Non-adaptive measurement-based quantum computation and multi-party Bell inequalities

Matty J Hoban\textsuperscript{1,5}, Earl T Campbell\textsuperscript{1,2}, Klearchos Loukopoulos\textsuperscript{3} and Dan E Browne\textsuperscript{1,4}

\textsuperscript{1} Department of Physics and Astronomy, University College London, Gower Street, London WC1E 6BT, UK
\textsuperscript{2} Institute of Physics and Astronomy, University of Potsdam, 14476 Potsdam, Germany
\textsuperscript{3} Department of Materials, Oxford University, Parks Road, Oxford OX1 4PH, UK
\textsuperscript{4} Centre for Quantum Technologies, National University of Singapore, Singapore 117543, Singapore
E-mail: m.hoban@ucl.ac.uk

New Journal of Physics 13 (2011) 023014 (18pp)
Received 27 September 2010
Published 3 February 2011
Online at http://www.njp.org/
doi:10.1088/1367-2630/13/2/023014

Abstract. Quantum correlations exhibit behaviour that cannot be resolved with a local hidden variable picture of the world. In quantum information, they are also used as resources for information processing tasks, such as measurement-based quantum computation (MQC). In MQC, universal quantum computation can be achieved via adaptive measurements on a suitable entangled resource state. In this paper, we look at a version of MQC in which we remove the adaptivity of measurements and aim to understand what computational abilities remain in the resource. We show that there are explicit connections between this model of computation and the question of non-classicality in quantum correlations. We demonstrate this by focusing on deterministic computation of Boolean functions, in which natural generalizations of the Greenberger–Horne–Zeilinger paradox emerge; we then explore probabilistic computation via, which multipartite Bell inequalities can be defined. We use this correspondence to define families of multi-party Bell inequalities, which we show to have a number of interesting contrasting properties.

\footnotesize{\textsuperscript{5} Author to whom any correspondence should be addressed.}
1. Introduction

Space-like separated measurements on entangled quantum systems can reveal correlations that would not appear if Nature were described by a local hidden variable (LHV) theory [1]. Such correlations can violate a Bell inequality, a condition expressing a restriction on the correlations permitted in any LHV theory. Violations of Bell inequalities provide a dramatic distinction between locally realistic classical physics and quantum mechanics.

The field of quantum information processing has developed with the aim of exploiting the non-classical properties of quantum systems for practical tasks. Non-classical (i.e. Bell inequality violating) correlations are an important quantum resource in several areas of quantum information. For example, they can be used to guarantee the security of quantum key distribution [2] even if the devices used cannot be trusted; in distributed computational tasks, non-classical correlations can reduce the communication required between parties [3, 4]. One of the most renowned applications of quantum mechanics to information processing is quantum computation. We know that a quantum computer, if realized, would permit efficient solutions to problems for which no efficient classical algorithm is known [5]. Despite the importance of entanglement in quantum computation and despite its evident non-classical nature, the link between Bell inequality violations and quantum computational speed-up remains unclear. Recently, however, it was shown [6, 7] that Bell inequalities do have a concrete connection with a particular model of quantum computation, measurement-based quantum computation (MQC).

MQC is a model of quantum computation, very different from the standard unitary circuit model. Computation progresses in two stages. First a many-particle entangled state is prepared, e.g. the cluster state [8], and then single-site (qubit) measurements are carried out. By an appropriate choice of measurement bases, any quantum computation can be realized in this model on a cluster state of sufficient size [8].

In all schemes of MQC that have been proposed so far (e.g. [9, 10]), measurement bases need to be adaptive. Adaptive measurements are carried out in a certain order, and each measurement basis is chosen depending on the outcome of the measurements that came before it. A vital component of MQC schemes, which is sometimes overlooked, is the classical computer, which records measurement outcomes and determines [8] the bases of future measurements. The adaptivity imposes a temporal structure on the computation, and adds
the requirement for fast-switching of measurement bases in any experimental implementation. It is therefore worthwhile considering whether MQC without adaptive measurements is possible, and if it is, what range (and complexity) of computations it can achieve. This would present significant practical advantages since the quantum coherence and entanglement would only need to exist for a vanishingly small time, since all measurements could be carried out simultaneously. Recently, some progress was made in characterizing the power of non-adaptive MQC, and it was shown [11] that one can implement efficiently any computation in the complexity class IQP (a model known as instantaneous quantum computation) [12]. There is evidence [13] that IQP may contain algorithms with a quantum speed-up; however, no concrete example is as yet known.

An interesting fact about the adaptivity in Raussendorf and Briegel’s MQC scheme [10] is that the side processing needed to implement the adaptivity does not require a universal classical computer. It suffices for the computations to be implemented solely by exclusive OR (XOR) gates. In other words, such computations are linear Boolean functions [6]. This motivated Anders and Browne to consider the minimal (in the sense of the number of qubits) quantum correlations capable of enabling universal classical computation with a linear side processor. Surprisingly they discovered that the correlations required are those that define both the Clauser–Horne–Shimony–Holt (CHSH) inequality [14] and the Greenberger–Horne–Zeilinger (GHZ) paradox [15].

There are a number of superficial similarities between experiments that aim to produce a Bell inequality violation and MQC. In both cases, the initialization of the experiment consists of the generation of an entangled state; the experiment then proceeds by the measurement of individual subsystems (usually qubits) in one of a range of bases. However, there is also an important distinction. In Bell inequality experiments, measurements must be space-like separated, whereas in MQC, adaptivity precludes this. In this paper, therefore, we shall restrict our focus to non-adaptive MQC, where this conflict does not arise.

Since non-adaptive MQC with linear side-processing will play a central role in this paper, it is worthwhile introducing a shorthand to refer to it. We therefore define the model of non-adaptive measurement-based quantum computation with linear side-processing (NMQC⊕). This is the standard MQC model with two key restrictions: measurements are non-adaptive and the classical side processor responsible for pre- and post-processing of data is limited to linear functions alone. The model of NMQC⊕ is represented schematically in figure 1. In this paper, we study the range of computations that can be achieved within NMQC⊕ both deterministically and non-deterministically and study the Bell inequalities that these computational tasks define. The importance of restricting the side computation to linear functions is that we can study classical computations (which we will always describe in terms of Boolean functions) in the NMQC⊕ model.

