BMBF.

[1] L. K. Grover, Proceedings, 28th Annual ACM Symposium on the Theory of Computing (STOC) , 212 (1996).

[2] P. W. Shor, SIAM J.Sci.Statist.Comput. 26 (1997) 1484 (1997).

[3] N. Mermin, Phys. Rev. Lett. **65**, 1838 (1990).

[4] C. Bennett and G. BRassard, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing , 175 (1984).

[5] W. Dür, H. Aschauer, and H.-J. Briegel, Phys. Rev. Lett. **91**, 107903 (2003).

[6] K. Chen and H.-K. Lo, eprint arXiv:quant-ph/0404133 (2004), quant-ph/0404133.

[7] W. Dür, J. Calsamiglia, and H.-J. Briegel, Phys. Rev. A **71**, 042336 (2005).

[8] D. Markham and B. C. Sanders, Phys. Rev. A **78**, 042309 (2008).

[9] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998).

[10] W. Dür, H.-J. Briegel, J. I. Cirac, and P. Zoller, Phys. Rev. A **59**, 169 (1999).

[11] P. van Loock, T. D. Ladd, K. Sanaka, F. Yamaguchi, K. Nemoto, W. J. Munro, and Y. Yamamoto, Phys. Rev. Lett. **96**, 240501 (2006).

[12] S. Abruzzo, S. Bratzik, N. K. Bernardes, H. Kampermann, P. van Loock, and D. Bruß, Phys. Rev. A **87**, 052315 (2013).

[13] F. MacWilliams and N. Sloane, *The Theory of Error-Correcting Codes*, 2nd ed. (North-Holland Publishing Company, 1978).

[14] P. Shor, Phys. Rev. A **52**, R2493 (1995).

[15] A. Steane, Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences **452**, 2551 (1996).

[16] D. Gottesman, *Stabilizer codes and quantum error correction*, Ph.D. thesis, California Institute of Technology (1997).

[17] D. Lidar and T. Brun, *Quantum Error Correction* (Cambridge University Press, 2013).

[18] L. Jiang, J. M. Taylor, K. Nemoto, W. J. Munro, R. Van Meter, and M. D. Lukin, Phys. Rev. A **79**, 032325 (2009).

[19] W. Munro, K. Harrison, A. Stephens, S. Devitt, and K. Nemoto, Nat. Phot. **4**, 792 (2010).

[20] A. G. Fowler, D. S. Wang, C. D. Hill, T. D. Ladd, R. Van Meter, and L. C. L. Hollenberg, Phys. Rev. Lett. **104**, 180503 (2010).

[21] W. Munro, A. Stephens, S. Devitt, K. Harrison, and K. Nemoto, Nat. Phot. **6**, 777 (2012).

[22] N. K. Bernardes and P. van Loock, Phys. Rev. A **86**, 052301 (2012).

[23] S. Bratzik, H. Kampermann, and D. Bruß, Phys. Rev. A **89**, 032335 (2014).

[24] S. Muralidharan, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, Phys. Rev. Lett. **112**, 250501 (2014).

[25] H. J. Briegel and R. Raussendorf, Phys. Rev. Lett. **86**, 910 (2001).

[26] M. Hein, J. Eisert, and H. J. Briegel, Phys. Rev. A **69**, 062311 (2004).

[27] G. Tóth and O. Gühne, Phys. Rev. Lett. **94**, 060501 (2005).

[28] M. Hein, W. Dür, and H.-J. Briegel, Phys. Rev. A **71**, 032350 (2005).

[29] O. Gühne, G. Tóth, P. Hyllus, and H. J. Briegel, Phys. Rev. Lett. **95**, 120405 (2005).

[30] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Van den Nest, and H. . Briegel, eprint arXiv:quant-ph/0602096 (2006), quant-ph/0602096.

[31] D. Markham, A. Miyake, and S. Virmani, New Journal of Physics **9**, 194 (2007).

[32] D. Cavalcanti, R. Chaves, L. Aolita, L. Davidovich, and A. Acín, Phys. Rev. Lett. **103**, 030502 (2009).

[33] J.-Y. Wu, H. Kampermann, and D. Bruß, ArXiv e-prints (2015), arXiv:1504.03302 [quant-ph].

[34] M. Epping, H. Kampermann, and D. Bruß, *On the error analysis of encoded quantum repeaters* (in prep.).

[35] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*, Cambridge Series on Information and the Natural Sciences (Cambridge University Press, 2000).

[36] See Supplemental Material at [URL inserted by publisher] for the details of the calculation.

[37] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).

[38] T. Cover and N. Sloane, *Elements of Information Theory*, 2nd ed. (Wiley, 1978).

[39] M. Elia and G. Taricco, Annales Des Telecommunications **50**, 721 (1995).

[40] A. Paetznick and B. Reichardt, QIC **12**, 1034 (2012).

[41] T. C. Ralph, A. J. F. Hayes, and A. Gilchrist, Phys. Rev. Lett. **95**, 100501 (2005).

[42] M. Van den Nest, J. Dehaene, and B. De Moor, Phys. Rev. A **69**, 022316 (2004).

[43] A. Cabello, L. E. Danielsen, A. J. López-Tarrida, and J. R. Portillo, Phys. Rev. A **83**, 042314 (2011).

G

On the error analysis of quantum repeaters with encoding

Title:	On the error analysis of quantum repeaters with encoding
Authors:	M.E., Hermann Kampermann, and Dagmar Bruß
Journal:	Applied Physics B: Lasers and Optics
Impact factor:	1.856
Date of submission:	30 July 2015
Publication status:	Under review
Contribution by M.E.:	First author (input approx. 80%)
Results:	Details of the error analysis in quantum repeaters with encoding with a focus on error propagation. Comparison of the standard repeater scheme with encoding based repeaters. Discussion of abortion strategies on occurence of a critical amount of errors.

Applied Physics B manuscript No.
(will be inserted by the editor)

On the error analysis of quantum repeaters with encoding

Michael Epping[1], **Hermann Kampermann**[1], **Dagmar Bruß**[1]

Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, Germany

Received: date / Revised version: date

Abstract Losses of optical signals scale exponentially with the distance. Quantum repeaters are devices that tackle these losses in quantum communication by splitting the total distance into shorter parts. Today two types of quantum repeaters are subject of research in the field of quantum information: Those that use two-way communication and those that only use one-way communication. Here we explain the details of the performance analysis for repeaters of the second type. Furthermore we compare the two different schemes. Finally we show how the performance analysis generalizes to large-scale quantum networks.

1 Introduction

Signals in long distance telecommunications are subject to corruptions. Typically the amplitude decreases exponentially with the covered distance [11]. Thus intermediate repeaters which amplify and purify the signal are necessary building blocks for reliable transmission. In quantum cryptography and communication the signals transport coherent quantum information.
One possibility to overcome the exponential scaling of losses with distance is the entanglement swapping and -distillation based repeater scheme, which was developed by H.-J. Briegel, W. Dür, J. Cirac and P. Zoller in [3]. Here entangled pairs are distributed amongst neighboring repeater stations and Bell measurements on each station result in entangled states covering a larger distance (so-called entanglement swapping). These operations introduce errors which can be tackled by entanglement distillation, i.e. protocols that concentrate several imperfect copies of entangled states into a single copy with higher fidelity with respect to a maximally entangled state [2,6,7]. Two-way classical communication is used to acknowledge reception of photons and success of distillation.
A different approach, introduced by L. Jiang, J. Taylor, K. Nemoto, W. Munro, R. Van Meter, and M. Lukin in [13], replaces the entanglement distillation step by the use of quantum error correction codes for forward error correction, i.e. communication is only required in one direction. In comparison to the previous schemes these improve the repeater rate at the cost of being more demanding in terms of resources and the quality of operations. Subsequent work considered different codes and improved the error analysis [16,10,17,18,9].
In the present paper we attempt to give a simple analysis of repeaters of the latter type. Before describing the error analysis we motivate the quantum repeater circuits in Section 2. We use the stabilizer formalism, which is very convenient in this context. Section 3 summarizes the error model of depolarizing noise, which is widely used in the context of error correction. Section 4 then discusses a quantum repeater in the circuit model. We put emphasis on the sources of errors and their propagation and estimate the effective error rates of the physical qubits. The considered repeater schemes are based on error correction codes, which implies that several physical qubits form a logical qubit. This redundancy allows to correct errors and the strength of this correction is discussed in Section 5. The overall performance of the repeater scheme, i.e. its ability to produce a specific entangled state, is then analyzed in Section 6 and compared to the original scheme. Finally we sketch in Section 7 how repeaters with encoding generalize to large-scale quantum networks using the ideas we presented in [9].

2 The circuit of quantum repeaters can be understood in the stabilizer formalism

Before diving into the error analysis of the quantum repeater we motivate the circuit using the stabilizer formalism [19,12]. This language simplifies the multipartite generalization. Furthermore we think it is an aesthetic way of constructing and understanding the circuit.
A state $|\psi\rangle$ is said to be stabilized by an operator s if it

is an eigenstate of s to the eigenvalue $+1$, i.e.

$$s|\psi\rangle = |\psi\rangle. \tag{1}$$

The set of all operators that stabilize the state is called the stabilizer of the state. An n qubit state can be uniquely defined by n independent operators g_i, $i = 1, 2, ..., n$, that stabilize it. They generate the stabilizer of the state, i.e. the product of two stabilizer elements is contained in the stabilizer, too. Here we shortly call an element of the stabilizer, i.e. the operator, a stabilizer. No confusion should arise from this abbreviation.

