Logical paradoxes in quantum computation

Nadish de Silva
Department of Computer Science
University College London
London, UK
nadish.desilva@utoronto.ca

Abstract

The precise features of quantum theory enabling quantum computational power are unclear. Contextuality—the denial of a notion of classical *physical reality*—has emerged as a promising hypothesis: e.g. Howard *et al.* showed that the magic states needed to practically achieve quantum computation are contextual.

Strong contextuality, as defined by Abramsky-Brandenburger, is an extremal form of contextuality describing systems that exhibit logically paradoxical behaviour.

After introducing number-theoretic techniques for constructing exotic quantum paradoxes, we present large families of strongly contextual magic states that are computationally optimal in the sense that they enable universal quantum computation via deterministic injection of gates of the Clifford hierarchy. We thereby bolster a refinement of the resource theory of contextuality that emphasises the computational power of logical paradoxes.

1 Introduction

Issues. Identification of the precise features of quantum theory accounting for quantum advantages over classical devices, and of the mechanisms by which they do so, remains an open problem in quantum computation. Physicists and quantum information theorists seek high-level principles behind quantum advantages in order to optimise resources and serve as guideposts towards novel protocols and algorithms.

A promising, emerging hypothesis is *contextuality*: a concept from the foundations of quantum mechanics first articulated by Bell-Kochen-Specker [13, 47] that is commonly understood as the denial of a classical notion of reality. Essentially, contextuality is the failure of correlated probabilistic data to be reproducible by a classical probability model. It subsumes *nonlocality*—the failure of separated systems to respect a strong classical assumption about causality [14]—as a special case. With these concepts, tensions between classical and quantum physics, e.g. the Einstein-Podolsky-Rosen paradox [28], are formally articulated to a degree that experiments (e.g. [10, 39]) can be performed to refute classical ontological assumptions.

An important lesson of recent studies of contextuality is that it is a logical phenomenon that is most clearly understood independently of quantum physics, the setting in which it first appeared

[1–7, 11, 44]. At its core, contextuality is concerned with systems (quantum or otherwise) possessing properties whose values are not assumed to be simultaneously ascertainable. The primary question asked of such systems is whether they can, in principle, be modelled under the assumption that all properties do simultaneously have consistent values. The central technical tools are Bell inequalities [14, 17, 46] that bound the strength of classical correlations.

The notion of *strong contextuality*, due to Abramsky-Brandenburger [5], is an extremal form of contextuality describing probabilistic systems that exhibit logically paradoxical behaviour. Whereas standard contextuality is witnessed by the violation of a probabilistic Bell inequality, strong contextuality is witnessed by a logical paradox [6]. These paradoxes lie at the heart of contextuality in the sense that any contextual data is a convex mixture of classical and strongly contextual data [4].

Access to the contextual correlations that can arise from quantum systems has been suggested as a critical resource for realising the advantages of quantum devices for a variety of computational [9, 25, 31, 38, 45, 51, 54, 57] and communicational [4, 19, 22, 56] tasks. Our motivation is to consider the role of logical paradoxes realised by extremally contextual quantum resources for the task of practically achieving universal quantum computation, i.e. the ability to perform any quantum gate with arbitrary precision.

We build on recent, seminal work of Howard *et al.* [43], following [21, 31, 32, 37, 48, 57–59], establishing the neccessity of probabilistically contextual resources for achieving universal quantum computation in the model of fault-tolerant quantum computation via state injection. In this model, a heavily restricted quantum computer capable of only *stabilizer operations* [33] (whose circuits use only Clifford gates) is implemented. These restrictions facilitate the error-correction necessary of any practical model of quantum computing; however, they are so strong that the scheme is efficiently classically simulable [34] and thus offers none of the power of quantum computation. The ability to perform a non-Clifford gate promotes this scheme to universal quantum computation. This can be achieved by state injection [35]: a variation on the quantum teleportation protocol that consumes a resource *magic state* and implements a non-Clifford gate. In essence, states can be converted, via stabilizer operations, into gates. Typical magic states must undergo a stochastic distillation and injection process, due to Bravyi and Kitaev [15], requiring randomly many repeated attempts before being successfully converted into a non-Clifford gate. Howard *et al.* [43] showed that single-qudit magic states of odd, prime dimension exhibit standard contextuality with respect to two-qudit stabilizer measurements once paired with an ancilla qudit.

Logical paradoxes are known to be critical resources in a diverse variety of settings: e.g. nonlocal games [16, 19], zero-error information theory [22], measurement-based computation [55], etc. Across these settings, a striking pattern emerges: access to contextual resources can improve the probability of success of achieving

some task whereas access to paradoxes can enable deterministic advantage. We are interested in whether this pattern extends to the complex task of universal quantum computation.

Results. In this paper, we present large families of multiqudit magic state-based paradoxes (Theorem 1) arising from the Clifford hierarchy [33], a distinguished class of gates admitting direct, deterministic injection. They are fundamentally different from all known quantum paradoxes in requiring novel number-theoretic arguments (Lemmas 3.1 and 3.2) that we introduce below.

Significance. The existence of these paradoxes is striking given that there is no a priori reason that they should be realised by quantum states, let alone by those magic states that serve as ideal computational resources. Finding these complex paradoxes is possible only by testing the hypothesis of paradox-driven advantage. The alignment of resourcefulness of magic states with extremal contextuality in the the logical sense validates logical aspects of contextuality as highly useful from a computational perspective. Extending the theme of probabilistic vs. deterministic advantages from standard vs. strong contextuality from simpler tasks (e.g. measurement-based computation of nonlinear finite functions) to the complex setting of full-blown universal quantum computation suggests a common underlying logical mechanism behind contextuality-powered advantages in computation and communication. This suggests further scope for the use of logical methods in reaching a structural understanding of quantum computational advantage.

Contents. In the next sections, we briefly review contextuality, contextuality as a computational resource, and the magic state model of quantum computation before presenting our paradoxical magic states and indicating future directions towards understanding the paradoxes at the heart of contextuality as powerful computational resources.