It has already been shown, by Raussendorf [7], that general nonlinear Boolean functions may be achieved in a model equivalent to NMQC⊕, and each of these can be seen as a particular multi-qubit generalization of a GHZ paradox. GHZ paradoxes can be thought of as representing special cases of Bell inequality violations in the many-party setting. We show here that a broad class of natural multi-party generalizations of the CHSH inequality, where measurements are restricted to two settings and two outcomes, can be cast (as computational non-locality ‘games’) directly in the NMQC⊕ framework. Doing so immediately provides new structures for the classification of Bell inequalities and allows us to derive the general properties of n-party families of Bell inequalities true for all n.
Although the connection between MQC and Bell inequalities was recently made, there is a long tradition of viewing Bell inequalities as information theoretic tasks, for example in the context of quantum games [16, 17]. This approach is to frame the Bell inequality experiment in terms of the achievement of a certain task by a set of players, who are given certain resources and who must abide by certain rules. In Bell inequality games, the players represent the physicists making the measurements. The rules of the game include the requirement that these players do not communicate during the task (or be space-like separated) and the resource might be an entangled quantum state shared between players. In the context of Bell inequalities, we compare two kinds of resources available to the players. Players with access to only classical resources represent the behaviour found in LHV theories, whereas players with access to entangled states represent quantum behaviours. When a quantum player beats a classical one in a certain game (usually by achieving a higher mean success probability in a repeated task), this represents the violation of a Bell inequality. The quantum games approach to Bell inequalities has been very successful and, in particular, the family of XOR games, generalizations of the CHSH inequality, where the players encode the output of their task in the parity of the bits that they produce, are well characterized and understood [16].

Here we show that NMQC⊕ naturally defines a family of multi-party quantum games, which in turn can be seen to be equivalent to a broad family of generalized CHSH inequalities. The task in the game will be the completion of a computation (in the NMQC⊕ model) specified by a particular Boolean function \( f(x) \) on an \( n \)-bit string \( x \). In section 3, we study tasks that, with quantum resources can be performed deterministically under NMQC⊕. Furthermore, we show that all functions can be achieved in this model and characterize an upper bound on the necessary number of measurements required for a generic function that is not always efficient in the size of \( x \). Then we focus on two specific families of functions and calculate lower bounds on the number of measurements that can be achieved. This setting, in which tasks that succeed deterministically with quantum resources but that are impossible to achieve deterministically
with LHV or classical correlations, are natural generalizations of the GHZ ‘all-or-nothing’ refutation of LHV models.

In section 4, we consider non-deterministic games. If we attempt to compute a function $f(x)$ in NMQC$_⊕$, with less than the minimal number of measurements required for a deterministic computation, then we know that the computation can only succeed with less than unity probability. However, we can still calculate the best mean success probability of the game for quantum and classical resources. Bell inequalities can be associated with the upper bounds on these games for classical correlations. We show that the NMQC$_⊕$ framework captures all of the broad family of generalizations of the CHSH introduced by Werner and Wolf [18] and Żuchowski and Brukner [24]. We shall then use it to calculate upper bounds on success with quantum resources or potential quantum violation of the classical, LHV upper bound for the families of functions identified in the previous sections, including the surprising result that the (arguably) most natural instance of a generalization of the CHSH inequality to the many-party setting has no quantum violation for $n > 2$. We conclude, in section 5, with a discussion of the consequences of results and open questions that remain.

We adopt the following notation throughout this paper. For bit-string $x$, $x_j$ will represent the $j$th bit of $x$ and $|x|$ will represent its length. $W(x)$ will represent the Hamming weight (number of nonzero bits) of $x$.

2. The NMQC$_⊕$ model

We begin by formalizing NMQC$_⊕$, as outlined in figure 1. The goal is to compute a Boolean function $f(x)$ given an $n$-bit input bit-string $x$. The available resource is a quantum state on which we may carry out spatially separated measurements. Each measurement can be carried out in one of two bases, e.g. $M_0$ or $M_1$, and so we denote the choice of all measurement bases and their measurement outcomes by bit strings $s$ and $m$, respectively, where the elements of each are each $j$th party’s choice of measurement $s_j$ and outcome $m_j$. The length of these bit-strings $|s| = |m|$ is determined by the number of measurements. For a non-adaptive model, the measurement settings cannot depend on outcomes of other measurement outcomes, but they depend only on the input string $x$. All side processing must be linear, in this model, so the measurement settings, $s$, depend only linearly on $x$. Without loss of generality we can assume that the linear function is homogenous, and write

$$s = (Px)⊕,$$  \hspace{1cm} (1)

where $P$ is an $n$-by-$|s|$ binary matrix and addition is modulo 2. Any NMQC$_⊕$ protocol is completely described by this matrix $P$, the quantum state used and the measurement bases. Note that it is essential that the measurement settings, $s$, have a non-trivial dependence on the input, $x$, since a fixed basis measurement would be merely equivalent to a classical device outputting bits according to a classical probability distribution. Finally, the output of the computation is achieved by linear post-processing on values of $m$, typically the parity of $m$. Deterministic NMQC$_⊕$ is achieved when the parity of $m$ always gives $f(x)$ for all values of $x$.

3. Deterministic computations and the Greenberger–Horne–Zeilinger paradoxes

Recall that every Boolean function $f(x)$ on an $n$-bit string $x$ can be represented uniquely as a polynomial over the finite field $Z_2$ (i.e. using modulo 2 arithmetic). This polynomial is known

New Journal of Physics 13 (2011) 023014 (http://www.njp.org/)
as the algebraic normal form (ANF) for the function. The ANF allows one to naturally classify Boolean functions according to the degree of the associated polynomial. Linear functions are functions of degree 1, i.e. of the form \( f(x) = a_0 + \bigoplus_{j=1}^{n} a_j x_j \), where \( a_k \) are bits and \( x_j \) is the \( j \)th bit of \( x \). A nonlinear function is one that cannot be written in this form.

It is not a priori clear whether this very restricted model of NMQC\(_{\oplus}\) would be particularly expressive. After all, it seems that few unitary circuits in MQC can be achieved deterministically without adaptive measurements. Nevertheless, in [7], Raussendorf showed, within a framework essentially identical to NMQC\(_{\oplus}\), that nonlinear functions can be computed by measurements on Reed–Muller states, a certain family of stabilizer states, and furthermore, that each nonlinear function led to a GHZ-like paradox, i.e. its deterministic evolution would be impossible to achieve with LHV correlations.

Our first result is to show that, in fact, all Boolean functions \( f(x) \) can be achieved deterministically in NMQC\(_{\oplus}\). Furthermore, our result is constructive, identifying the resource states and a means to compute the measurement bases to compute the function. It also provides an upper bound to the number of measurements needed for implementing any Boolean function deterministically in NMQC\(_{\oplus}\).

**Theorem 1.** In NMQC\(_{\oplus}\), with quantum resources, any Boolean function \( f(x) \), on an arbitrary \( n \)-bit string \( x \), can be computed with unity probability. This can be achieved with the resource state \( \frac{1}{\sqrt{2}}(0^{\otimes (2^n-1)} + 1^{\otimes (2^n-1)}) \), i.e. a \((2^n-1)\)-qubit generalized GHZ state.