2.1 The stabilizer of a maximally entangled state

Consider the maximally entangled state shared by parties A and B

$$|\bullet\!\!-\!\!\bullet\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|+\rangle_B + |1\rangle_A|-\rangle_B), \tag{2}$$

where $|0\rangle$ and $|1\rangle$ form the canonical basis of the Hilbert space of a single qubit and $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. The state $|\bullet\!\!-\!\!\bullet\rangle_{AB}$ is local unitary equivalent to any Bell pair in the standard notation,

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \tag{3}$$

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle), \tag{4}$$

$$|\phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \tag{5}$$

$$\text{and } |\phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \tag{6}$$

i.e. they are identical up to local basis changes. The state of Eq. (2) is stabilized by the two operators

$$g_A = X_A Z_B \text{ and } g_B = Z_A X_B. \tag{7}$$

Here

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ and } Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{8}$$

are Pauli matrices and the index denotes the party on which this operator acts.
Since g_A and g_B are independent, they uniquely define the state of Eq. (2). This implies that a repeater scheme is successful if the state produced by the repeater is stabilized by these operators.

2.2 Transformation of the stabilizer in a circuit

Suppose that s stabilizes the state $|\psi\rangle$ of a system on which now a (unitary) gate U acts. Then

$$UsU^\dagger U|\psi\rangle = U|\psi\rangle, \tag{9}$$

i.e. the operator $UsU^\dagger$ stabilizes the state after the operation of the gate. Because the stabilizer generators uniquely define the quantum state, keeping track of these operators during a quantum computation is equivalent to keeping track of the quantum state. And while it might seem to be more effort to write down and manipulate the set of stabilizer generators than two hold a single quantum state it can be much easier in special situations [19]. This is because the state space increases exponentially with the number of qubits. On the contrary the number of generators increases linearly with the number of qubits and the set of operators occurring as stabilizer generators can be very limited depending on the performed gates. For example it can be restricted to the Clifford group (see Gottesman-Knill-Theorem [12]). This will be the case for quantum repeaters.
We need the controlled-Phase gate

$$C_Z^{(i,j)} = |0\rangle_i\langle 0|_i \otimes \mathbb{1}_j + |1\rangle_i\langle 1|_i \otimes Z_j \tag{10}$$

that changes the phase of the second qubit if the first qubit is in state $|1\rangle$. Fig. 1 shows the circuit diagram symbol for a C_Z gate. C_X gates are defined analogously

(a) C_Z-gate (b) C_X-gate

Fig. 1 The circuit diagram symbols of common entangling gates.

to Eq. (10). These are equivalent to C_Z gates up to a local basis change on the second qubit.
The C_Z gate transforms the stabilizers $X_A\mathbb{1}_B$ and $\mathbb{1}_A X_B$ that correspond to the product state $|+\rangle_A|+\rangle_B$ into the stabilizers g_A and g_B. Thus it is an entangling gate.

2.3 Inserting and removing intermediate qubits

The idea of quantum repeaters is to counter the exponential losses in a fiber by cutting the long transmission line of length L into smaller parts of length L_0. The repeater stations connect these shorter channels. Intermediate qubits are inserted, entangled with their neighbors and measured. During this process some kind of error correction (using two-way or one-way communication) is performed. We now describe the basic scheme in the stabilizer formalism. The error correction will be discussed in Section 5. We also ignore the channel for now, since it is not important for understanding why the circuit produces a maximally entangled state. It is included in Section 4.
Suppose the total number of qubits N is even for simplicity. We sequentially number the qubits from A to B

by 1 to N, where 1 is the qubit of A and N is the one of B. We start with all qubits in the $|+\rangle$ state, i.e. the natural choice of stabilizer generators is $g_i = X_i$. Now neighboring qubits are entangled by C_Z gates. After application of the C_Z gates the list of stabilizers reads

$$\begin{aligned} g_1 =& X_1 Z_2, \\ g_N =& X_N Z_{N-1}, \\ \text{and } g_i =& Z_{i-1} X_i Z_{i+1} \text{ for } 1 < i < N. \end{aligned} \tag{11}$$

By multiplication of g_i with even and odd i we see that

$$S_A = X_1 X_3 X_5 ... X_{N-1} Z_N \tag{12}$$

$$\text{and } S_B = Z_1 X_2 X_4 X_6 ... X_N \tag{13}$$

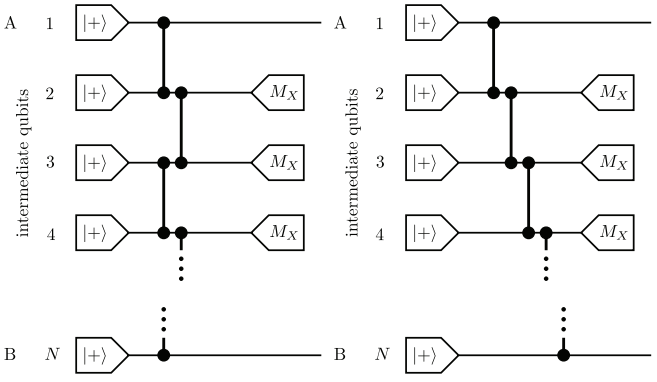
are two stabilizers of the state, respectively. We call these two stabilizers connecting A and B the main stabilizers, because they will play a central role in understanding the quantum repeater in the stabilizer formalism. In the multipartite case discussed at the end of this article, there will be one main stabilizer per party.

Now the intermediate qubits $(2, 3, ..., N-1)$ are measured in X basis, because this transforms the stabilizer in the desired way. We replace the corresponding operator in the stabilizer (see Eq. (11)) by the measurement outcome to obtain a stabilizer of the reduced state. The state of A and B after all measurements is stabilized by $\pi_A g_A = \pi_A X_A Z_B$ and $\pi_B g_B = \pi_B Z_A X_B$, where $\pi_A = \pm 1$ and $\pi_B = \pm 1$ are the parities of the measurement outcomes on odd and even qubits, respectively. One can correct for these measurement outcome dependent factors by applying so called by-product operators, here $X_A^{\pi_B} Z_A^{\pi_A}$. After this correction the state is stabilized by g_A and g_B as desired. Therefore the circuit that initializes all qubits in the $|+\rangle$ state, connects all neighboring qubits via C_Z gates and measures the intermediate qubits in the X-basis can be used to create a maximally entangled pair shared by A and B.

In the context of the original quantum repeater [3,1], the described procedure of projecting onto a bipartite entangled state is usually called entanglement swapping and the application of the by-product operators is called a correction of the "Pauli-frame".

Note that all the C_Z gates commute. Hence the order of these gates is irrelevant in the ideal case, but it becomes relevant when the error propagation is analyzed. There are mainly two orderings of the gates: sequentially and in two steps (e.g. first gates with odd labeled control qubits, then gates with even labelled control qubits). The two corresponding circuits are shown in Fig. 2. Apart from the error correction method quantum repeater schemes can also differ in the order of the gates and the position of the transmission channels inside the circuit.

The produced state given in Eq. 2 and the state stabilized by the generators given in Eq. (11) are examples of graph states [4,20]. It is possible to create and distribute every graph state in a similar way [9]. We describe this generalization in Section 7.



(a) Application of C_Z gates in two time-steps.

(b) Application of C_Z gates in $N-1$ time-steps.

Fig. 2 The basic circuit of quantum repeaters. Intermediate qubits are inserted and measured such that the state of A and B is projected onto a maximally entangled state. The two shown circuits are equivalent, because C_Z gates commute.

3 The error model of depolarizing noise

As a simple noise model we employ the depolarizing channel $\varepsilon_f(\rho)$ [19]. It depends on a parameter f which defines the strength of the noise. With probability f (for "failure") the state ρ is replaced by the completely mixed state $\mathbb{1}/d$, while it remains ρ with probability $(1-f)$, which leads to the state

$$\varepsilon_f(\rho) = (1-f)\rho + f\frac{\mathbb{1}}{d}, \tag{14}$$

where d is the dimension of the Hilbert space.

3.1 Error discretization

One can replace the identity term in Eq. (14) in the single qubit version using that

$$\frac{\mathbb{1}}{2} = \frac{\rho + X\rho X + XZ\rho ZX + Z\rho Z}{4}. \tag{15}$$

This leads to the form

$$\varepsilon_f(\rho) = (1-f)\rho + f\frac{\rho + X\rho X + XZ\rho ZX + Z\rho Z}{4}, \tag{16}$$

which has the following interpretation. With probability $(1-f)$ the channel acts as the ideal identity channel, while it "fails" with probability f. In case of failure there is a chance of $\frac{1}{2}$ for an X error to occur and an independent chance of $\frac{1}{2}$ for a Z error to occur.

The analogous relation to Eq. (15) for n qubits reads

$$\frac{\mathbb{1}}{2^n} = \frac{1}{4^n} \sum_{i_1, i_2, ..., i_n \in \{\mathbb{1}, X, XZ, Z\}} \bigotimes_{k=1}^{n} i_k \rho \bigotimes_{k=1}^{n} i_k^\dagger \tag{17}$$

and leads to the same error probabilities. We use this relation for the error discretization of n-qubit gates and in

particular for the C_Z gate. Thus the description of continuous noise has been replaced by a description in terms of randomly occurring discrete errors X and Z [19]. This formulation is convenient with respect to error propagation and the stabilizer formalism.