2 Background

2.1 Contextuality: probabilistic and paradoxical

Here, we briefly summarize the prerequisite background on contextuality, following the framework of Abramsky-Brandenburger [5]. We emphasize that contextuality is a property of probabilistic data with respect to a set of measurements in an experimental setup wherein it is not assumed that all measurements can be performed together. Thus, it is a concept that applies not to any particular physical theory, but to the empirical data predicted by a physical theory. Of course, in the sequel, we are concerned with contextuality of data that arises from performing quantum measurements on quantum states.

An experiment is modelled by a *measurement scenario*: a triple $(\mathcal{M}, C, O)$ where $\mathcal{M}$ is a set of measurements and C is the set of *contexts*. A context is a maximal set $C \subset \mathcal{M}$ of measurements that can be performed together. The outcome set O is merely a set of labels for the outcomes possible upon performing a measurement. Nonlocality experiments are those where each measurement is associated to a site and contexts are choices of a measurement from each site. For example, the standard Bell scenario [13] is captured by $\mathcal{M} = \{A_0, A_1, B_0, B_1\}$, contexts $C = \{\{A_a, B_b\} : a, b \in \{0, 1\}\}$, and outcome set $O = \{0, 1\}$. Measurement of each $M \in \mathcal{M}$ yields a value from the outcome set O; a run of the experiment for the context C produces a joint outcome $o : C \to O$. Empirical data from performing experiments on a system in a fixed state is captured by a choice, for each context C, of a conditional distribution

$P_C = P(-|C) : O^C \to [0, 1]$ on joint outcomes. Data satisfying physically reasonable conditions of generalised nonsignalling—the marginal distributions $P_C|_{C \cap C'}$ and $P_{C'}|_{C \cap C'}$ agree for all C and C'—constitute an *empirical model P*.

An empirical model P is *noncontextual* (*local*) when its predictions can be accounted for by a *noncontextual (locally causal) hidden variable model*. Such a hidden variable model can be assumed to have a canonical form [5, 30]: the hidden variable space is $\Lambda = O^{\mathcal{M}}$, with each hidden variable being a function $\lambda : \mathcal{M} \to O$ (a choice of predetermined outcome for all measurements), together with a distribution $\mu : \Lambda \to [0, 1]$ over hidden variables that recovers the P_C as marginal distributions $\mu|_C$. Data arising from a hidden variable model will satisfy all Bell inequalities [6, 17, 46, 52] that bound the strength of classical correlations; thus, contextuality is witnessed by violation of a probabilistic inequality.

A hidden variable $\lambda : \mathcal{M} \to O$ and an empirical model P are *consistent* when, for each context C, the joint outcome λ prescribes to the measurements in C is *possible*: $P_C(\lambda|_C) \neq 0$. An empirical model is *strongly contextual* when it is inconsistent with all hidden variables, i.e. for every hidden variable λ, there is an experiment for which λ predicts an impossible outcome. Whereas the standard probabilistic form of contextuality is witnessed by a violation of an inequality, strong contextuality is witnessed by a logical paradox [7]. Strong contextuality generalises the notion of *maximal nonlocality* of Elitzur-Popescu-Rohrlich [29] and Barrett *et al.* [12]. Well-known examples include the GHZ state [36] (see Figure 1) and the PR box [53].
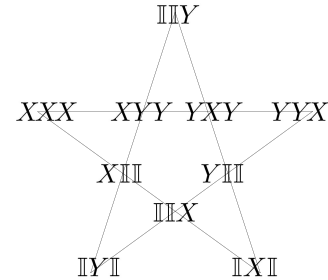

Figure 1. Mermin's star paradox [49]. The GHZ state is an eigenstate of the qubit Pauli measurements on the horizontal line with eigenvalues +1,-1,-1,-1 (from right to left) thereby fixing the value of any consistent hidden variable λ on these measurements. However, no assignment of outcomes to the other measurements can respect the parity consistency constraints imposed by the algebraic relations between measurements: since the product of the measurements along any non-horizontal line is the identity, the product of outcomes along these lines must be 1. Thus, the GHZ state is strongly contextual with respect to the above measurements. This linear algebraic paradox can be cast as a constraint satisfaction problem [20]. The magic states we will consider below need not be eigenstates of any stabiliser measurements.

The intuitive idea that a strongly contextual system behaves paradoxically can be formalised. For each measurement $M \in \mathcal{M}$ and outcome $o \in O$, the symbol $M \to o$ is interpreted as "M is measured resulting in the outcome o". One can construct a *sentence* with, for $M \in C$ of a fixed context and $o \in O$, symbols $M \to o$ and the connectives AND, OR, and NOT. The *theory* of an empirical

model are all those sentences that are always true after any run of the experiment. An empirical model is strongly contextual if and only if its theory is logically inconsistent.

Every empirical model P is a convex mixture of a noncontextual part P^{NC} and a strongly contextual part P^{SC} as $P = \text{CF}(P)P^{SC} + [1 - \text{CF}(P)]P^{NC}$. Here, $\text{CF}(P)$ is a measure of contextuality known as the *contextual fraction* [5]; it generalises the nonlocal fraction [12]. An empirical model is strongly contextual if and only if $\text{CF}(P)$ is 1 (or, the *noncontextual fraction* $[1 - \text{CF}(P)]$ is 0). Thus, the contextual fraction measures the degree to which a model provides probabilistic access to paradoxical data. Strongly contextual models are extremally contextual in a geometric sense: they correspond to points on those faces of the nonsignalling polytope with no noncontextual vertices [3, 8].

2.2 Contextuality as a computational resource

Contextuality and nonlocality have been shown to be critical to achieving advantages in a variety of informatic tasks. A general scheme that results of this flavour fit is as follows: a restricted model of computation or communication is proven to have some upper bound on its success in achieving some task before showing that same model, once supplemented with the ability to perform measurements on a contextual system, gains a probabilistic advantage. The pattern of strongly contextual resources conferring deterministic advantages is seen across computational and communicational settings. Sharing an unlimited number of PR boxes between two parties renders all communication complexity problems trivial [56]. Kochen-Specker configurations play an essential role in boosting the zero-error (i.e. deterministic) capacity of certain classical channels [22]. Perfect strategies for nonlocal games [19] require strongly contextual resources [4].