**Proof of Theorem 1.** Our proof is constructive. Recall that in NMQC\(_{\oplus}\) each measurement device (or party) receives a bit-value \( s_j \), which is a linear function on input bit-string \( x \). Each then makes their measurement accordingly, returning the output of their measurement \( m_j \) (as a bit-value) to the side processor. Here, the \((2^n-1)\) parties share a generalized GHZ state, as defined above. The \( j \)th party will receive bit value \( s_j \). They will then make a measurement in the following basis: \( \cos(s_j \phi_j)\sigma_j + \sin(s_j \phi_j)\sigma_y \), where \( \phi_j \) is an angle that is yet to be specified. Note that a 0 input, in all cases, corresponds to a measurement of \( \sigma_z \). They will report the output of these measurements as a bit-value (e.g. 0 for eigenvalue +1 and 1 for eigenvalue –1), which is returned to the side processor.

The output of the NMQC\(_{\oplus}\) computation \( f(x) \) will be encoded (deterministically) in the parity of these outcome bits from the joint outcome of all parties. A simple analysis of the properties of GHZ states (see also [18]) shows us that the parity of the output bits will deterministically be equal to \( f(x) \) if the following equation is satisfied:

\[
e^{i \sum_j s_j(x) \phi_j} = -1^{f(x)+c}, \quad \forall x \in \{0, 1\}^n,
\]

where \( s = (Px)_{\oplus} \). The bit \( c \in \{0, 1\} \) represents a linear operation that maybe implemented in post-processing, and we can thus, without loss of generality, restrict \( f(x) \) to functions where \( f(0^{\otimes n}) = 0 \) and add any additional bit-flip in post-processing. The exponent on the lhs of (2) is a sum over real numbers (in the angles \( \phi_j \)), whereas the term in the exponent of the rhs is a Boolean function, which we are expressing as a polynomial over \( Z_2 \), i.e. with addition modulo 2. We shall exploit the fact that these different types of addition lead to different notions on linear independence. To emphasize this distinction, we refer to linear (in-)dependence over the reals as \( \mathbb{R}\)-linear (in-)dependence and linear (in-)dependence over \( Z_2 \) as \( Z_2\)-linear (in-)dependence.

The set of linear Boolean functions on \( x \), which appear in the sum on the lhs of the equation, are not necessarily \( Z_2 \) linearly independent, but as we shall show below, all such
functions are linearly independent over the reals. This means that linear functions (over $\mathbb{Z}_2$) can be combined linearly (in the real vector space) to produce a \textit{nonlinear} Boolean function. It is this mathematical fact that allows nonlinear functions to appear on the rhs of equation (2) and forms the basis for the ability for nonlinear functions to be computed within $\text{NMQC}_\oplus$.

Since this effect may seem at first hand surprising, we provide an explicit example. Consider the AND function $x_1x_2$ on two bits $x_1$ and $x_2$. This can be written as a linear combination of $\mathbb{Z}_2$-linear functions as follows:

$$x_1x_2 = \frac{1}{2} (x_1 + x_2 - (x_1 \oplus x_2)) .$$

(3)

This is an instance of a more general identity expressing the parity of a bit-string in real arithmetic

$$\bigoplus_i x_i = \frac{1}{2} \left[ 1 - \prod_i (1 - 2x_i) \right] = \sum_b (-2)^{W(b)-1} \prod_j x_j^{b_j},$$

(4)

where we sum over all $n$-length bit-strings $b$, and $W(b)$ is the Hamming weight of $b$. We complete our proof by showing that within the linear Boolean functions on bit-string $x$, we can find a complete basis (over the reals) for the vector space of real-valued functions on $x$, and thus any Boolean function $f(x)$ can be represented as an $\mathbb{R}$-linear combination of them.

An example of such a basis is the set of functions $f_a(x) = \bigoplus_{j=1}^n a_j x_j$ for all bit-strings $a$ (except the all zeros string), augmented by the constant function $f_0(x) = 1$. We see that this set has the required number of elements $2^n$ to form a basis, so it merely remains to be proven that these are $\mathbb{R}$-linearly independent. To do so, we exploit the fact that the monomial functions (i.e. Boolean functions with a single multiplicative term) are linearly independent in both $\mathbb{R}$ and $\mathbb{Z}_2$.

Every monomial function can be expressed as a real linear combination of parity functions. To see this, note that equation (4) shows us that every function $f_a(x)$, when expressed in arithmetic over the reals, is an $\mathbb{R}$-linear combination of a single monomial $\prod_{j \in a, a_j = 1} x_j$ of degree $W(a)$ and monomials of lesser degree than $W(a)$. Thus the degree $W(a)$ monomial is a linear combination of $f_a(x)$ and monomials of lesser degree. Since the degree 2 monomials can by equation (3) be expressed as linear combinations of parity functions, inductive reasoning tells us that all higher degree monomials must also be expressible as real linear combinations of parity functions alone. Since the monomials are linearly independent with respect to the reals, this implies that the functions $f_a(x)$ for all $n$-bit strings $a$ indeed form a basis for $n$-bit functions over the reals. Furthermore, this implies that all functions where $f(0^{\otimes n}) = 0$ can be achieved by $\mathbb{R}$-linear combinations of parity functions $f_a(x) = \bigoplus_{j=1}^n a_j x_j$.

Hence, solutions of equation (2) exist for any Boolean function $f(x)$ on $n$ bits. Solving (2) provides the measurement angles $\phi_j$ needed to implement the computation. This completes the proof. \qed

We see that the generalized GHZ states are universal resources for Boolean functions, in a similar sense to the way cluster states are universal resources for quantum computation. GHZ states always form the optimal resource for computations in $\text{NMQC}_\oplus$, in the sense that they minimize the number of qubits required for the computation. This is very closely related to Werner and Wolf’s proof that GHZ states always provide maximal violations of any generalized CHSH inequality [18] as shall be touched upon later in this paper.

\textbf{Corollary 1.} Raussendorf shows in [7] that non-entangled quantum states can only facilitate deterministic $\text{NMQC}_\oplus$ computations for degree 1 functions. Thus, the achievement of a

\textbf{New Journal of Physics} 13 (2011) 023014 (http://www.njp.org/)
nonlinear Boolean function in $\text{NMQC}_\oplus$ requires entanglement and may be considered (as discussed in [7]) a type of GHZ paradox.

Theorem 1 provides an upper bound to the number of qubits required to perform any Boolean function in $\text{NMQC}_\oplus$. Unfortunately, this bound is exponential in the size $n$ of the input string, and this computation strategy is therefore inefficient. It is pertinent to ask whether this many qubits are necessary or whether, for some functions, a more compact measurement scheme can be found. We shall now therefore calculate, for two families of functions, the lower bounds in the number of measurements required for deterministic evaluation under $\text{NMQC}_\oplus$.

The families we consider are both natural multipartite generalizations of the two-bit AND function:

- $n$-tuple AND function: $g_n(x) = \prod_{j=1}^{n} x_j$. This function computes the joint product of all bits.
- Pairwise AND function: $h_n(x) = \bigoplus_{j=1}^{n-1} x_j \bigoplus_{k=j+1}^{n} x_k$. This function computes the sum (modulo 2) of the pairwise product of all pairs of bits.