3.2 Description of erasure errors

We model erasures with the same error model, but in contrast to noise they are noticed in the sense that it is known which qubit is affected. We think of this as a third measurement outcome, a no-detection outcome, that we denote by a "?". Analogously to the unnoticed errors, the state of an erased qubit is replaced by the completely mixed state $\mathbb{1}/2$, i.e. it leads to X and Z errors from the viewpoint of discretized errors. The response of the elements of the circuit to erased qubits might strongly depend on the physical implementation and the error model can be improved for specific examples. Notice that this simple model possesses the main property in the context of entanglement distribution: If a qubit gets lost, then it cannot become correlated with any other qubit via a gate that processes them after the loss happened.

3.3 Error propagation by gates

Gates propagate errors, i.e. errors e before a gate are equivalent to possibly different errors e' after the gate [19]. Consider an arbitrary gate U. An error e before U corresponds to the overall action of Ue onto the state. Due to unitarity of U we can write

$$Ue = \underbrace{UeU^\dagger}_{e'} U = e'U, \tag{18}$$

i.e. the error is propagated to an $e' = UeU^\dagger$ error. Table 1 lists this relation for the most common cases.
Tracking the propagation of X and Z errors in a quantum circuit is a crucial part of the error analysis.

4 Physical errors in quantum repeater circuits

We first analyze the physical error rates of the circuit with a single qubit per station shown in Fig. 3, which, in contrast to Fig. 2, now includes the transmission channels. Section 4.3 treats an important variation of this circuit and the error correction is discussed in Section 5.
Any operation inside a circuit can cause an error. We use different indices to the symbol f to denote the failure rates of the corresponding process. These are preparation (f_P), transmission (f_T), gates (f_G) and measurement (f_M). We add another index u or n for unnoticed and noticed errors, respectively. Errors might be noticed by a non-detection event, i.e. no click in some time bin where we expected one. This gives the additional knowledge of the qubit on which this error occurred. Apart from that we treat these errors using the same model which we introduced in Section 3.

Table 1 Propagation of X and Z errors by the Hadamard- (H), controlled-Not- (C_X), and controlled-Phase-gate (C_Z). Here the index i with $i = 1, 2$ refers to the i-th qubit. Note that you can also read the stabilizer transformation $UsU^\dagger$ from this table.

$Ue = e'U$
$HX = ZH$
$HZ = XH$
$C_X X_1 = X_1 X_2 C_X$
$C_X Z_1 = Z_1 C_X$
$C_X X_2 = X_2 C_X$
$C_X Z_2 = Z_1 Z_2 C_X$
$C_Z X_1 = X_1 Z_2 C_Z$
$C_Z Z_1 = Z_1 C_Z$
$C_Z X_2 = Z_1 X_2 C_Z$
$C_Z Z_2 = Z_2 C_Z$

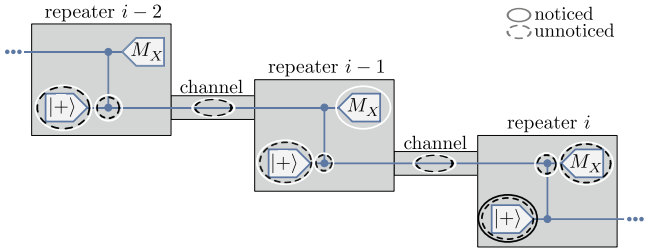


Fig. 3 A basic circuit for a quantum repeater with encoding. Errors at the encircled locations inside the circuit indicate possible causes for a flipped measurement outcome at repeater i, see text. Errors inside white (black) circles contribute to the noticed (unnoticed) error rate at station with number i. Solid (dashed) circles denote errors that are noticed (unnoticed).

Typical transmission losses have the form [11]

$$f_{T,n} = 1 - (1 - f_{C,n}) e^{-\frac{L_0}{L_{\text{att}}}}, \tag{19}$$

where $f_{C,n}$ describes coupling losses, $L_0 = \frac{L}{N-1}$ is the repeater spacing and $L_{\text{att}} \approx 20$ km gives the fiber attenuation.
To estimate the effective error rate of the measurement outcomes, we collect all sources of errors that affect the outcome of a specific measurement. An error on the measurement outcome remains, if an odd number of errors propagate from the source processes to the measurement, while an even number of errors cancels each other. We therefore introduce the functions

$$P_{\text{even}}(P, N) = \frac{1}{2}\left(1 + (1-2P)^N\right) \tag{20}$$

$$\text{and } P_{\text{odd}}(P, N) = \frac{1}{2}\left(1 - (1-2P)^N\right), \tag{21}$$

which denote the probability to have an even and odd number of events, respectively, in a sequence of N runs,

Table 2 All causes of unnoticed measurement errors at repeater i. The corresponding processes are marked by a black circle in Fig. 3.

probability	operator	site
$\frac{f_{P,u}}{2}$	X	Preparation of $i-2$
$\frac{f_{G,u}}{2}$	X	Gate of $i-2$
$\frac{f_{T,u}}{2}$	X	Channel from $i-2$ to $i-1$
$\frac{f_{P,u}}{2}$	Z	Preparation of $i-1$
$\frac{f_{G,u}}{2}$	Z	Gate of $i-1$
$\frac{f_{T,u}}{2}$	Z	Channel from $i-1$ to i
$\frac{f_{G,u}}{2}$	Z	Gate of i
$\frac{f_{M,u}}{2}$	Z	Measurement of i
$\frac{f_{P,u}+f_{P,n}}{2}$	X	Preparation of i
$\frac{f_{G,u}}{2}$	X	Gate of i

Table 3 All causes of noticed measurement errors at repeater i. The corresponding processes are marked by a white circle in Fig. 3.

probability	operator	site
$\frac{f_{P,n}}{2}$	X	Preparation of $i-2$
$\frac{f_{G,n}}{2}$	X	Gate of $i-2$
$\frac{f_{T,n}}{2}$	X	Channel from $i-2$ to $i-1$
$\frac{f_{M,n}}{2}$	Z	Measurement of $i-1$
$\frac{f_{P,n}}{2}$	Z	Preparation of $i-1$
$\frac{f_{G,n}}{2}$	Z	Gate of $i-1$
$\frac{f_{T,n}}{2}$	Z	Channel from $i-1$ to i
$\frac{f_{G,n}}{2}$	Z	Gate of i
$\frac{f_{M,n}}{2}$	Z	Measurement of i

where in each run the probability of the event is P. We generalize these formulas to the case where the probability of the event differs in each run. These probabilities are pooled into a vector $\mathbf{p}$ of dimension N and one can write

$$P_{\text{even}}(\mathbf{p}) = \sum_{\substack{n=0 \\ |n|_H \text{ even}}}^{2^N-1} \prod_{k=1}^{N} p_k^{n^{(k)}} (1-p_k)^{1-n^{(k)}} \quad (22)$$

$$\text{and } P_{\text{odd}}(\mathbf{p}) = \sum_{\substack{n=0 \\ |n|_H \text{ odd}}}^{2^N-1} \prod_{k=1}^{N} p_k^{n^{(k)}} (1-p_k)^{1-n^{(k)}}. \quad (23)$$

Here $|n|_H$ is the Hamming weight of n in binary representation and $n^{(k)}$ is the k-th binary digit of n. These definitions allow a compact notation for the exact error rate.

Consider the measurement on the repeater station i in Fig. 3. In total there are ten sources of errors for this measurement (circles in Fig. 3): three preparations, three gates, two channels and two measurements. Errors at positions in the circuit other than the shown ones cannot propagate to the measurement under consideration. We first focus on sources of an unnoticed error of the X-measurement on station i (black circles in Fig. 3). The measurement outcome is flipped by Z errors, as $Z|+\rangle = |-\rangle$ and $Z|-\rangle = |+\rangle$, but not by X errors as $X|+\rangle = |+\rangle$ and $X|-\rangle = -|-\rangle$. We give a complete list of error causes of an unnoticed error in Table 2. We exemplify the route of an error for the X-error occurring with probability $\frac{f_{P,u}}{2}$ in the preparation at $i-2$. It passes the gate of that station and the subsequent channel. At the repeater $i-1$ it propagates to an Z error on the qubit i, passes channel and gate and flips the measurement outcome.

Noticed errors on the qubit that is measured at station $i-1$ have a high probability of 50 % to lead to a flipped measurement outcome at site i. We thus choose to mark the outcome of that measurement as "?". In this way we exclude these noticed errors from the unnoticed error rate of i, which reads

$$\begin{aligned} f_u = & P_{\text{odd}}\left(\left(P_{\text{odd}}\left(\frac{f_{P,u}}{2},2\right), \frac{f_{P,n}+f_{P,u}}{2},\right.\right. \\ & \left.\left. P_{\text{odd}}\left(\frac{f_{G,u}}{2},3\right), P_{\text{odd}}\left(\frac{f_{T,u}}{2},2\right), \frac{f_{M,u}}{2}\right)\right). \end{aligned} \quad (24)$$

The full list of sources of noticed errors in the measurement at site i is given by Table 3 and in Fig. 3 white circles mark the corresponding positions in the circuit. The outcome is "?" if *any* of these errors occurred. This happens with probability

$$f_n = 1-(1-f_{P,n})^2(1-f_{G,n})^3(1-f_{T,n})^2(1-f_{M,n})^2. \quad (25)$$

4.1 How far do errors propagate?

On the first glance it might seem possible that errors propagate along the whole line of repeater stations to Bob. This is not the case. The measurement outcome on repeater i is only affected by errors on repeater stations $i-2$ to i. The C_Z gates propagate X to Z errors on the neighboring qubit. These do not propagate across C_Z gates. Thus only elements of the circuit that involve a neighboring qubit of the one measured in qubit i need to be considered. For a full error analysis all these sources need to be included. In particular, it is usually not exhaustive to consider only a single repeater station independently of the previous ones. One has to pay attention to such restrictions when comparing different repeater schemes from the literature.