We are primarily interested in two computational tasks that are known to benefit from access to contextuality: measurement-based computation and fault-tolerant quantum computation via state injection. Measurement-based computation is a generalisation of the model of measurement-based quantum computation (MBQC). In MBQC, a restricted classical computer, having received classical input, directs measurements on an entangled resource quantum state. Remarkably, although no quantum gates are directly implemented, such models are capable of universal quantum computation. Measurement-based computation is an abstraction of MBQC wherein no particular background physical theory is assumed. Instead, measurements are performed on an abstract resource system whose behaviour is described by an empirical model. Below, we describe known results on the necessity of contextuality and strong contextuality for measurement-based computers to accomplish the task of computing finite functions; note that these results are not concerned with universal quantum computation.

Subsequently, we review how universal quantum computation is achieved fault-tolerantly in the circuit model via magic state distillation. In this setting, contextual resources are not themselves directly measured, in contrast to the measurement-based model. Rather, elementary operations are performed on a system composed of both an input quantum state and the resource state with the net effect that a non-elementary gate is performed on the input. Contextuality is a necessary criterion for those states serving as

useful resources. By presenting paradoxes realised by computationally optimal magic states, we establish the relevance of the logical perspective to the task of universal quantum computation.
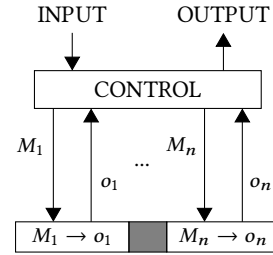

Figure 2. Computation of functions by sequential measurements on a resource system. The input and previous outcomes are processed to choose the next measurement. Having performed all the measurements, the input and the outcomes are processed to give the output. All processing is done by a restricted control computer capable of performing mod-2 arithmetic [54]

.

2.3 Measurement-based computation

Anders and Browne [9] proved that a computer capable only of mod-2 addition supplemented with access to measurements on a GHZ state can deterministically compute the OR of two bits (a nonlinear function). The input bits determine the measurements performed on the three qubits; linear post-processing of the measurement outcomes yields the desired output. Raussendorf [54] generalised this to mod-2 linear measurement-based computers. A computer restricted to performing mod-2 addition that can control measurements on an empirical model can compute a nonlinear function with high probability only if the empirical model is contextual. The computation's failure probability is lower bounded by the product of the resource state's noncontextual fraction [4] and a measure of the function's nonlinearity. So, *deterministically* computing a nonlinear function requires a *strongly* contextual resource.

2.4 The magic state model

Fault-tolerant quantum computing works by supplementing stabilizer operations (that are easy to both implement and classically simulate) with access to magic states. We briefly summarize elements of this theory here. The allowed measurements are Weyl operators built from spin operators. Following Gross' phase space formalism [37], the dimension d is an odd prime number. The single-qudit Pauli spin matrices are defined by

$$X(q)\,|j\rangle = |j + q\rangle \quad \text{and} \quad Z(p)\,|j\rangle = \omega^{pj}\,|j\rangle$$

where

$$\omega = e^{2\pi i/d}$$

and addition is modulo d. A Weyl operator, represented by *phase point* coordinates in $\mathbb{Z}_d^2$, is defined by

$$W(p, q) = \omega^{-2^{-1}pq}Z(p)X(q)$$

where 2^{-1} is the multiplicative inverse of 2 in $\mathbb{Z}_d$. An n-particle Weyl operator, represented by coordinates in $\mathbb{Z}_d^{2n}$, is defined as

$$W(p_1, q_1, ..., p_n, q_n) = W(p_1, q_1) \otimes ... \otimes W(p_n, q_n).$$

For convenience, we denote a point $(p_1, q_1, ..., p_n, q_n)$ in an n-particle phase space as $(\mathbf{p}, \mathbf{q})$. The *symplectic product* of two phase space points is defined by:

$$[(\mathbf{p}, \mathbf{q}), (\mathbf{p'}, \mathbf{q'})] = \sum_{i=1}^{n} p_i q_i' - p_i' q_i.$$

Weyl operators obey a composition law:

$$W(\mathbf{p}, \mathbf{q}) W(\mathbf{p'}, \mathbf{q'}) = \omega^{2^{-1}[(\mathbf{p}, \mathbf{q}), (\mathbf{p'}, \mathbf{q'})]} W(\mathbf{p} + \mathbf{p'}, \mathbf{q} + \mathbf{q'}).$$

Therefore,

$$W(\mathbf{p}, \mathbf{q}) W(\mathbf{p'}, \mathbf{q'}) = W(\mathbf{p'}, \mathbf{q'}) W(\mathbf{p}, \mathbf{q}) = W(\mathbf{p} + \mathbf{p'}, \mathbf{q} + \mathbf{q'})$$

if and only if

$$[(\mathbf{p}, \mathbf{q}), (\mathbf{p'}, \mathbf{q'})] = 0.$$

The n-Weyl operators (with phases) form the n-Pauli group:

$$C_1^n = \{\omega^{2^{-1}m} W(\mathbf{p}, \mathbf{q}) : m \in \mathbb{Z}_{2d}, (\mathbf{p}, \mathbf{q}) \in \mathbb{Z}_d^{2n}\}.$$

The Clifford gates are those unitaries preserving the Pauli group:

$$C_2^n = \{U : U C_1^n U^\dagger \subseteq C_1^n\}.$$

The Clifford hierarchy [33] is defined inductively:

$$C_k^n = \{U : U C_1^n U^\dagger \subseteq C_{k-1}^n\}.$$

It forms a nested sequence under inclusion:

$$C_1^n \subset C_2^n \subset C_3^n \subset ....$$

The magic states we will consider arise from the strict third level of the Clifford hierarchy: $C_3^n \setminus C_2^n$. Cui, Gottesman, and Krishna [23], building on work of Campbell [18] and Howard-Vala [42], give an explicit description of all diagonal gates in the kth level. (We note that not much is presently known about the nondiagonal gates of the Clifford hierarchy.) For $d > 3$, diagonal gates of the third level are those of the form:

$$U_\Phi = \sum_{\mathbf{j} \in \mathbb{Z}_d^n} \omega^{\Phi(\mathbf{j})} |\mathbf{j}\rangle \langle \mathbf{j}|$$

where Φ is an n-variable polynomial over $\mathbb{Z}^d$ of degree 3. Every strict third-level gate yields a magic state

$$|\Phi\rangle = U_\Phi |+\rangle^{\otimes n} = d^{-n} \sum_{\mathbf{j} \in \mathbb{Z}_d^n} \omega^{\Phi(\mathbf{j})} |\mathbf{j}\rangle.$$