Studying these families of functions, we are able to prove the following two lower bounds:

**Proposition 1.** To achieve the $n$-tuple AND function $g_n(x)$ deterministically in $\text{NMQC}_\oplus$ one requires no fewer than $(2^n - 1)$ qubits.

We prove this result in two steps, provided in appendices A and B. Firstly, we demonstrate (appendix A) that many different choices of linear pre-processing, as described by the $P$ matrix, are equivalent. Furthermore, we demonstrate that when $|s| < (2^n - 1)$ the $P$ matrix is always equivalent to a canonical form with a specific property. Next we show that (appendix B), given this canonical form of $P$, satisfying all the $2^n$ required equations would entail a contradiction and hence must be impossible.

**Proposition 2.** To achieve the pairwise AND function $h_n(x)$ deterministically in $\text{NMQC}_\oplus$ one requires no fewer than $(n + 1)$ qubits.

**Proof.** The resource that achieves this bound is an $(n + 1)$ qubit GHZ state $\frac{1}{\sqrt{2}}(|0\rangle^\otimes n \otimes |1\rangle + |1\rangle^\otimes n \otimes |0\rangle)$ where the qubits are numbered $j = 1, 2, \ldots, n, n + 1$ from left to right. A simple calculation will verify that with input bits consisting of $s_j = x_j$ for $j = 1, \ldots, n$ and $s_{n+1} = \bigoplus_{j} x_j$ for the $(n + 1)$th site and measurement bases $\sigma_x$ or $\sigma_y$ for inputs 0 or 1, respectively, the parity of all $(n + 1)$ outputs is always equal to $h_n(x)$.

We now prove that this is a lower bound. We do so by showing that no $n$-bit nonlinear function may be achieved deterministically in $\text{NMQC}_\oplus$ with $n$ measurements alone. Given $n$ independent two-setting measurements on an $n$-subsystem state, there are $2^n$ possible combinations of measurements. If the parity of all measurement outcomes for all these $n$ measurement sites is to be deterministic for every combination of settings, the state must be an eigenstate of every different $2^n$ tensor product combination of the local observables, with eigenvalue $(-1)^{f(x)}$. But since these are dichotomic measurements, the local observables $M_j$ are idempotent, i.e. $M_j^2 = I$. Hence, by considering all products of the operators (i.e. finding the full stabilizer of the state), one quickly finds that the joint eigenstate must also be an eigenstate of local unitaries on each site, i.e. must be a product state. Since we know that unentangled...
Figure 2. Each graph compares the size in input $x$ to the available number of sites labelled by the size of $s$; the shaded regions indicate whether we can perform a particular function deterministically or probabilistically with quantum resources in NMQC⊕: (a) for the $n$-tuple AND function we require the most resources ($(2^n - 1)$ measurement sites) that are required for determinism; therefore the region under this line is completely probabilistic; (b) for the pairwise AND function, we require exponentially fewer resources than for the $n$-tuple AND for deterministic computation. The regions are continuously shaded for clarity.

Proposition 1 shows that the upper bound in resources given by Theorem 1 is tight for certain Boolean functions. Proposition 2, on the other hand, shows that we can perform certain functions deterministically with just a single ancilliary qubit. It is striking that the two families of functions have such divergent behaviour. We can see graphically in figure 2 the contrast between the resources required for each function to produce deterministic and probabilistic computations.

Corollary 2. Proposition 1 shows that certain families of Boolean functions are impossible to achieve efficiently and deterministically in NMQC⊕. This implies that it is impossible to efficiently achieve universal quantum computation deterministically in NMQC⊕.

This verifies the long-held intuition that adaptive measurement is important for MQC. However, we note that this corollary only has relevance for MQC with linear side processing. It tells us nothing of the full power of non-adaptive MQC with nonlinear side processing. This remains an open question.

The Popescu–Rohrlich non-local (PR) box is a widely studied [19, 20] example of a correlation resource that is not achievable in quantum mechanics. In the language of NMQC⊕ it is simple to define; it is the correlation that allows one to calculate the two-bit AND function $f(x) = x_1x_2$ via two measurements alone (such that marginal distributions are unbiased and hence non-signalling). Although the PR box plays a central role in the study of bipartite correlations, recently there has been much interest in the many-body correlations supported in theories more general than quantum mechanics [21]. The most general such framework,
in which all non-signalling correlations are permitted, is commonly called ‘boxworld’ or a
generalized non-signalling theory [21]. We can use the NMQC⊕ framework to classify some
of the correlations in such a theory. For example, propositions 1 and 2 immediately identify that
any correlation that permits in NMQC⊕ the computation of a function with fewer measurement
sites than the lower bounds proven here exists only in boxworld and not in quantum theory. The
NMQC⊕ framework may therefore be useful for the study and categorization of some of the
many-party generalizations of the PR box.

4. Non-adaptive measurement-based quantum computation and Bell inequalities

We have seen that deterministic computations in NMQC⊕ naturally define generalizations of
the GHZ paradox. In this section, we turn our attention to non-deterministic computation, where
we see a close relation with multi-party generalizations of the CHSH inequality. We consider
non-deterministic games of the following form. An input bit-string \( x \) is supplied according
to probability distribution \( w(x) \). The goal of the game is to return the output of the Boolean
function \( f(x) \) within the framework of NMQC⊕. In this case, we do not demand that the
game is won deterministically; instead we accept a less than unity success probability and wish
that this probability be the highest possible. Specifying an upper bound to the mean success
probability, in the case of a classical or LHV correlation, is equivalent to defining a set of Bell
inequalities [16]. Similarly, specifying an upper bound with quantum resources is equivalent to
a generalization of Tsirelson’s bound [22]. Note that for non-deterministic games it is critical
that the prior probability distribution \( w(x) \) over the inputs \( x \) is specified, since this defines the
mean success probability that is the figure of merit for the game. This family of games was first
defined and studied in depth in [16].