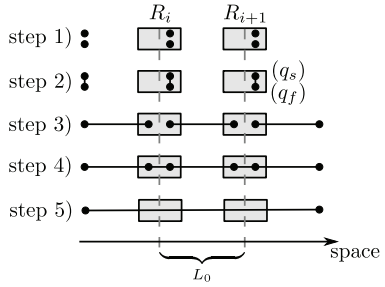
4.2 Bit flip errors caused by erasures

The effect of one lost qubit before the application of a two-qubit gate may strongly depend on the physical implementation of the gate. It is reasonable, however, to assume that there will be some unwanted effect on

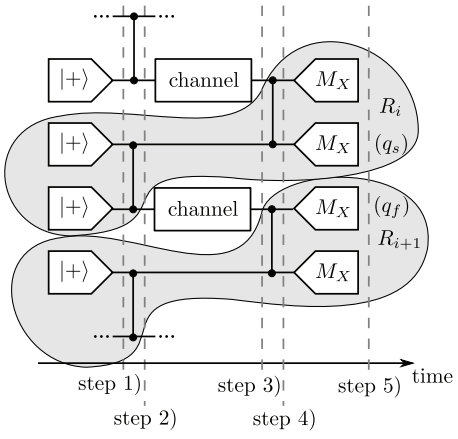
the remaining second qubit. In our error model the lost qubit is replaced by the completely mixed state, or equivalently, X and Z errors randomly occur at the position of the loss. These errors propagate across the two-qubit gates, possibly leading to flipped outcomes of measurements on these adjacent qubits. In this way losses in our model lead to noise on detected qubits.

4.3 Other circuits

An analogous error analysis can be done for other circuits, too. Here we discuss the error propagation in circuits where only half of the qubits are transmitted through the channel, while the other half remains stationary as another example. Fig. 4 shows a schematic of such a repeater and the corresponding circuit. Again we identify all sources of an flipped measurement outcome. The treatment of noticed errors differs for stationary and flying qubits, so we calculate two different error rates. The



(a) Spatial diagram



(b) Circuit diagram

Fig. 4 Schematic of a repeater with two qubits per station. Two repeaters R_i and R_{i+1} are shown in a spatial diagram (a) and the circuit diagram (b). Entangled pairs are created, distributed amongst neighboring repeater stations and then connected locally. In a last step local measurements project onto a two-qubit entangled state.

index s or f denotes stationary or flying qubits, respectively. The rates of unnoticed errors read

$$f_{q,s} = P_{\text{odd}}\left(\left(\frac{f_{P,u,f}}{2}, \frac{f_{G,u,f}}{2}, \frac{f_{T,u,f}}{2}, \frac{f_{P,u,s}}{2}, \frac{f_{G,u,s}}{2}, \frac{f_{G,u,s}}{2}, \frac{f_{M,u,s}}{2}, \frac{f_{P,u,f}+f_{P,n,f}}{2}\right)\right), \tag{26}$$

$$f_{q,f} = P_{\text{odd}}\left(\left(\frac{f_{P,u,s}+f_{P,n,s}}{2}, \frac{f_{P,u,f}}{2}, \frac{f_{T,u,f}}{2}, \frac{f_{G,u,f}}{2}, \frac{f_{M,u,f}}{2}, \frac{f_{P,u,s}+f_{P,n,s}}{2}, \frac{f_{G,u,s}+f_{G,n,s}}{2}\right)\right) \tag{27}$$

and the rates of noticed errors read

$$f_{l,s} = 1-(1-f_{P,n,f})(1-f_{G,n,f})(1-f_{T,n,f})\times \times(1-f_{M,n,f})(1-f_{P,n,s})(1-f_{G,n,s})(1-f_{M,n,s}) \tag{28}$$

$$f_{l,f} = 1-(1-f_{P,n,f})(1-f_{G,n,f})^2(1-f_{T,n,f})\times (1-f_{M,n,f}). \tag{29}$$

Note that, analogously to the other circuit, we choose to mark the stationary qubit as lost whenever the previous flying qubit got lost. This is not necessary but improves the error correction, as the stationary qubit has a high probability for errors in this case.

5 Logical error rates of encoded qubits

So far we considered the error rates on physical qubits. Quantum repeater with encoding use error correction codes [21,22,2,14] to encode the information of logical qubits into a larger number of physical qubits. The circuits discussed above are shifted to the logical level, i.e. the shown qubits and operations are now replaced by their logical counterparts. Before going into the details of the analysis of the logical errors we give a short reminder of Calderbank-Shor-Steane (CSS) codes [5,23].

5.1 Calderbank-Shor-Steane codes

Stabilizer codes can be defined via the generators of the stabilizer of the code space $g_1, ..., g_{n-k}$ (n and k are the numbers of physical and logical qubits, respectively) [**?**]. Valid codewords $|\psi\rangle$ satisfy $g_i|\psi\rangle = |\psi\rangle$. The logical $\bar{Z}_i$ operators, $i = 1, 2, ..., k$, are chosen such that they commute with and are independent from each other and the stabilizer generators. If the last are tensor products of either only X and $\mathbb{1}$ or only Z and $\mathbb{1}$, the code is called a CSS code. We give the popular example of the Seven-Qubit-Steane code in Table 4.

The transversal, i.e. qubitwise (see Fig. 5), application of controlled-NOT gates $C_X = |0\rangle\langle 0|\otimes\mathbb{1} + |1\rangle\langle 1|\otimes X$ performs the following mapping of the stabilizer generators.

Table 4 The stabilizer generators and logical operators of the Seven-Qubit-Steane code.

$$
\begin{aligned}
g_1 &= \mathbb{1} \otimes \mathbb{1} \otimes \mathbb{1} \otimes X \otimes X \otimes X \otimes X \\
g_2 &= \mathbb{1} \otimes X \otimes X \otimes \mathbb{1} \otimes \mathbb{1} \otimes X \otimes X \\
g_3 &= X \otimes \mathbb{1} \otimes X \otimes \mathbb{1} \otimes X \otimes \mathbb{1} \otimes X \\
g_4 &= \mathbb{1} \otimes \mathbb{1} \otimes \mathbb{1} \otimes Z \otimes Z \otimes Z \otimes Z \\
g_5 &= \mathbb{1} \otimes Z \otimes Z \otimes \mathbb{1} \otimes \mathbb{1} \otimes Z \otimes Z \\
g_6 &= Z \otimes \mathbb{1} \otimes Z \otimes \mathbb{1} \otimes Z \otimes \mathbb{1} \otimes Z \\
\bar{Z} &= Z \otimes Z \otimes Z \otimes Z \otimes Z \otimes Z \otimes Z \\
\bar{X} &= X \otimes X \otimes X \otimes X \otimes X \otimes X \otimes X
\end{aligned}
$$

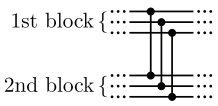


Fig. 5 Transversal implementation of a C_Z gate. The i-th gate acts on the i-th physical qubits of the first and second block.

If g_i contains only X operators, then $g_i \otimes \mathbb{1} \rightarrow g_i \otimes g_i$, $\mathbb{1} \otimes g_i \rightarrow \mathbb{1} \otimes g_i$, while a g_i containing Z operators is mapped according to $g_i \otimes \mathbb{1} \rightarrow g_i \otimes \mathbb{1}$ and $\mathbb{1} \otimes g_i \rightarrow g_i \otimes g_i$ (see Table 1). Thus transversal application of C_X is a valid gate in CSS codes, i.e. it preserves validity of the codeword.

The Seven-Qubit-Steane code and the quantum Golay code have even more symmetry: Exchanging X and Z operators in a stabilizer operator s leads to another element of the stabilizer s'. This implies that the transversal Hadamard gate is valid and hence also the transversal controlled-Phase gate C_Z (Fig. 5).

Transversal implementations of gates have advantageous error propagation properties: Because a single error on one block cannot lead to more than one error on the other block, these errors remain correctable after the application of the gate. If all gates are implemented transversally, then the physical error rates do not depend on the code or its size. Thus Eqs. (24) and (25) are true for all CSS codes.

5.2 Ideal measurement outcomes are codewords

The stabilizer generators that contain X correspond to the rows of the parity-check matrix of a (classical) linear block code. The classical parity-check matrix is obtained from the stabilizer generators by replacing a $\mathbb{1}$ by 0 and a X by 1 (and $\otimes$ by whitespace). The parity-check matrix H of a classical code can be used to check whether some word $\mathbf{c}$ is inside the code space, because $H\mathbf{c}^T = \mathbf{0}$ if and only if $\mathbf{c}$ is a codeword. In absence of any errors, the measurement of any stabilizer generator containing X operators gives a $+1$ result and, equivalently, the vector $\mathbf{c}$ of the individual X-measurements passes the parity check. That is, this vector of the X-measurement outcomes is a codeword of the associated classical linear block code.