As an example, the two-qutrit controlled-S gate (where $S = T^2$ and T is a higher-dimensional generalisation [42] of the $\pi/8$ gate) is $U_{j_1 j_2^2} \in C_3^2$. Its corresponding magic state was computationally found to be strongly contextual in [24].

Magic states arising from diagonal third-level gates $U_\Phi \in C_3^n \setminus C_2^n$ are optimal for enabling quantum universality in that they admit direct deterministic protocols for injecting the gate U_Φ [41]. Higher-level gates require more complex injection protocols involving access to EPR pairs and ancillary resources. Gates from outside the Clifford hierarchy may be implemented via state injection; however, this is a stochastic process that requires randomly many attempts.
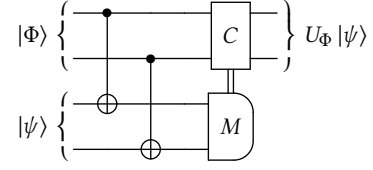

Figure 3. Schematic of a stabilizer circuit deterministically implementing a diagonal gate in the third level of the Clifford hierarchy [41]. CNOT gates entangle the input state and the magic state before a stabilizer measurement is made on the input. A Clifford correction, conditioned on the measurement outcome, is performed on the magic state lines resulting in the input having a gate applied to it.

3 Paradoxical magic states

3.1 Summary of results

We now define strong magic states as those corresponding to two-variable cubic polynomials with *no local terms*, i.e. the coefficients for the j^3, k^3 terms vanish, and show that they exhibit paradoxes with respect to stabilizer measurements:

$$\mathcal{M} = \{W(\mathbf{p}, \mathbf{q}) : (\mathbf{p}, \mathbf{q}) \in \mathbb{Z}_d^{2n}\}.$$

The contexts are the maximal commutative subsets of $\mathcal{M}$. Thus, we are concerned with *bona fide* contextuality rather than nonlocality. The possible outcomes O of measuring a Weyl operator is $\mathbb{Z}_d$ with $k \in \mathbb{Z}_d$ labelling the eigenvalue ω^k. Proofs are found in the following subsection.

Definition 1. *A two-qudit magic state*

$$|\Phi\rangle = d^{-2} \sum_{j, k \in \mathbb{Z}_d^2} \omega^{\Phi(j,k)} |j\rangle |k\rangle$$

is strong *if*

$$\Phi(j,k) = \phi_1 j^2 k + \phi_2 j k^2 + q(j,k)$$

with $q(j,k)$ being any quadratic polynomial and either ϕ_1 or $\phi_2 \not\equiv 0$.

These states are capable of injecting a gate built from arbitrary combinations of controlled-S gates on either qudit. The restrictions on local terms are not strictly necessary; they strike a balance between sufficient generality to establish a clear pattern whilst admitting tractable analytic arguments. Indeed, computations in low dimensions are consistent with the possibility that *all* magic states for diagonal $C_3^2 \setminus C_2^2$ gates in prime dimension 2 mod 3 are strongly contextual.

Theorem 1. *Suppose that the prime dimension $d \not\equiv 1 \pmod{3}$. All strong magic states $|\Phi\rangle$ are strongly contextual with respect to stabilizer measurements. It follows immediately that the states $C |\Phi\rangle$, where $|\Phi\rangle$ is strong and C is any Clifford gate, are also strongly contextual.*

We prove that for any strong magic state $|\Phi\rangle$, any Clifford gate C, and any hidden variable $\lambda : \mathbb{Z}_d^4 \to \mathbb{Z}_d$, λ is inconsistent with $C |\Phi\rangle$. After reducing to the case where $\phi_1 \not\equiv 0$, $q(j,k) = 0$, and $C = \mathbb{I}$, we show that λ must predict the occurrence of an impossible joint outcome for one of the following $d(d + 1)$ pairs of commuting measurements.

Type	Operators	Phase points
I_α	$Z \otimes \mathbb{I}$ and $\mathbb{I} \otimes Z^\alpha X$	$(1, 0, 0, 0)$ and $(0, 0, \alpha, 1)$
II_α	$\mathbb{I} \otimes Z$ and $Z^\alpha X \otimes \mathbb{I}$	$(0, 0, 1, 0)$ and $(\alpha, 1, 0, 0)$
$III_{\alpha, \beta}$	$Z \otimes Z^\beta$ and $X \otimes Z^\alpha X^{-\beta^{-1}}$	$(1, 0, \beta, 0)$ and $(0, 1, \alpha, -\beta^{-1})$

Table 1. The three families of contexts needed for our argument. Here, $\alpha, \beta \in \mathbb{Z}_d$ and $\beta \neq 0$. Operator phases omitted.

The following, surprising lemma allows us to dramatically reduce (from exponentially to polynomially many) the number of hidden variables $\lambda : \mathbb{Z}_d^{2n} \to \mathbb{Z}_d$ we must consider. It was established earlier by Delfosse *et al.* [26]; we give an independently obtained, algebraic proof in the following subsection.