In NMQC⊕, every measurement has two settings and two outcomes. Multipartite
generalizations of the CHSH inequality for dichotomic two-setting measurements were defined
and studied by Werner and Wolf [18] and independently by Żukowski and Brukner [24]. A
traditional way of defining Bell inequalities is as a bound on a linear combination of conditional
expectation values \( \epsilon(s) \), where \( s \) represents the bit-string defining the measurement settings,
and \( \epsilon(s) \) is the expectation value of \((-1)^{\oplus_j m_j} \) with the outcome of the \( j \)th measurement as bit \( m_j \). In other words, using \(+1\) and \(-1\) instead of \(0\) and \(1\) to denote measurement outcomes \( \epsilon(s) \)
represents the expectation value of the product of the outcomes. In our notation, \( \epsilon(s) \) is defined
in terms of probabilities \( p(\oplus_j m_j | s) \):

\[
\epsilon(s) = p(\oplus_j m_j = 0 | s) - p(\oplus_j m_j = 1 | s).
\]

The generalized CHSH inequalities of Werner, Wolf, Żukowski and Brukner (WWŽB) take the form

\[
\sum_s \beta(s) \epsilon(s) \leq u,
\]

where \( \beta(s) \) are real coefficients, and \( u \) is a real value that is the upper bound to this quantity.
When the correlation is due to an LHV source, we label the upper bound \( u = c \). For the upper
bound for measurements on a quantum state, we use the notation \( u = q \). In this way, equation (6)
incorporates both Bell inequality and Tsirelson bound. The normalization of \( \beta(s) \) is arbitrary,
and can be chosen as best suits the calculations in hand. Werner and Wolf normalize the values
of \( \beta(s) \) such that \( c \) is always unity. To simplify our expressions here, however, we choose
a different normalization and set $\sum_s |\beta(s)| = 1$. This can be achieved for any CHSH-type inequality of the form (6) via a simple rescaling.

Werner and Wolf [18] give a compact expression that allows $q$ to be derived for a given set of coefficients $\beta(s)$ from a simple variational formula. The connection between such Bell inequalities and NMQC$_{\oplus}$ is straightforward and expressed via the theorem below. In fact, it suffices to consider a restricted form of NMQC$_{\oplus}$, which we shall label NMQC$_{\star \oplus}$, in which pre-processing of the input data $x$ is fixed to the identity map (i.e. $s = x$). In discussing NMQC$_{\star \oplus}$, we shall use $x$ and $s$ interchangeably.

**Theorem 2.** Every multipartite Bell (Tsirelson) inequality of the form of equation (6) (normalized to $\sum_s |\beta(s)| = 1$) can be re-expressed as a bound on the maximum mean probability $\bar{p}$ of an NMQC$_{\star \oplus}$ computation of a Boolean function $f(x) = \text{sign}(\beta(s))$ with $s = x$ and $n = |s|$ measurements, where input bits $s$ are supplied according to the probability distribution $w(s) = |\beta(s)|$,

$$\bar{p} \leq \frac{u + 1}{2},$$

(7)

where this particularly simple form is due to the choice of normalization $\sum_s |\beta(s)| = 1$.

**Proof of theorem 2.** The proof of this theorem is similar in content to observations made in [3, 16, 23], and indeed, the well-known mapping of the CHSH inequality to the CHSH game. However, the proof is simple, so we shall provide it here. We begin by substituting equation (5) into (6). Using the law-of-excluded middle for binary outcomes $p(\oplus, m_j = 0|s) + p(\oplus, m_j = 1|s) = 1$ and some simple algebra, we can rewrite equation (5) as

$$\epsilon(s) = (-1)^{f(s)}(2p(\oplus, m_j = f(s)|s) - 1),$$

(8)

which is true for any Boolean function $f(s)$. Substituting this into equation (6) and letting $f(s) = \text{sign}(\beta(s))$ and $w(s) = |\beta(s)|/(\sum_s |\beta(s)|)$, we obtain

$$\left| \sum_s w(s)p\left(\bigoplus_{j=1}^m \mu_j = f(s)|s\right) \right| \leq \frac{u + \sum_s |\beta(s)|}{2 \sum_s |\beta(s)|}.$$  

(9)

Werner and Wolf showed that the optimal quantum bound $u = q$ is always achieved by carrying out measurements on a GHZ state [18], thus echoing the optimal quantum resource state in theorem 1.

The expression on the left is the mean success probability of computing the function $f(s)$ in the NMQC$_{\star \oplus}$ model. Note that, in this model, the only possible post-processing step for any function that does not act trivially on any input bits is the XOR of all output bits, or the NOT of this bit. This completes the proof.

Theorem 2 informs us that the quantum game corresponding to any WWZB Bell inequality is a computation in NMQC$_{\oplus}$. Or oppositely put, the ability for a computation to be achieved in NMQC$_{\oplus}$ can always be represented as a Bell inequality. Note also that since pre-processing can be incorporated into the prior probability distribution $w(s)$, this result can be generalized, in a straightforward way, to the full class NMQC$_{\oplus}$.

The NMQC$_{\oplus}$ setting thus provides a framework in which we study families of Bell inequalities, over arbitrary numbers of parties, and calculate some of their generic properties.
As an example of this, we return to the two families of functions defined in the previous section, the \( n \)-bit pairwise AND and the \( n \)-tuple AND. Just as in the deterministic case these families provide interestingly contrasting behaviour. Note that both families include, for the \( n = 2 \) case, the bi-partite AND function and hence embody the standard CHSH inequality. We limit our study to the case where inputs \( s \) satisfy a uniform distribution, i.e. where \( w(s) = 2^{-n} \).

**Proposition 3.** The \( NMQC^* \oplus \) quantum game defined by the \( n \)-tuple AND function \( g_n(s) \) has no quantum advantage (i.e. \( q = c \)) for \( n \geq 3 \) if inputs are supplied from a uniform distribution \( w(s) = 2^{-n} \). For \( n > 2 \), the upper bounds on mean success probability are \( (1 - \frac{1}{2^n}) \) for both the quantum and LHV cases.

This result is proved in appendix C. This upper bound can be achieved by a computer that always outputs 0, so the quantum resources can be considered to provide no advantage for this computation whatsoever. Strikingly, the CHSH inequality (for \( n = 2 \)) is the only member of this family where quantum mechanics exceeds the LHV bound.

**Proposition 4.** The \( NMQC^* \oplus \) quantum game defined by the multipartite pairwise AND function \( h_n(s) \) on \( n \)-bits supplied from a uniform distribution \( w(s) = 2^{-n} \) possesses a quantum advantage with respect to LHV resources for every \( n \). The ratio of the upper bounds for the associated Tsirelson/Bell inequalities \( q/c \) grows exponentially in \( n \).

This can be seen by recognizing that the Bell inequalities defined by \( h_n(s) \) on a uniform distribution are equivalent (up to the relabelling of input and output bits) to the well-studied generalized Svetlichny inequalities [25], which can be verified via some algebraic manipulation (a similar fact is noted in [26]). It is well known that the ratio of quantum to classical upper bounds for these inequalities scales exponentially in \( n \). In fact, when \( n \) is even these inequalities are equivalent to the Mermin inequalities [27] known [18] to possess the maximal ratio of quantum to classical bounds of any inequality of the form (6). For even \( n \), the bounds are \( c = 2 \frac{2^n}{n} \) and \( q = 2 \frac{2^n}{n} \). For odd \( n \), \( c = 2 \frac{2^n}{1-n} \) and \( q = 2 \frac{2^n}{1-n} \).