5.3 Calculating the logical error rate

After the $\bar{X}$-measurement we are dealing with classical data. In the presence of imperfections, some of the bits will be flipped. Some values are marked as "?" due to a non-detection event. This data could have been generated by a classical channel with both bit flip and erasure errors. Thus a classical decoder can be used to find and correct the errors on the data.

Some loss patterns in the data are not likely to be corrected. In this case it can be beneficial to abort the protocol and throw away the data, i.e. rerun the experiment. This leads to a success probability of the protocol. If $\mathcal{F}$ is the set of fatal error patterns on which we choose to abort, then the success probability of the protocol is

$$P_{\text{succ}} = 1 - \sum_{e \in \mathcal{F}} P_{\text{e}}(e), \tag{30}$$

where $P_{\text{e}}(e)$ is the probability of the error pattern e. The impact of the choice of $\mathcal{F}$ on the performance of the protocol with respect to some figure of merit is discussed in Section 6.2.

If the protocol has not been aborted, then after decoding we are left with a valid codeword (but not necessarily the correct one), from which we can calculate the $\bar{X}$ outcome, which is the parity of the bits that contribute to $\bar{X}$ (i.e. the positions where $\bar{X}$ contains a $\mathbb{1}$ are excluded). The logical error rate $\bar{f}_u$ is the probability to arrive at the wrong $\bar{X}$ outcome when following the above procedure. Averaged over the logical qubits of one block we get

$$\bar{f}_u(f_u, f_n) = \frac{1}{k} \sum_{e \notin \mathcal{F}} f(e) P_{\text{e}}(e), \tag{31}$$

where $f(e)$ is the number of wrong logical outcomes in a single block. For small codes this can be easily calculated by trying the decoder on any possible error pattern. For larger codes this calculation cannot be done by "brute-force" anymore and more clever approaches are necessary.

We explicitly performed the sum in Eq. (31) for the Seven-Qubit-Steane code and the fatal error set

$$\mathcal{F} = \{e | e \text{ contains more than } n_{\max} \text{ losses}\} \tag{32}$$

for $n_{\max} = 1, 2, ..., 7$. The results are listed in Table 5. For larger codes, like the Golay code [15], the logical error rate can be taken from the literature [8]. There the probability p_w that the decoding outputs the wrong codeword is given. Half of the codewords have even and half have odd parity. We therefore assume that the probability of a logical error is $\bar{f}_u = \frac{p_w}{2}$.

Table 5 Logical error rates of the Steane code for different abortion strategies: $n_{\max}$ is the maximal number of tolerated losses before abortion.

$n_{\max} = 0$:

$$\begin{aligned}\bar{f}_u(f_u, f_n) &= (f_n-1)^7 f_u^2 \left(48f_u^5 - 168f_u^4 + 252f_u^3 - 210f_u^2 + 98f_u - 21\right)\\ P_{\text{succ}}(f_n) &= (1-f_n)^7\end{aligned}$$

$n_{\max} = 1$:

$$\begin{aligned}\bar{f}_u(f_u, f_n) &= (f_n-1)^6 f_u \left(48\left(f_n-1\right)f_u^6 - 168\left(f_n-1\right)f_u^5 + 252\left(f_n-1\right)f_u^4 - 210\left(f_n-1\right)f_u^3\right.\\ &\quad \left.+14\left(9f_n-7\right)f_u^2 + 21\left(1-3f_n\right)f_u + 21f_n\right)\\ P_{\text{succ}}(f_n) &= \left(f_n-1\right)^6\left(6f_n+1\right)\end{aligned}$$

$n_{\max} = 2$:

$$\begin{aligned}\bar{f}_u(f_u, f_n) &= \left(f_n-1\right)^5 f_u \left(48\left(f_n-1\right)^2 f_u^6 - 168\left(f_n-1\right)^2 f_u^5 + 252\left(f_n-1\right)^2 f_u^4 - 210\left(f_n-1\right)^2 f_u^3\right.\\ &\quad \left.+14\left(f_n\left(3f_n-16\right)+7\right)f_u^2 + 21\left(f_n\left(3f_n+4\right)-1\right)f_u - 21f_n\left(2f_n+1\right)\right)\\ P_{\text{succ}}(f_n) &= -\left(f_n-1\right)^5\left(15f_n^2+5f_n+1\right)\end{aligned}$$

$n_{\max} = 3$:

$$\begin{aligned}\bar{f}_u(f_u, f_n) &= \tfrac{1}{2}\left(f_n-1\right)^4\left(f_n^3\left(96f_u^7 - 336f_u^6 + 504f_u^5 - 420f_u^4 + 308f_u^3 - 210f_u^2 + 84f_u + 7\right)\right.\\ &\quad -2f_n^2 f_u\left(144f_u^6 - 504f_u^5 + 756f_u^4 - 630f_u^3 + 266f_u^2 - 21f_u - 21\right)\\ &\quad +2f_n f_u\left(144f_u^6 - 504f_u^5 + 756f_u^4 - 630f_u^3 + 322f_u^2 - 105f_u + 21\right)\\ &\quad \left.+2f_u^2\left(-48f_u^5 + 168f_u^4 - 252f_u^3 + 210f_u^2 - 98f_u + 21\right)\right)\\ P_{\text{succ}}(f_n) &= \left(f_n-1\right)^4\left(20f_n^3+10f_n^2+4f_n+1\right)\end{aligned}$$

$n_{\max} = 4$:

$$\begin{aligned}\bar{f}_u(f_u, f_n) &= \tfrac{1}{2}\left(f_n-1\right)^3\left(3f_n^4\left(32f_u^7 - 112f_u^6 + 168f_u^5 - 140f_u^4 + 84f_u^3 - 42f_u^2 + 14f_u - 7\right)\right.\\ &\quad -f_n^3\left(384f_u^7 - 1344f_u^6 + 2016f_u^5 - 1680f_u^4 + 840f_u^3 - 252f_u^2 + 42f_u + 7\right)\\ &\quad +12f_n^2 f_u^2\left(48f_u^5 - 168f_u^4 + 252f_u^3 - 210f_u^2 + 98f_u - 21\right)\\ &\quad -6f_n f_u\left(64f_u^6 - 224f_u^5 + 336f_u^4 - 280f_u^3 + 140f_u^2 - 42f_u + 7\right)\\ &\quad \left.+2f_u^2\left(48f_u^5 - 168f_u^4 + 252f_u^3 - 210f_u^2 + 98f_u - 21\right)\right)\\ P_{\text{succ}}(f_n) &= -15f_n^7 + 35f_n^6 - 21f_n^5 + 1\end{aligned}$$

$n_{\max} = 5$:

$$\begin{aligned}\bar{f}_u(f_u, f_n) &= \tfrac{1}{2}\left(f_n-1\right)^2\left(6f_n^5 f_u\left(16f_u^6 - 56f_u^5 + 84f_u^4 - 70f_u^3 + 42f_u^2 - 21f_u + 7\right)\right.\\ &\quad -2f_n^4\left(240f_u^7 - 840f_u^6 + 1260f_u^5 - 1050f_u^4 + 546f_u^3 - 189f_u^2 + 42f_u - 7\right)\\ &\quad +f_n^3\left(960f_u^7 - 3360f_u^6 + 5040f_u^5 - 4200f_u^4 + 2016f_u^3 - 504f_u^2 + 42f_u + 7\right)\\ &\quad -6f_n^2 f_u\left(160f_u^6 - 560f_u^5 + 840f_u^4 - 700f_u^3 + 336f_u^2 - 84f_u + 7\right)\\ &\quad +2f_n f_u\left(240f_u^6 - 840f_u^5 + 1260f_u^4 - 1050f_u^3 + 518f_u^2 - 147f_u + 21\right)\\ &\quad \left.+2f_u^2\left(-48f_u^5 + 168f_u^4 - 252f_u^3 + 210f_u^2 - 98f_u + 21\right)\right)\\ P_{\text{succ}}(f_n) &= 6f_n^7 - 7f_n^6 + 1\end{aligned}$$

$n_{\max} = 6$:

$$\begin{aligned}\bar{f}_u(f_u, f_n) &= f_n^7\left(48f_u^7 - 168f_u^6 + 252f_u^5 - 210f_u^4 + 126f_u^3 - 63f_u^2 + 21f_u - \tfrac{7}{2}\right)\\ &\quad -\tfrac{21}{2}f_n^6\left(2f_u-1\right)^3\left(4f_u^4 - 8f_u^3 + 6f_u^2 - 2f_u + 1\right)\\ &\quad +\tfrac{21}{2}f_n^5\left(2f_u-1\right)^3\left(12f_u^4 - 24f_u^3 + 18f_u^2 - 6f_u + 1\right)\\ &\quad -105f_n^4 f_u\left(2f_u-1\right)^3\left(2f_u^3 - 4f_u^2 + 3f_u - 1\right) + \tfrac{7}{2}f_n^3\left(2f_u-1\right)^3\left(60f_u^4 - 120f_u^3 + 90f_u^2 - 30f_u - 1\right)\\ &\quad -63f_n^2 f_u\left(2f_u-1\right)^3\left(2f_u^3 - 4f_u^2 + 3f_u - 1\right) + 21f_n f_u\left(2f_u-1\right)^3\left(2f_u^3 - 4f_u^2 + 3f_u - 1\right)\\ &\quad +f_u^2\left(-48f_u^5 + 168f_u^4 - 252f_u^3 + 210f_u^2 - 98f_u + 21\right)\\ P_{\text{succ}}(f_n) &= 1 - f_n^7\end{aligned}$$