Lemma 3.1. *Suppose that $n \geq 2$ and that $\lambda : \mathbb{Z}_d^{2n} \to \mathbb{Z}_d$ is a hidden variable for n-particle stabilizer quantum mechanics that is consistent with a quantum state. Then, $\lambda(\boldsymbol{p}, \boldsymbol{q}) = \boldsymbol{\lambda} \cdot (\boldsymbol{p}, \boldsymbol{q})$ for some $\boldsymbol{\lambda} \in \mathbb{Z}_d^{2n}$.*

We then establish a number-theoretic criterion for the impossibility of a joint outcomes upon performing measurements on a state $|\Phi\rangle$. A *permutation polynomial* is a (possibly multivariable) polynomial over $\mathbb{Z}_d$ that takes each value in $\mathbb{Z}_d$ equally many times:

$$\forall \mathbf{x} \in \mathbb{Z}_d^n, \quad |p^{-1}(\mathbf{x})| = d^{n-1}.$$

In general, the problem of determining whether a polynomial over a finite field is a permutation polynomial is a difficult one; its study remains an active area of number theory [40].

Lemma 3.2. *The joint outcome (A, B) is impossible for the measurement of $U = W(\boldsymbol{p}, \boldsymbol{q})$ and $V = W(\boldsymbol{p'}, \boldsymbol{q'})$ with $[U, V] = 0$ on the state $|\Phi\rangle$ if and only if, for all $(j, k) \in \mathbb{Z}_d^2$, the polynomial $\Psi(x, y)$ is a permutation polynomial where*

$$\begin{aligned}
\Psi(x, y) = &-xA - yB - 2^{-1}((xp_1 + yp_1')(xq_1 + yq_1') + (xp_2 \\
&+ yp_2')(xq_2 + yq_2')) + j(xp_1 + yp_1') + k(xp_2 + yp_2') \\
&+ \Phi(j - (xq_1 + yq_1'), k - (xq_2 + yq_2')).
\end{aligned}$$

We will require elements of Dickson's classification of one-variable permutation polynomials over finite fields of low degree [27].

Theorem 2 (Dickson, 1896). *Suppose d is a prime power, $d \not\equiv 1 \pmod 3$ and $f : \mathbb{Z}_d \to \mathbb{Z}_d$ is a polynomial of degree at most 3. Then, f is a permutation polynomial if and only if $f(x) = ag(x + b) + c$ where $a \neq 0$ and $g(x) = x$ or x^3.*

By Lemma 3.1, a hidden variable λ prescribes to $W(p_1, q_1, p_2, q_2)$ the outcome $\lambda_1 p_1 + \lambda_2 q_1 + \lambda_3 p_2 + \lambda_4 q_2$. By substituting the phase points of our chosen measurements, the coefficients of the polynomial describing the state $|\Phi\rangle$, and the outcomes prescribed by a hidden variable λ into the master equation of Lemma 3.2, we see that inconsistency of λ with $|\Phi\rangle$ for the measurements of Table 1 is equivalent to one of the following $d(d + 1)$ polynomials being a

permutation polynomial for all possible choices of $j, k \in \mathbb{Z}_d$:

$$\begin{aligned}
\Psi_{I_\alpha}(x, y) = &\, x(j - \lambda_2) + y^2(j\phi_2 - 2^{-1}\alpha) + y(\alpha(k - \lambda_4) - \lambda_3 \\
&- j^2\phi_1 - 2jk\phi_2)
\end{aligned}$$

$$\begin{aligned}
\Psi_{II_\alpha}(x, y) = &\, x(k - \lambda_4) + y^2(k\phi_1 - 2^{-1}\alpha) + y(\alpha(j - \lambda_2) - \lambda_1 \\
&- k^2\phi_2 - 2jk\phi_1)
\end{aligned}$$

$$\begin{aligned}
\Psi_{III_{\alpha, \beta}}(x, y) = &\, x(j - \lambda_2 + \beta(k - \lambda_4)) + y^3(\beta^{-1}(\phi_1 - \beta^{-1}\phi_2) \\
&+ y^2(\beta^{-1}(2^{-1}\alpha - 2j\phi_1 - 2k\phi_2 + \beta^{-1}j\phi_2) + k\phi_1) \\
&+ y(\alpha(k - \lambda_4) + \beta^{-1}(\lambda_3 + j^2\phi_1 + 2jk\phi_2) - \lambda_1 \\
&- 2jk\phi_1 - k^2\phi_2)
\end{aligned}$$

In the next subsection, we prove by inspection that this must hold and, thus, that no hidden variable is consistent with $|\Phi\rangle$. We conclude that all strong magic states are strongly contextual with respect to stabilizer operations.

3.2 Proofs of main results

Here, we provide explicit details of the proofs of the main results. First, we establish that the algebraic relations between commuting Weyl operators enforce a strong condition on hidden variables: they must be group homomorphisms from phase space to outcomes. This dramatically reduces (from $d^{d^{2n}}$ functions to d^{2n} homomorphisms) the number of hidden variables we need to consider. The assumption of multiple qudits is crucial here.

Lemma 3.1. *Suppose that $n \geq 2$ and that $\lambda : \mathbb{Z}_d^{2n} \to \mathbb{Z}_d$ is a hidden variable for n-particle stabilizer quantum mechanics that is consistent with a quantum state. Then, $\lambda(\boldsymbol{p}, \boldsymbol{q}) = \boldsymbol{\lambda} \cdot (\boldsymbol{p}, \boldsymbol{q})$ for some $\boldsymbol{\lambda} \in \mathbb{Z}_d^{2n}$.*

Proof. The hidden variable λ prescribes the outcome $\lambda(\mathbf{p}, \mathbf{q})$ to $W(\mathbf{p}, \mathbf{q})$. If λ is consistent with a quantum state, these outcomes must respect the algebraic relations between commuting Weyl operators:

$$\lambda(\mathbf{p}, \mathbf{q}) + \lambda(\mathbf{p'}, \mathbf{q'}) = \lambda(\mathbf{p+p'}, \mathbf{q+q'})$$

whenever

$$[(\mathbf{p}, \mathbf{q}), (\mathbf{p'}, \mathbf{q'})] = 0.$$

Thus, when $n = 2$:

$$\lambda(p_1, q_1, p_2, q_2) = \lambda(p_1, q_1, 0, 0) + \lambda(0, 0, p_2, q_2)$$

and, whenever $p_1 q_1 = -p_2 q_2$, we have that

$$\begin{aligned}
\lambda(p_1, q_1, p_2, q_2) &= \lambda(p_1, 0, p_2, 0) + \lambda(0, q_1, 0, q_2) \\
&= \lambda(p_1, 0, 0, 0) + \lambda(0, 0, p_2, 0) \\
&\quad + \lambda(0, q_1, 0, 0) + \lambda(0, 0, 0, q_2).
\end{aligned}$$