5. Discussion

We have shown that there is a concrete connection between many-party Bell inequalities and non-adaptive measurement-based quantum computation and, indeed, the \( NMQC^* \oplus \) model provides a concise method for defining Bell inequalities via quantum games. The framework we developed unified a number of known results and led to several new results and insights, both with implications for measurement-based computation and Bell inequalities. The prominent appearance of the GHZ states in this work should not be a surprise. Werner and Wolf [18] showed that such states always provide the optimal quantum bounds for Bell inequalities of the form of equation (6). Theorem 2 thus implies that these states will always be optimal in \( NMQC^* \oplus \). The broader family of Reed–Muller states introduced by Raussendorf [7] are not required for these purposes.

There are a number of ways in which one might generalize these results. Firstly, it is natural to investigate whether higher-dimensional variations of MQC [28] might share the same relationship with Bell inequalities for more than two settings and outcomes per measurement. Higher-dimensional MQC is a straightforward generalization of the qubit case. However, there are certain difficulties that will need to be overcome to make this connection. Firstly,
while higher-dimensional GHZ paradoxes have been identified [29], in none of these cases do the correlations represent a full nonlinear function, but correlations only hold for a subset of possible input strings. Whether this subset might be identified with pre-computation and whether or not higher-dimensional GHZ paradoxes might be found that achieve a full function in higher dimension $\text{NMQC} \otimes$ remains a question for future study. Secondly, by considering computations with multiple output bits, one could start exploring the full region of conditional output probabilities for both the quantum (i.e. generalize the Tsirelson–Landau–Masanes region [22, 30]) and LHV cases.

Recently, attempts have been made to axiomatize quantum physics [19] via information theoretic approaches [20]. Principles such as Information Causality [31] and Macroscopic Locality [32] have been successfully applied to derive, or at least bound, the set of correlations permitted under quantum mechanics in the bi-partite setting. These approaches, while very successful for the bi-partite case, do not easily generalize to the multi-party setting. Since the $\text{NMQC} \otimes$ framework naturally poses Bell inequalities in an informational theoretic framework, this could be a fruitful starting point for axiomatic reconstructions of multi-party quantum correlations.

A related idea, considered earlier by van Dam [23] and Brassard et al [33], was to question whether the limitations on quantum correlations, expressed by Tsirelson-type bounds, might be imposed by Nature, in order to prevent distributed computation being achieved with trivial communication complexity. It was noted by van Dam that if PR boxes existed in Nature, then arbitrary distributed Boolean functions between two separated players could be achieved with just a single bit of communication. Brassard et al argued that perhaps Tsirelson’s bound on the CHSH inequality might take precisely that value which precludes such a dramatic collapse of communication complexity. They showed, using Von Neumann’s majority code error correction scheme, that there existed potential values of Tsirelson’s bound less than 4 (but higher than $2\sqrt{2}$) at which communication complexity for all functions would be a single bit. However, this argument did not recover Tsirelson’s bound exactly.

Recently, a multipartite generalization of this approach was considered by Marcovitch and Reznik [26]. They showed that the Von Neumann majority gate correction scheme could be generalized to many-party functions by replacing the PR box by a non-local box defined by the pairwise AND function $h_n(x)$. They showed that the assumption that such an error correction is impossible places an upper limit on the quantum bound for the generalized Svetlichny inequalities, providing evidence that Brassard et al’s conjecture might hold in the multi-party case. Our results have interesting implications for such arguments. Since for $n$-tuple AND functions quantum and classical bounds coincide (under the assumption, implicit in the above works, that the input distribution is uniform), any bounds derived via communication complexity for quantum correlations must also be tight for classical correlations. If the communication complexity conjecture were true, this would imply that the classical upper bound for the distributed computation would place a lower bound on the (classical) threshold for Von Neumann’s error correction scheme. In other words, two classical bounds would be causally related, but related via a quantum argument.

The approaches taken here are typical of recent attempts in quantum information science to use computer science formalisms to clarify, simplify and generalize results in physics. Thinking of Bell inequality experiments as computations has been very fruitful, and it seems likely that such approaches will continue to provide fresh insights into long-studied physics problems.
Appendix A. Equivalence of $P$ matrices

The $P$ matrix (size $n$-by-$|s|$) specifies the linear dependence between the measurement settings, $s$, and the input, $x$. This appendix demonstrates that many choices of $P$ are equivalent. Whenever $|s| < 2^n - 1$, this equivalence allows all $P$ to be brought into a form where no column has all entries equal to one, formally $\prod_j P_{j,k} = 0, \forall j$. This property is exploited when we prove proposition 1. We begin by proving the following lemma.

**Lemma 1.** An $\text{NMQC}_{\oplus}$ computation with $|s|$ measurements and with pre-processing map $P$ can deterministically compute a function $f(x) = \prod_{j=1}^{n} (x_j \oplus 1)$ if and only if there exists a computation with pre-processing map $P' = (PM)_{\oplus}$, which can also deterministically compute $f(x)$, where $M$ is any invertible binary $n$-by-$n$ matrix. Hence, the impossibility of a deterministic computation with $|s|$ measurements in $\text{NMQC}_{\oplus}$ with pre-processing map $P$ implies the impossibility of computation with $|s|$ measurements by any pre-processing map $P' = (PM)_{\oplus}$.

Recall that a function is deterministically computed whenever (2) is satisfied, such that

$$e^{i(Px)\phi} = -1^{f(x)+c}, \quad \forall x \in \{0, 1\}^n.$$ \hfill (A.1)

Taking the action of a binary, invertible matrix $M$, the above expression is altered to give

$$e^{i(PMx)\phi} = -1^{f(x)+c}, \quad \forall x \in \{0, 1\}^n.$$ \hfill (A.2)

We note that the set $\{x | x \in \{0, 1\}^n\}$ is identical to $\{Mx | x \in \{0, 1\}^n\}$ for any invertible binary $n$-by-$n$ matrix $M$. Secondly, $f(x) = f(Mx)$ for the function $f(x) = \prod_{j=1}^{n} (x_j \oplus 1)$ since the $x = \{0, 0, \ldots, 0\}$ all zeros case is unaffected by these linear transformations $M$. Hence, if equation (A.1) is satisfied by $P$ and $\phi$, it is also satisfied if $P$ becomes $(PM)_{\oplus}$.

Next we show that (assuming $|s| < 2^n - 1$) all $P$ are equivalent to some $P' = (PM)_{\oplus}$, such that the desirable property $\prod_k P'_{j,k} = 0, \forall j$ holds. Denoting the $j$th row of $P$ by $[P]_j$, we observe that, since $|s| < 2^n - 1$, the rows $[P]_j$ will not include every possible non-trivial binary string. We label one of the missing binary strings as $w$. There always exists an invertible $M$ such that $wM = \{1, 1, \ldots, 1\}$. Since the map is invertible all rows $[P]_j \neq w$ are mapped to $[PM]_j \neq \{1, 1, \ldots, 1\}$.