$n_{\max} = 7$:

$$\begin{aligned}\bar{f}_u(f_u, f_n) &= 3f_n^7\left(2f_u-1\right)^3\left(2f_u^4 - 4f_u^3 + 3f_u^2 - f_u + 1\right) - \tfrac{21}{2}f_n^6\left(2f_u-1\right)^3\left(4f_u^4 - 8f_u^3 + 6f_u^2 - 2f_u + 1\right)\\ &\quad +\tfrac{21}{2}f_n^5\left(2f_u-1\right)^3\left(12f_u^4 - 24f_u^3 + 18f_u^2 - 6f_u + 1\right) - 105f_n^4 f_u\left(2f_u-1\right)^3\left(2f_u^3 - 4f_u^2 + 3f_u - 1\right)\\ &\quad +\tfrac{7}{2}f_n^3\left(2f_u-1\right)^3\left(60f_u^4 - 120f_u^3 + 90f_u^2 - 30f_u - 1\right) - 63f_n^2 f_u\left(2f_u-1\right)^3\left(2f_u^3 - 4f_u^2 + 3f_u - 1\right)\\ &\quad +21f_n f_u\left(2f_u-1\right)^3\left(2f_u^3 - 4f_u^2 + 3f_u - 1\right) + f_u^2\left(-48f_u^5 + 168f_u^4 - 252f_u^3 + 210f_u^2 - 98f_u + 21\right)\\ P_{\text{succ}}(f_n) &= 1\end{aligned}$$

6 The final state

We motivated in Section 2, that the described circuits produce a maximally entangled state and how this can be understood in the stabilizer formalism. The same reasoning still holds when the operators are shifted to the logical level. The logical state is stabilized by the logical stabilizers, which transform under the action of logical gates analogously to the physical stabilizers. Remember that the state before the measurements is stabilized by the main stabilizers S_A and S_B and thus after the $\bar{X}$-measurements it is stabilized by g_A and g_B up to byproduct operators. These byproduct operators depend on the measurement outcomes. They are necessary even in the ideal case, where all operations and measurements are perfect.

Odd numbers of logical errors on the same main stabi-

lizer lead to the wrong parity and thus to the application of the wrong byproduct operators, which implies that a state orthogonal to the intended state given in Eq. (2) is produced. We use the symbols e_A and e_B for the two corresponding error rates on the final state. They read

$$e_A = P_{\text{odd}}\left(\bar{f}_u, \left\lfloor \frac{N-2}{2} \right\rfloor\right) \tag{33}$$

$$\text{and } e_B = P_{\text{odd}}\left(\bar{f}_u, \left\lceil \frac{N-2}{2} \right\rceil\right), \tag{34}$$

and can be interpreted as X- and Z-error rates on qubit 1 of Alice. Thus the fidelity of the state is

$$F = (1-e_A)(1-e_B). \tag{35}$$

6.1 The secret fraction and the costs

A very important application of quantum repeaters is with respect to quantum key distribution. In this case one is not interested in the fidelity of the state but in the number of secret bits one can gain from many copies of the state in a quantum key distribution protocol. The ratio of secret bits per distributed entangled state is called secret fraction and in the standard BB84 protocol it is given by

$$r_\infty = \max\{1 - h(e_A) - h(e_B), 0\}, \tag{36}$$

where $h(p) = -p\log_2(p) - (1-p)\log_2(1-p)$ is the binary entropy. The secret key rate of a quantum repeater,

$$R_{\text{QKD}} = R_{\text{raw}} r_\infty, \tag{37}$$

is the product of the raw key generation rate R_{raw} and the secret fraction r_∞. If we set the probability of matching basis choice of Alice and Bob ("sifting") to 1, which is possible in the asymptotic case [**?**], then R_{raw} corresponds to the generation rate of entangled states. In a forward error correction scheme this repetition rate of the repeater is basically given by the fundamental time needed for processing the signal at a single repeater station and the success probability of the protocol. We assume that the speed of the operations is limited by the time T_M needed for the measurement at the repeater station. In this case

$$R_{\text{raw}} = \frac{P_{\text{succ}}}{T_M}. \tag{38}$$

For simplicity we will set the fundamental time T_M to 1 when considering forward error correction schemes only. In an attempt to do a fair comparison between repeater schemes with different codes, we use the cost function

$$C' = \frac{Nn}{R_{\text{QKD}} L} \tag{39}$$

as a figure of merit [18]. Here N is the number of encoded blocks, n is the number of physical qubits per block, R_{QKD} is the secret key rate and L is the total distance bridged by the line of repeater stations.

6.2 The impact of abortion strategies

In the previous sections we derived all the necessary formulas to compare different strategies of encoding. We start the discussion of this result by comparing different abortion strategies $\mathcal{F}$ for the simple Seven-Qubit-Steane code, see Table 4. It is based on the (7,4)-Hamming code, which has a Hamming distance of $d = 3$. This implies that it can correct $\frac{d-1}{2} = 1$ unnoticed errors or $d-1 = 2$ noticed errors.
More noticed errors are unlikely to be corrected and thus an abortion of the protocol will prevent the production of too noisy states. Abortion on two or less losses decreases the success probability unnecessarily. One might therefore expect, that $n_{\max} = 2$ gives the optimal fatal error set $\mathcal{F}$. Fig. 6 supports these considerations.

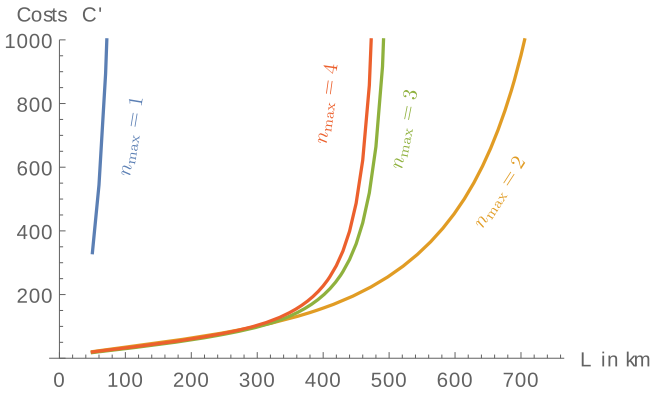


Fig. 6 The cost of the repeater using the Seven-Qubit-Steane code for different abortion strategies. The number $n_{\max}$ denotes the maximal number of tolerated losses. The gate failure rate is $f_G = 10^{-4}$ for this plot.

6.3 The distillation based protocol

We compare the costs of repeaters with encoding to the standard repeater with two-way communication using the results of [1]. There the repeater rate is calculated (amongst others) for the following setup. The total distance is divided into $2^{\tilde{N}}$ shorter channels of length $L_0 = L/2^{\tilde{N}}$ by repeater stations. Initially $2^{\tilde{k}}$, $\tilde{k} \in \mathbb{N}\cup\{0\}$ entangled states of fidelity F_0 w.r.t. some maximally entangled state are distributed amongst neighboring repeater stations. Here two-way classical communication is necessary in order to acknowledge success of the distribution. After k rounds of distillation using the protocol of [6] for each channel a single pair with higher fidelity is left (if the initial fidelity is greater than $\frac{1}{2}$). Afterwards a Bell measurement on each repeater station projects onto the final entangled state shared by Alice and Bob.
The rate R^O_{QKD} is (to some extent) limited by the classical communication time which is necessary to acknowledge the successful transmission and distillation. For the

two-way protocol we incorporate the measurement time T_M by adjusting the time needed to distribute a Bell pair amongst two neighboring qubits to

$$T_0 = \frac{\beta L_0}{c} + T_M, \tag{40}$$

where β is a factor depending on the position of the source which we choose to be 1 and $c = 2 \times 10^5$ is the speed of light in the fiber. Apart from this change we use the formulas derived in [**?**]. The total amount of qubits is $2^{\tilde{N}+\tilde{k}+1}$. Hence the costs of the original repeater read

$$C' = \frac{2^{\tilde{N}+\tilde{k}+1}}{R^O_{QKD} L}. \tag{41}$$

In the considered parameter regime the rate does not double when using distillation. It therefore never pays off to perform distillation with respect to the cost function C', i.e. we set $\tilde{k} = 0$. In our calculation we assume

$$F_0 = 1 - \frac{3}{4} f_G. \tag{42}$$

This fidelity is obtained when using a gate to produce the initial Bell pair. Fig. 7 shows the cost comparison for a gate failure rate of $f_G = 10^{-3}$ and three different measurement times $T_M = 1\ \mu\text{s}, 10\ \mu\text{s}, 100\ \mu\text{s}$.
One immediately sees that the costs of the one-way repeater scheme are proportional to the measurement time T_M. This is clear from the fact that this time is the only limiting factor in the repetition rate of this repeater. For the two-way repeater this is not the case. Decreasing the measurement time below approximately ten microseconds does not improve the costs, because then the communication time dominates the fundamental time (see Eq. (40)) and becomes the limiting factor of the rate.