Thus, λ is linear in phase coordinates for the first qudit:

$$\lambda(1, k, 0, 0)$$

$$= \lambda(1, k, 0, -2^{-1}k) + \lambda(0, 0, 0, 2^{-1}k)$$

$$= [\lambda(1, 2^{-1}k, 1, -2^{-1}k) + \lambda(0, 2^{-1}k, -1, 0)] + \lambda(0, 0, 0, 2^{-1}k)$$

$$= [\lambda(1, 0, 0, 0) + \lambda(0, 2^{-1}k, 0, 0) + \lambda(0, 0, 1, 0) + \lambda(0, 0, 0, -2^{-1}k)]$$

$$\quad + [\lambda(0, 2^{-1}k, 0, 0) + \lambda(0, 0, -1, 0)] + \lambda(0, 0, 0, 2^{-1}k)$$

$$= \lambda(1, 0, 0, 0) + \lambda(0, k, 0, 0)$$

Similarly, $\lambda(0, 0, 1, k) = \lambda(0, 0, 1, 0) + \lambda(0, 0, 0, k)$. Thus, λ is linear. For $n > 2$, the same argument holds. □

Next, we establish a master equation governing the possibility vs. impossibility of observing a given joint outcome upon measurement of a pair of commuting Weyl measurements on a state $|\Phi\rangle$. The lemma is easily extended to more qudits/measurements and to polynomials Φ of any degree and holds for any prime dimension d.

Lemma 3.2. *The joint outcome (A, B) is impossible for the measurement of $U = W(\boldsymbol{p}, \boldsymbol{q})$ and $V = W(\boldsymbol{p'}, \boldsymbol{q'})$ with $[U, V] = 0$ on the state $|\Phi\rangle$ if and only if, for all $(j, k) \in \mathbb{Z}_d^2$, the polynomial $\Psi(x, y)$ is a permutation polynomial where*

$$\Psi(x, y) = -xA - yB - 2^{-1}((xp_1 + yp_1')(xq_1 + yq_1') + (xp_2$$
$$+ yp_2') + (xq_2 + yq_2')) + j(xp_1 + yp_1') + k(xp_2 + yp_2')$$
$$+ \Phi(j - (xq_1 + yq_1'), k - (xq_2 + yq_2')).$$

Proof. The eigenvalues of a Weyl operator W are ω^k for $k \in \mathbb{Z}_d$. The projection onto the 1-eigenspace of W is given by

$$\Pi(0|W) = d^{-1} \sum_{x \in \mathbb{Z}_d} W^x.$$

This can be seen by noting that $W^d = \mathbb{I}$, $W^\dagger = W^{-1}$. Therefore, the projection onto the ω^k-eigenspace of W is given by

$$\Pi(k|W) = d^{-1} \sum_{x \in \mathbb{Z}_d} \omega^{-xk} W^x.$$

Measuring $U = W(\mathbf{p}, \mathbf{q})$ and $V = W(\mathbf{p'}, \mathbf{q'})$ with $[U, V] = 0$ and obtaining the joint outcome $(A, B) \in \mathbb{Z}_d^2$ corresponds to the projection:

$$\Pi(A, B|U, V) = \Pi(A|U)\Pi(B|V)$$
$$= d^{-2}(\sum_{x \in \mathbb{Z}_d} \omega^{-xA} U^x)(\sum_{y \in \mathbb{Z}_d} \omega^{-yB} V^y)$$
$$= d^{-2} \sum_{x, y \in \mathbb{Z}_d} \omega^{-xA - yB} U^x V^y$$
$$= d^{-2} \sum_{x, y \in \mathbb{Z}_d} \omega^{-xA - yB} W(\mathbf{P}, \mathbf{Q})$$
$$= d^{-2} \sum_{x, y \in \mathbb{Z}_d} \omega^{-xA - yB - 2^{-1}(\mathbf{P} \cdot \mathbf{Q})} Z(P_1) X(Q_1) \otimes Z(P_2) X(Q_2)$$

where $(\mathbf{P}, \mathbf{Q})$ is shorthand for $x(\mathbf{p}, \mathbf{q}) + y(\mathbf{p'}, \mathbf{q'})$.

Applying this to a two-qudit magic state $|\Phi\rangle = d^{-2} \sum_{j, k \in \mathbb{Z}_d} \omega^{\Phi(j, k)} |j\rangle |k\rangle$, we obtain:

$$\Pi(A, B|U, V) |\Phi\rangle = d^{-4} \sum_{x, y \in \mathbb{Z}_d} \sum_{j, k \in \mathbb{Z}_d} \omega^{-xA - yB - 2^{-1}(P_1 Q_1 + P_2 Q_2) + \Phi(j, k)} Z(P_1) X(Q_1) \otimes Z(P_2) X(Q_2) |j\rangle |k\rangle$$
$$= d^{-4} \sum_{x, y \in \mathbb{Z}_d} \sum_{j, k \in \mathbb{Z}_d} \omega^{-xA - yB - 2^{-1}(P_1 Q_1 + P_2 Q_2) + \Phi(j, k)} Z(P_1) \otimes Z(P_2) |j + Q_1\rangle |k + Q_2\rangle$$
$$= d^{-4} \sum_{x, y \in \mathbb{Z}_d} \sum_{j, k \in \mathbb{Z}_d} \omega^{-xA - yB - 2^{-1}(P_1 Q_1 + P_2 Q_2) + \Phi(j - Q_1, k - Q_2)} Z(P_1) \otimes Z(P_2) |j\rangle |k\rangle$$
$$= d^{-4} \sum_{j, k \in \mathbb{Z}_d} \sum_{x, y \in \mathbb{Z}_d} \omega^{-xA - yB - 2^{-1}(P_1 Q_1 + P_2 Q_2) + jP_1 + kP_2 + \Phi(j - Q_1, k - Q_2)} |j\rangle |k\rangle$$