Appendix B. Proof of proposition 1

**Proposition 1.** To achieve the $n$-tuple AND function $g_n(x)$ deterministically in $\text{NMQC}_{\oplus}$, one requires no fewer than $(2^n - 1)$ qubits.
For the purposes of the proof it is simpler to consider the function $k_n(x) = 1 \oplus \prod_j^n (x_j \oplus 1)$. This function is obtained from $g_n(x)$ under local relabelling (NOT) of the input bits. Thus bounds we prove for $k_n(x)$ will thus also hold for $g_n(x)$. For deterministic evaluation of the function, equation (2) must be satisfied, which we assume to be true and then derive a contradiction.

Assuming that equation (2) holds for $x = \{0, 0, \ldots, 0\}$ entails

$$e^0 = (-1)k_n(0,0,\ldots,0+c) = (-1)^c,$$

and hence $c = 0$. Next, assuming (2) holds for $x \neq \{0, 0, \ldots, 0\}$ (for which $k_n(x) = 1$) entails

$$e^{(P_x)T}φ = (-1)^{k_n(x)} = (-1), \quad ∀x \neq 0, 0, \ldots, 0,$$

and hence

$$(P_x)Tφ = \pi(2t + 1), \quad ∀x \neq 0, 0, \ldots, 0,$$

for some integer $t_x$. We can construct a sum over all $x$ that alternates in sign:

$$\left[ \sum_{x \in \{0,1\}^n} (-1)^{W(x)}(P_x)T \right]φ = \sum_{x \mid |x| \neq 0} (-1)^{W(x)}[\pi(1 + 2t_x)].$$

Collecting terms on the rhs that have the Hamming weight, $W(x)$, equal to $y$ and defining $t'_x = \sum_{x \mid W(x) = y} t_x$ gives a summation over numbers

$$= \sum_{y=1}^n (−1)^y \pi \left( \frac{n!}{y!(n−y)!} + 2t'_x \right),$$

$$= \pi(2t − 1),$$

where $t$ is again an integer, such that $t = \sum_{y=1}^n (−1)^y t'_x$. Our proof proceeds by showing that the lhs of (B.4) vanishes and therefore results in the contradiction that $π(2t − 1) = 0$. The $j$th element of the lhs of (B.4) is

$$\left[ \sum_{x \in \{0,1\}^n} (-1)^{W(x)}(P_x)T \right]_j = \sum_{x \in \{0,1\}^n} (-1)^{W(x)} \left( \bigoplus_k P_{j,k}x_k \right).$$

Next we observe that this vanishes if for any $k$, we have $P_{j,k} = 0$. To see this we assume without loss of generality that $P_{j,n} = 0$. Consider pairs of terms for $x'$ and $x''$ that are identical except for the $n$th element, such that $x' = \{x_1, x_2, \ldots , x_{n−1}, 0\}$ and $x'' = \{x_1, x_2, \ldots , x_{n−1}, 1\}$. For these terms $\left( \bigoplus_k P_{j,k}x_k \right) = (\bigoplus_k P_{j,k}x''_k)$ since $P_{j,n} = 0$ the value of the $n$th element does not matter. However, $W(x'') = W(x') + 1$, and so $(-1)^{W(x''')} = -(-1)^{W(x''')}$ and so the two terms cancel. The whole summation can be broken up into distinct pairs of the form, $x'$ and $x''$, and since each pair cancels, the whole sum must vanish.

Recall that for our proof by contradiction we wish to show that the vector of equation (B.4) is zero for every element (every $j$). The preceding argument shows that the $j$th element will vanish unless $\prod_k P_{j,k} = 1$; that is, the $j$th row of $P$ is a row of all ones. However, appendix A demonstrated that every $P$ is computationally equivalent to many other $P'$ matrices. Furthermore, whenever $|x| < 2^n − 1$, we can find an equivalent $P'$ for which no row contains all ones. This completes the proof.

To see why the proof fails for $(2^n − 1)$ distinct measurements, we note that in this case, $P$ must always have the all-ones row (under the assumption that all rows are distinct and no row contains all zeros), and then a solution to equation (2) may always be found, as shown explicitly in the proof of theorem 1.
Appendix C. Proof of proposition 3

Proposition 3. The NMQC∗ ⊕ quantum game defined by n-tuple AND function g_n(s) has no quantum advantage (i.e. q = c) for n ≥ 3 if inputs are supplied from a uniform distribution \( w(s) = \frac{1}{2^n} \). For n > 2 the upper bounds on mean success probability are \( (1 - \frac{1}{2^n}) \) for both the quantum and LHV cases.

To prove this, we explicitly derive the Tsirelson bound for this particular family of Bell inequalities and show that it is equal to the bound obtained by the trivial classical strategy, where every measurement device always outputs zero. In the WWŻB form, with normalization \( \sum |\beta(s)| = 1 \), the inequality may be (according to theorem 2) written as

\[
\left| \sum_s (-1)^{\prod_{k=1}^n s_k} \frac{\epsilon(s)}{2^n} \right| \leq c \leq q.
\] (C.1)

For the trivial classical strategy, \( \epsilon(s) = 1 \) for all \( s \), and thus the quantity on the lhs of the inequality is equal to \( (2^n - 2)/2^n \). To prove the proposition, we will show that the quantum upper bound (and hence also the classical upper bound) for this quantity is also equal to \( (2^n - 2)/2^n \).

Werner and Wolf [18] show that \( q \) must satisfy the following equation:

\[
q = \sup_{\{\phi_k\}} \left| \sum_s (-1)^{\prod_{k=1}^n s_k} \prod_{k=1}^n e^{i s_k \phi_k} \right|.
\] (C.2)

Due to the form of this equation, we may, without loss of generality, restrict \( \phi_k \) to the range \( \phi_k \in (-\pi, \pi) \). We simplify equation (C.2), using the fact that \( (-1)^{\prod_{k=1}^n s_k} = \pm 1 \) for all bit-strings \( s \) except when \( s \) is the ‘all-ones’ bit-string, to write

\[
2^n q = \sup_{\{\phi_k\}} \left| \sum_s \prod_{k=1}^n e^{i s_k \phi_k} - 2e^{i \sum_k \phi_k} \right|.
\] (C.3)

The sum over \( s \) then factorizes to achieve

\[
2^n q = \sup_{\{\phi_k\}} \left| 2^n \prod_{k=1}^n \cos \left( \frac{\phi_k}{2} \right) - 2e^{i \sum_k \phi_k} \right|.
\] (C.4)

We now adopt a geometric argument. The goal is to maximize the modulus of a sum of two complex numbers. These numbers may be represented, on the plane, as the two sides of a triangle, as illustrated in figure C.1. The first side has length \( 2^n \prod_{k=1}^n \cos(\frac{\phi_k}{2}) \), the second is of length 2 and the angle between these sides is \( \sum_k \frac{\phi_k}{2} \). We complete the proof by showing that when \( n > 7 \), the length of the third side of the triangle can never exceed \( 2^n - 2 \) and hence \( q \) cannot exceed the classical value.