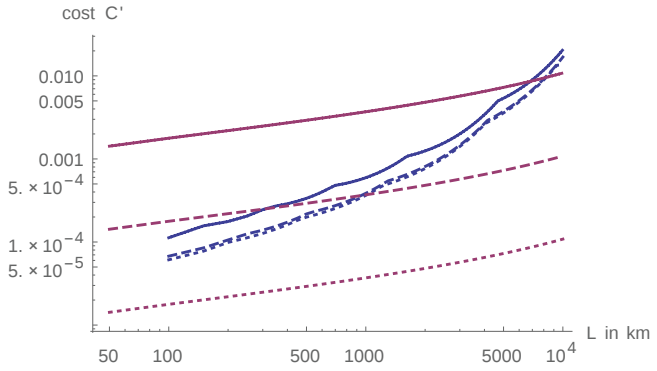


Fig. 7 The costs C' (in qubit seconds per bit and kilometer) of the standard repeater (blue) and for the one with Golay code (purple) as a function of the total distance L. The gate errors are $f_G = 10^{-3}$, other errors are neglected. The measurement time is $T_M = 1\ \mu$s (dotted), $T_M = 10\ \mu$s (dashed), and $T_M = 100\ \mu$s (solid).

The sharp bends in the cost curve for the original repeater are due to the fact that [1] considers only powers of two for the number of divisions of the transmission line. The straight line of the cost curve for the one-way repeater (over a large range of distances) shows that the costs per kilometer of this repeater using the Golay code increases polynomially with the total distance.

6.4 On the quality of some approximations

In the present paper we described the exact error analysis, mainly because the function P_{odd} gives a convenient description of combined error rates. It is more readable than the evaluated polynomials, while the computational complexity is not an issue here. Nevertheless forward error correction requires a very low probability of operational errors of $\lesssim 10^{-2}$ in order for the processing of the qubits not to introduce more errors than are correctable. And thus it is reasonable to approximate the derived formulas for small error rates. On the other hand one usually considers the highest error rate that still allows to produce a secret key. This is the most interesting regime from a practical point of view due to the strong limitations of current technology. A similar effect arises from the use of the cost function as a figure of merit which punishes the use of resources and rewards e.g. higher losses in between the stations to some extent. Thus a critical verification of the accuracy of these approximations is advisable.
The first order estimates of P_{odd}(see Eqs. (21) and (23)) are

$$P_{\text{odd}}(P, N) = NP + \mathcal{O}(P^2) \tag{43}$$

$$\text{and} \qquad P_{\text{odd}}(\mathbf{p}) = \sum_i (\mathbf{p})_i + \mathcal{O}((\mathbf{p})_i^2). \tag{44}$$

With these and $1 - (1-f)^N \approx Nf$ for small f we find that (see Eqs. (24) and (25))

$$f_u \approx \frac{3}{2} f_{P,u} + \frac{1}{2} f_{P,n} + \frac{3}{2} f_{G,u} + f_{T,u} + \frac{1}{2} f_{M,u} \tag{45}$$

$$\text{and } f_n \approx 2 f_{P,n} + 3 f_{G,n} + 2 f_{T,n} + 2 f_{M,n}. \tag{46}$$

Because operational errors are small ($\lesssim 10^{-2}$), the second order contributions are even smaller and Eq. (45) seems to be a good approximation. The losses however are typically bigger than ten percent (for repeater separations of $\gtrsim 1$ km, see Eq. (19)) so Eq. (46) turns out to be a bad approximation, because second order contributions are not neglectable.
We use the Golay code to exemplify how the small inaccuracy of Eq. (45) may become significant when the operational errors are near the maximally tolerable value in some situation and the number of repeater stations is large. Using the logical error rate given in Eq (50) one can calculate the cost C'. For a total distance of

(a) A mathematical graph.

(b) The line graph with six vertices.

Fig. 8 Examples of graphs.

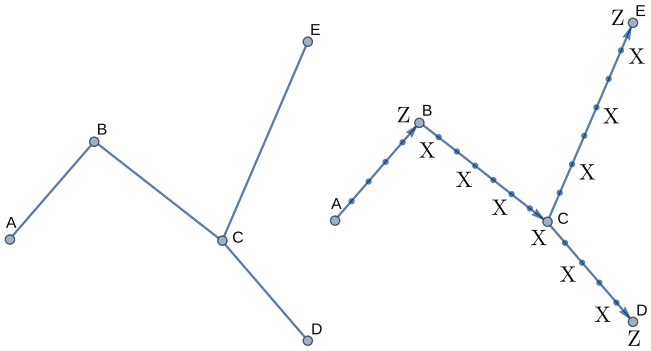
$L = 600$ km, a gate error rate of $f_G = 5 \times 10^{-3}$ and $w = 1500$ repeater stations it is $C' \approx 3464$ using Eq. (24) while it evaluates to $C' \approx 6500$ using the approximation of Eq. (45). The discrepancy becomes even more obvious for slightly larger repeater separations. Setting $w = 1400$ now $C' \approx 23448$ according to Eq. (24) while Eq. (45) leads to a zero secret key rate (i.e. infinite costs).

7 Generalization to the multipartite scenario

We described in Section 2 how the production of the final state can be understood in the stabilizer formalism. Measurements of the operators of the main stabilizers located on the intermediate qubits (i.e. all except the two of the parties) reduces the stabilizers to the stabilizers of the final state up to by-product operators. This procedure can be easily transferred to general graph states. We remind the reader that they are quantum states associated with mathematical graphs [4,20]. A Graph $G = (V, E)$ consists of a set of vertices V and a set of edges $E \subset V \times V$, see Fig. 8 (a) for an example. We denote the number of vertices ($|V|$) by N.
The corresponding quantum state is the one stabilized by

$$g_i = X_i \prod_{\substack{j \\ (i,j)\in E}} Z_j, \tag{47}$$

for all $i \in V$. One can arrive at these stabilizers by starting from $g_i = X_i$ (i.e. the state $|+\rangle^{\otimes N}$) and applying a C_Z gate from qubit i to qubit j for all qubits $i < j$ with $(i, j) \in E$ (see Table 1), i.e. for all edges in the graph. We thus note that the repeater circuit discussed in the previous sections (see Fig. 2) creates a graph state where $E = \{(i, i + 1)|1 \leq i < N\}$. We call this graph a line graph (not to be confused with the line graph of a graph, i.e. the graph where vertices and edges exchange their role), see Fig. 8 (b).
Now the production/distribution of a general graph state is straight forward. To design the repeater network we start from the final graph and insert intermediate vertices for the repeater stations (see Fig.9). We insert an even number of repeater stations w_{ij} on each edge $(i, j) \in E$, for simplicity. In analogy to the bipartite case the main stabilizer centered on some party is obtained by multiplication of the graph state generators centered on every second qubit until the neighboring parties are reached



(a) The final graph state.

(b) The main stabilizer centered on C.

Fig. 9 Example of a network of parties A to E.

(with a Z-operator), see Fig. 9 (b). On the added vertices the main stabilizer have the form of chains of X-operators (see also [24]). This ensures that the main stabilizers are transformed into the stabilizer generators g_i of the final graph state by X-measurements on the repeater stations, i.e. the corresponding graph state is produced. The circuit is obtained again by noting that each edge of the graph corresponds to a C_Z gate.
While the circuit of the repeater stations do not change compared to the bipartite case, the parties now apply more gates depending on the degree of their vertex (i.e. the number of edges at this position). Usually the number of repeater stations is much bigger than the number of parties for the error correction based scheme. One might therefore neglect the impact of the additional gates. Nevertheless they can be easily incorporated in Eqs. (24) and (25) which become

$$\begin{aligned} f_{i,u} =& P_{\text{odd}}\Bigg(\Bigg(P_{\text{odd}}\left(\frac{f_{P,u}}{2}, 1+\deg^-(i)\right), \\ & P_{\text{odd}}\left(\frac{f_{P,n}+f_{P,u}}{2}, \deg^+(i)\right), \\ & P_{\text{odd}}\left(\frac{f_{G,u}}{2}, 1+\deg(i)\right), \\ & P_{\text{odd}}\left(\frac{f_{T,u}}{2}, 1+\deg^-(i)\right), \frac{f_{M,u}}{2}\Bigg)\Bigg) \end{aligned} \tag{48}$$

and

$$\begin{aligned} f_{i,n} =& 1-(1-f_{P,n})^{1+\deg^-(i)}(1-f_{G,n})^{1+\deg(i)} \\ & (1-f_{T,n})^{1+\deg^-(i)}(1-f_{M,n})^{1+\deg^-(i)}, \end{aligned} \tag{49}$$

where $\deg(i)$, $\deg^-(i)$, and $\deg^+(i)$ are the degree, in-degree, and out-degree of vertex i, respectively. Here the direction of the edges corresponds to the direction of the transmission.
Note that local unitariy equivalence of graph states can be used to simplify the state distribution.

8 Conclusions

We described how quantum repeaters can be understood in the stabilizer formalism and how this formulation naturally leads to the description of general repeater networks. Analyzing the error propagation in the circuit diagram leads to the error rates of the (physical) measurements on the repeater stations. To this end we identified all errors that may flip the measurement outcome at a specific repeater station in this circuit. It turns out that up to three repeater stations have to be considered in this calculation.

We calculated the secret key rate for a general CSS code given its logical error rate and exemplified this calculation with the Seven-Qubit-Steane code and the quantum Golay code. The comparison with the original quantum repeater scheme shows that the quantum Golay code is particularly resource efficient for large distances (and short measurement times of $\lesssim 10\ \mu$s).

We investigated the quality of approximations of the physical error rates to the first order of the failure rates of the circuit elements (like gates) and found that these can be inaccurate in case of many repeater stations.