Observing the joint outcome (A, B) for the measurements U, V on the state $|\Phi\rangle$ is impossible precisely when $\Pi(A, B|U, V) |\Phi\rangle = 0$; that is, when the terms

$$\sum_{x, y \in \mathbb{Z}_d} \omega^{-xA - yB - 2^{-1}(P_1 Q_1 + P_2 Q_2) + jP_1 + kP_2 + \Phi(j - Q_1, k - Q_2)}$$

vanish for all $j, k \in \mathbb{Z}_d$. Such a term is a sum of d^2 many primitive d^{th}-roots of unity and, since d is prime, it vanishes if and only if each dth-root appears d many times. Thus, impossibility of the measurement outcome is equivalent to

$$\Psi(x, y) = -xA - yB - 2^{-1}((xp_1 + yp_1')(xq_1 + yq_1') + (xp_2$$
$$+ yp_2') + (xq_2 + yq_2')) + j(xp_1 + yp_1') + k(xp_2 + yp_2')$$
$$+ \Phi(j - (xq_1 + yq_1'), k - (xq_2 + yq_2'))$$

being a permutation polynomial in x, y for all $j, k \in \mathbb{Z}_d$. □

We are now ready to prove our main theorem.

Theorem 1. *Suppose that the prime dimension $d \not\equiv 1 \pmod 3$. All strong magic states $|\Phi\rangle$ are strongly contextual with respect to stabilizer measurements. It follows immediately that the states $C |\Phi\rangle$,*

where $|\Phi\rangle$ is strong and C is any Clifford gate, are also strongly contextual.

Proof. Suppose

$$|\Phi\rangle = d^{-2} \sum_{j, k \in \mathbb{Z}_d^2} \omega^{\Phi(j, k)} |j\rangle |k\rangle$$
$$= d^{-2} \sum_{j, k \in \mathbb{Z}_d^2} \omega^{\phi_1 j^2 k + \phi_2 j k^2 + q(j, k)} |j\rangle |k\rangle$$

is a strong magic state and C is any Clifford gate. As Clifford gates act as permutations on the Pauli operators under conjugation, they preserve all properties of contextuality with respect to stabilizer measurements. Therefore, by constructing the diagonal Clifford gate $U_q = \sum_{j, k \in \mathbb{Z}_d^2} \omega^{q(j, k)} |j\rangle |k\rangle \langle k| \langle j|$, we can apply the Clifford gate $(C U_q)^\dagger$ to $C |\Phi\rangle$ and find that $C |\Phi\rangle$ is strongly contextual if and only if the state $d^{-2} \sum_{j, k \in \mathbb{Z}_d^2} \omega^{\phi_1 j^2 k + \phi_2 j k^2} |j\rangle |k\rangle$ is. So, without loss of generality, $C = \mathbb{I}$ and $\Phi(j, k) = \phi_1 j^2 k + \phi_2 j k^2$ with either $\Phi_1 \not\equiv 0$ or $\Phi_2 \not\equiv 0$. By possibly swapping qudits, we can assume that $\Phi_1 \not\equiv 0$.

To prove that $|\Phi\rangle$ is strongly contextual, we must prove that every possible hidden variable $\lambda : \mathbb{Z}_d^{2n} \to \mathbb{Z}_d$ is inconsistent with $|\Phi\rangle$. Given a pair of state and hidden variable, we will show that for one of the contexts of Table 1, the joint outcome predicted by λ to occur will, in fact, have probability zero of being the result of performing the measurements of that context on the state $|\Phi\rangle$. More specifically, we will show that if a λ predicts joint outcomes with nonzero probability for all contexts of type I_α and II_α, it must predict a joint outcome with probability zero for the measurements of some context of type $\mathrm{III}_{\alpha,\beta}$.

Type	Operators	Phase points
I_α	$Z \otimes \mathbb{I}$ and $\mathbb{I} \otimes Z^\alpha X$	$(1, 0, 0, 0)$ and $(0, 0, \alpha, 1)$
II_α	$\mathbb{I} \otimes Z$ and $Z^\alpha X \otimes \mathbb{I}$	$(0, 0, 1, 0)$ and $(\alpha, 1, 0, 0)$
$\mathrm{III}_{\alpha,\beta}$	$Z \otimes Z^\beta$ and $X \otimes Z^\alpha X^{-\beta^{-1}}$	$(1, 0, \beta, 0)$ and $(0, 1, \alpha, -\beta^{-1})$

Table 1. The three families of contexts needed for our argument. Here, $\alpha, \beta \in \mathbb{Z}_d$ and $\beta \neq 0$. Operator phases omitted.

By Lemma 3.1, λ prescribes to $W(p_1, q_1, p_2, q_2)$ the outcome $\lambda_1 p_1 + \lambda_2 q_1 + \lambda_3 p_2 + \lambda_4 q_2$. By substituting the phase points of our chosen measurements, the coefficients of the polynomial describing the state $|\Phi\rangle$, and the outcomes prescribed by a hidden variable λ into the master equation of Lemma 3.2, we see that inconsistency of λ with $|\Phi\rangle$ for the measurements of Table 1 is equivalent to one of the following $d(d+1)$ polynomials being a permutation polynomial for all possible choices of $j, k \in \mathbb{Z}_d$:

$$\Psi_{\mathrm{I}_\alpha}(x, y) = x(j - \lambda_2) + y^2(j\phi_2 - 2^{-1}\alpha) + y(\alpha(k - \lambda_4) - \lambda_3 - j^2\phi_1 - 2jk\phi_2)$$

$$\Psi_{\mathrm{II}_\alpha}(x, y) = x(k - \lambda_4) + y^2(k\phi_1 - 2^{-1}\alpha) + y(\alpha(j - \lambda_2) - \lambda_1 - k^2\phi_2 - 2jk\phi_1)$$

$$\Psi_{\mathrm{III}_{\alpha,\beta}}(x, y) = x(j - \lambda_2 + \beta(k - \lambda_4)) + y^3(\beta^{-1}(\phi_1 - \beta^{-1}\phi_2)) + y^2(\beta^{-1}(2^{-1}\alpha - 2j\phi_1 - 2k\phi_2 + \beta^{-1}j\phi_2) + k\phi_1) + y(\alpha(k - \lambda_4) + \beta^{-1}(\lambda_3 + j^2\phi_1 + 2jk\phi_2) - \lambda_1 - 2jk\phi_1 - k^2\phi_2)$$