We proceed by assuming the opposite of what we want to prove and demonstrating a contradiction. For there to be a quantum violation of the classical bound, \( 2^n q > 2^n - 2 \) needs to be satisfied. Via the triangle inequality, for this inequality to be satisfied, the length of the base of the triangle must be greater than \( 2^n - 4 \), and thus

\[
\prod_{k=1}^n \cos \left( \frac{\phi_k}{2} \right) > 1 - 2^{2-n}.
\] (C.5)
Since \( \phi_k \in (-\pi, \pi) \) all terms in the product are non-negative; hence we can impose the weaker condition for (C.5) that \( \forall \phi_k \),

\[
\cos\left(\frac{\phi_k}{2}\right) > 1 - 2^{2-n}. \tag{C.6}
\]

which implies

\[
-n \arccos(1 - 2^{2-n}) < \sum_{k=1}^{n} \frac{\phi_k}{2} < n \arccos(1 - 2^{2-n}) \tag{C.7}
\]

or

\[
\left| \sum_{k=1}^{n} \frac{\phi_k}{2} \right| < n \arccos(1 - 2^{2-n}). \tag{C.8}
\]

Proceeding geometrically, we now use the cosine rule to find the length of the third side of the triangle

\[
(2^n q)^2 = 4 + 2^{2n} \prod_{k=1}^{n} \cos^2\left(\frac{\phi_k}{2}\right) - 2^{n+2} \cos\left(\sum_{l=1}^{n} \frac{\phi_l}{2}\right) \prod_{m=1}^{n} \cos\left(\frac{\phi_m}{2}\right). \tag{C.9}
\]

To obtain a quantum violation, we need \((2^n q)^2 > 4 + 2^{2n} - 2^{n+2}\). Since \( \phi_k \in (-\pi, \pi) \), \( \prod_{m=1}^{n} \cos(\frac{\phi_m}{2}) \) is non-negative, and hence a violation can only be achieved if \( \cos(\sum_{k=1}^{n} \frac{\phi_k}{2}) \) is negative, which implies \( |\sum_{k=1}^{n} \frac{\phi_k}{2}| > \frac{\pi}{2} \).

Using this, together with inequality (C.8), we achieve

\[
n \arccos(1 - 2^{2-n}) > \frac{\pi}{2} \tag{C.10}
\]

or equivalently

\[
\cos\left(\frac{\pi}{2n}\right) > (1 - 2^{2-n}). \tag{C.11}
\]

This inequality is only satisfied for integers \( n \leq 7 \); hence, due to the contradiction with our initial assumption, for \( n > 7 \) the quantum and classical bounds of the Bell inequality must coincide with that of the trivial strategy \((2^n - 2)/2^n\), and there is no quantum advantage. Direct numerical verification of the bounds, via equation (C.4) for \( n < 7 \), indicates that the bounds coincide for all integer values \( 3 \leq n \leq 7 \), completing the proof. \( \square \)
References

[1] Bell J S 1964 Physics 1 195
[2] Acin A et al 2007 Phys. Rev. Lett. 98 230501
[3] Brukner C et al 2004 Phys. Rev. Lett. 92 127901
[4] Buhrman H, Cleve R, Massar S and de Wolf R 2010 Rev. Mod. Phys. 82 665
[5] Shor P W 1997 SIAM J. Comput. 26 1484–509
[6] Anders J and Browne D E 2009 Phys. Rev. Lett. 102 050502
[7] Raussendorf R 2009 arXiv:0907.5449 [quant-ph]
[8] Raussendorf R, Browne D E and Briegel H J 2003 Phys. Rev. A 68 022312
[9] Gross D and Eisert J 2007 Phys. Rev. Lett. 98 220503
Gross D, Eisert J, Schuch N and Perez-Garcia D 2007 Phys. Rev. A 76 052315
[10] Raussendorf R and Briegel H J 2001 Phys. Rev. Lett. 86 5188–91
Briegel H J, Browne D E, Dur W, Raussendorf R and Van den Nest M 2009 Nat. Phys. 5 19–26
[11] Browne D E, Kashefi E and Perdrix S 2010 Proc. Fifth Conf. on the Theory of Quantum Computation, Communication and Cryptography (TQC 2010) (Berlin: Springer)
[12] Shepherd D and Brenner M J 2008 arXiv:0809.0847 [quant-ph]
[13] Brenner M J, Josza R and Shepherd D J 2010 arXiv:1005.1407 [quant-ph]
[14] Clauser J F, Horne M A, Shimony A and Holt R A 1969 Phys. Rev. Lett. 23 880
[15] Greenberger D M, Horne M A and Zeilinger A 1989 Bell’s Theorem, Quantum Theory, and Conceptions of the Universe ed M Kafatos (Dordrecht: Kluwer Academic)
[16] Cleve R, Hoyer P, Toner B and Watrous J 2004 Proc. IEEE Conf. on Computational Complexity pp 236–49
[17] Broadbent A and Tapp A 2008 arXiv:0810.5317 [quant-ph]
[18] Werner R F and Wolf M M 2001 Phys. Rev. A 64 032112
[19] Popescu S and Rohrlich D 1994 Found. Phys. 24 379
[20] Barrett J et al 2005 Phys. Rev. A 71 022101
[21] Barrett J 2007 Phys. Rev. A 75 032304
[22] Cirel’son B S 1980 Lett. Math. Phys. 4 93
[23] van Dam W 2000 PhD Thesis Oxford University, UK (arXiv:quant-ph/0501159)
[24] Żukowski M and Brukner C 2002 Phys. Rev. Lett. 88 210401
[25] Collins D, Gisin N, Popescu S, Roberts D and Scarani V 2002 Phys. Rev. Lett. 88 170405
[26] Marcovitch S and Reznik B 2008 Phys. Rev. A 77 032120
[27] Mermin N D 1990 Phys. Rev. Lett. 65 1838
Ardehali M 1992 Phys. Rev. A 46 5375
Belinskii A V and Klyshko D N 1993 Phys.—Usp 36 653
[28] Van den Nest M, Miyake A, Dür W and Briegel H J 2006 Phys. Rev. Lett. 97 150504
Mora C E, Piani M, Miyake A, Van den Nest M, Dür W and Briegel H J 2010 Phys. Rev. A 81 042315
[29] Kaszlikowski D and Zukowski M 2002 Phys. Rev. A 66 042107
[30] Masanes L 2003 arXiv:quant-ph/0309137
[31] Pawlowski M et al 2009 Nature 461 1101
[32] Navascues M and Wunderlich H 2009 Proc. R. Soc. A 466 881–90
[33] Brassard G et al 2006 Phys. Rev. Lett. 96 250401