The repeater rate strongly depends on the abortion strategy, i.e. the set of error patterns on which one chooses to abort and restart the protocol. It is reasonable to abort on d and more losses, where d is the code distance.

References

1. Silvestre Abruzzo, Sylvia Bratzik, Nadja K. Bernardes, Hermann Kampermann, Peter van Loock, and Dagmar Bruß. Quantum repeaters and quantum key distribution: Analysis of secret-key rates. *Phys. Rev. A*, 87:052315, May 2013.
2. Charles H. Bennett, David P. DiVincenzo, John A. Smolin, and William K. Wootters. Mixed-state entanglement and quantum error correction. *Phys. Rev. A*, 54:3824–3851, Nov 1996.
3. H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller. Quantum repeaters: The role of imperfect local operations in quantum communication. *Phys. Rev. Lett.*, 81:5932–5935, Dec 1998.
4. Hans J. Briegel and Robert Raussendorf. Persistent entanglement in arrays of interacting particles. *Phys. Rev. Lett.*, 86:910–913, Jan 2001.
5. A. R. Calderbank and Peter W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, 54:1098–1105, Aug 1996.
6. David Deutsch, Artur Ekert, Richard Jozsa, Chiara Macchiavello, Sandu Popescu, and Anna Sanpera. Quantum privacy amplification and the security of quantum cryptography over noisy channels. *Phys. Rev. Lett.*, 77:2818–2821, Sep 1996.
7. W. Dür, H. Aschauer, and H.-J. Briegel. Multiparticle entanglement purification for graph states. *Phys. Rev. Lett.*, 91:107903, Sep 2003.
8. M. Elia and G. Taricco. A decoding algorithm for the (23, 12, 7) golay code with error and erasure correction. *Annales Des Telecommunications*, 50(9-10):721–731, 1995.
9. M. Epping, H. Kampermann, and D. Bruß. Graph State Quantum Repeater Networks. *ArXiv e-prints*, April 2015.
10. Austin G. Fowler, David S. Wang, Charles D. Hill, Thaddeus D. Ladd, Rodney Van Meter, and Lloyd C. L. Hollenberg. Surface code quantum communication. *Phys. Rev. Lett.*, 104:180503, May 2010.
11. Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Rev. Mod. Phys.*, 74:145–195, Mar 2002.
12. D. Gottesman. *Stabilizer codes and quantum error correction*. PhD thesis, California Institute of Technology, 1997.
13. Liang Jiang, J. M. Taylor, Kae Nemoto, W. J. Munro, Rodney Van Meter, and M. D. Lukin. Quantum repeater with encoding. *Phys. Rev. A*, 79:032325, Mar 2009.
14. Emanuel Knill, Raymond Laflamme, and Lorenza Viola. Theory of quantum error correction for general noise. *Phys. Rev. Lett.*, 84:2525–2528, Mar 2000.
15. F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland Publishing Company, 2nd edition, 1978.
16. W.J. Munro, K.A. Harrison, A.M. Stephens, S.J. Devitt, and K. Nemoto. From quantum multiplexing to high-performance quantum networking. *Nat. Phot.*, 4:792, 2010.
17. W.J. Munro, A.M. Stephens, S.J. Devitt, K.A. Harrison, and K. Nemoto. Quantum communication without the necessity of quantum memories. *Nat. Phot.*, 6:777–781, 2012.
18. Sreraman Muralidharan, Jungsang Kim, Norbert Lütkenhaus, Mikhail D. Lukin, and Liang Jiang. Ultrafast and fault-tolerant quantum communication across long distances. *Phys. Rev. Lett.*, 112:250501, Jun 2014.
19. M.A. Nielsen and I.L. Chuang. *Quantum Computation and Quantum Information*. Cambridge Series on Information and the Natural Sciences. Cambridge University Press, 2000.
20. D. Schlingemann and R. F. Werner. Quantum error-correcting codes associated with graphs. *Phys. Rev. A*, 65:012308, Dec 2001.
21. P.W. Shor. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A*, 52:R2493–R2496, Oct 1995.
22. A. M. Steane. Error correcting codes in quantum theory. *Phys. Rev. Lett.*, 77:793–797, Jul 1996.
23. Andrew Steane. Multiple-particle interference and quantum error correction. *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 452(1954):2551–2577, 1996.
24. J.-Y. Wu, H. Kampermann, and D. Bruß. X-chains reveal substructures of graph states. *ArXiv e-prints*, April 2015.

A The logical error rate of the Golay code

We give the logical error rate of the decoder by M. Elia and G. Taricco [8] for completeness. This decoder does not abort, so $P_{\mathrm{succ}} = 1$. Note that we assume $\bar{f}_q \approx \frac{p_w}{2}$, where p_w is the word error rate.

$$
\begin{aligned}
\bar{f}_u(f_u, f_n) =& \frac{1}{2}\Bigg(-\frac{f_n^{23}}{4096} + \frac{23\,(f_n+f_u-1)\,f_n^{22}}{2048} - \frac{253\,(f_n+f_u-1)^{\,2} f_n^{21}}{1024} + \frac{1771}{512}\,(f_n+f_u-1)^{\,3} f_n^{20} - \frac{8855}{256}\,(f_n+f_u-1)^{\,4} f_n^{19} \\
&+ \frac{33649}{128}\,(f_n+f_u-1)^{\,5} f_n^{18} - \frac{100947}{64}\,(f_n+f_u-1)^{\,6} f_n^{17} + \frac{245157}{32}\,(f_n+f_u-1)^{\,7} f_n^{16} - 30613\,(f_n+f_u-1)^{\,8} f_n^{15} \\
&- \frac{253}{16}\,(f_n-1)\,(f_n+f_u-1)^{\,7} f_n^{15} + 101200\,(f_n+f_u-1)^{\,9} f_n^{14} \\
&+ \frac{3795}{8}\,(f_n-1)\,(f_n+f_u-1)^{\,8} f_n^{14} - 272734\,(f_n+f_u-1)^{\,10} f_n^{13} - \frac{26565}{4}\,(f_n-1)\,(f_n+f_u-1)^{\,9} f_n^{13} \\
&+ 560924\,(f_n+f_u-1)^{\,11} f_n^{12} + \frac{115115}{2}\,(f_n-1)\,(f_n+f_u-1)^{\,10} f_n^{12} - 695520\,(f_n+f_u-1)^{\,12} f_n^{11} \\
&- 319424\,(f_n-1)\,(f_n+f_u-1)^{\,11} f_n^{11} + \frac{8855}{2}\,(f_n+f_u-1)^{\,11}\,(-f_n+2f_u+1)\,f_n^{11} \\
&+ 949256\,(f_n-1)\,(f_n+f_u-1)^{\,12} f_n^{10} - 97405\,(f_n+f_u-1)^{\,12}\,(-f_n+2f_u+1)\,f_n^{10} \\
&+ 779240\,(f_n+f_u-1)^{\,13}\,(-f_n+2f_u+1)\,f_n^{9} + 18975\,(f_n+f_u-1)^{\,13}\,(-f_n+6f_u+1)\,f_n^{9} \\
&- 485760\,(f_n+f_u-1)^{\,14}\,(-f_n+6f_u+1)\,f_n^{8} - 2277\,(f_n+f_u-1)^{\,14}\,(-f_n+14f_u+1)\,f_n^{8} \\
&+ 32384\,(f_n+f_u-1)^{\,15}\,(-f_n+14f_u+1)\,f_n^{7} + \frac{253}{2}\,(f_n-1)\,(f_n+f_u-1)^{\,14}\,(-f_n+14f_u+1)\,f_n^{7} \\
&+ 212520\,(f_n+f_u-1)^{\,14}\left(-(f_n-1)^{\,2} + 10f_u\,(f_n-1) + 8f_u^2\right) f_n^{7} \\
&- 100947\,(f_n-1)\,(f_n+f_u-1)^{\,15}\,(-f_n+14f_u+1)\,f_n^{6} \\
&- 28336\,(f_n+f_u-1)^{\,16}\,(-f_n+2f_u+1)\,(-f_n+14f_u+1)\,f_n^{5} \\
&- 5313\,(f_n+f_u-1)^{\,16}\left((f_n-1)^{\,2} - 15f_u\,(f_n-1) + 30f_u^2\right) f_n^{5} \\
&+ 8855\,(f_n+f_u-1)^{\,17}\left((f_n-1)^{\,2} - 17f_u\,(f_n-1) + 90f_u^2\right) f_n^{4} \\
&- 1771\,(f_n+f_u-1)^{\,17}\left((f_n-1)^{\,3} - 17f_u\,(f_n-1)^{\,2} + 138f_u^2\,(f_n-1) + 96f_u^3\right) f_n^{3} \\
&- 253\,(f_n+f_u-1)^{\,18}\left(-(f_n-1)^{\,3} + 18f_u\,(f_n-1)^{\,2} - 171f_u^2\,(f_n-1) + 90f_u^3\right) f_n^{2} \\
&+ 23\,(f_n+f_u-1)^{\,19}\left(-(f_n-1)^{\,3} + 19f_u\,(f_n-1)^{\,2} - 190f_u^2\,(f_n-1) + 560f_u^3\right) f_n + (f_n+f_u-1)^{\,23} \\
&-23f_u\,(f_n+f_u-1)^{\,22} + 253f_u^2\,(f_n+f_u-1)^{\,21} - 1771f_u^3\,(f_n+f_u-1)^{\,20} + 1\Bigg)
\end{aligned}
\tag{50}
$$