We have dropped all terms constant in x, y as the translation of a permutation polynomial is still a permutation polynomial. Notice that all the above polynomials $p(x, y)$ in x, y are the sum of two single-variable polynomials $p_x(y), p_y(y)$ in x and y: $p(x, y) = p_x(x) + p_y(y)$. If $p_x(x)$ is a single-variable permutation polynomial, it follows that $p(x, y)$ is a two-variable permutation polynomial. Our proof thereby proceeds by closely analysing these polynomials and repeatedly applying Dickson's theorem (Theorem 2).

First, consider $\Psi_{\mathrm{I}_\alpha}(x, y)$ for $\alpha = 2\lambda_2\phi_2$. If λ is consistent with $|\Phi\rangle$, there must exist a pair $j, k \in \mathbb{Z}_d$ for which Ψ_{I_α} is *not* a permutation polynomial in x, y. When $j \neq \lambda_2$, $\Psi_{\mathrm{I}_\alpha}(x, y)$ is the sum of a nonzero linear term in x (a single-variable permutation polynomial) and a polynomial in y; thus, it is a permutation polynomial in x, y. Therefore, $j = \lambda_2$. Making this substitution, the x term vanishes and, by our choice of α, so does the coefficient for the y^2 term. As Ψ_{I_α} is simply linear in y and, by assumption, not a permutation

polynomial, its linear coefficient must vanish. Thus, either λ is inconsistent with $|\Phi\rangle$ or $\lambda_3 = -\lambda_2(2\lambda_4\phi_2 + \lambda_2\phi_1)$.

By a similar analysis of $\Psi_{\mathrm{II}_\alpha}(x, y)$, we find that by choosing $\alpha = 2\lambda_4\phi_1$, either λ is inconsistent with $|\Phi\rangle$ or $\lambda_1 = -\lambda_4(2\lambda_2\phi_1 + \lambda_4\phi_2)$.

Finally, we make the substitutions for λ_1, λ_3 in $\Psi_{\mathrm{III}_{\alpha,\beta}}(x, y)$ and note that, as they too are linear in x, they are permutation polynomials unless $j = \lambda_2 - \beta(k - \lambda_4)$. For convenience, we multiply the resulting expression by $\beta \neq 0$:

$$y^3(\phi_1 - \beta^{-1}\phi_2) + y^2(2^{-1}\alpha + 3k(\beta\phi_1 - \phi_2) + \beta^{-1}\lambda_2\phi_2 + \lambda_4\phi_2$$
$$- 2\beta\lambda_4\phi_1 - 2\lambda_2\phi_1) + y(3\beta k^2(\beta\phi_1 - \phi_2) + k(\beta(\alpha - 4\lambda_2\phi_1$$
$$+ 2\lambda_4\phi_2) - 4\beta^2\lambda_4\phi_1 + 2\lambda_2\phi_2) + \beta(-\alpha\lambda_4 + \lambda_4^2\phi_2 + 4\lambda_2\lambda_4\phi_1)$$
$$+ \beta^2\lambda_4^2\phi_1 - 2\lambda_2\lambda_4\phi_2)$$

We consider two cases. First, if $\phi_2 \equiv -1$, then, by choosing $\alpha = 6(\lambda_2\phi_1 - \lambda_4)$ and $\beta = \phi_1^{-1}$, the resulting polynomial factors as:

$$2(y + \phi_1^{-1}(k - \lambda_4))^3.$$

However, if $\phi_2 \not\equiv -1$, we may choose $\alpha = 2(\phi_2 + 1)^{-1}(\lambda_2\phi_1(\phi_2 + 2) + \lambda_4(\phi_2^2 - 1))$ and $\beta = \phi_1^{-1}(\phi_2 + 1)$; the resulting polynomial factors as:

$$(y + \phi_1^{-1}(k - \lambda_4)(\phi_2 + 1))^3.$$

In both cases, the type III polynomial, for our choices of α and β, is a permutation polynomial for all $j, k \in \mathbb{Z}_d$ and, therefore, λ is inconsistent with $|\Phi\rangle$. We conclude that $|\Phi\rangle$ is strongly contextual with respect to two-qudit stabilizer measurements. □

4 Conclusions

The surprising finding of an abundance of exotic quantum paradoxes (of arbitrarily large dimension) among those magic states that are optimal as resources for quantum computation bolsters a refinement of the resource theory of contextuality that emphasises the computational power of logical paradoxes. This intuitive hypothesis for the origin of the computational advantages provided by contextuality emerges from observing the pattern across informatic settings of determinstic advantages enabled by strongly contextual resources together with the view of standard contextuality as a stochastic mixture of classical and paradoxical parts [4]. It is rendered more compelling by its applicability in the experimentally tractable setting of universal quantum computation via state injection.

A key desideratum of a property of systems considered to be a resource is that the benefits conferred scale with the strength of that property. Thus, our results validate both the idea of contextuality as an essential resource in quantum computation and seeing logical paradoxes as a highly useful resource-theoretic notion of extremal contextuality among many potential measures of contextuality.

Outside of purely communicational tasks, it is in the setting of measurement-based computation where the centrality of logical paradoxes to enabling advantage has been made most clear. Here, the classical part of a resource offers no benefits; it is the paradox that does all the work. Our results differ from this setting in two critical ways. There, paradoxes enable enlarging the class of finite functions that can be computed (with resources that may be quantum) whereas our interest is in enabling full-blown universal quantum computation in the circuit model (with resources that must be quantum).

The second key difference is that measurement-based computation, framed entirely in terms of measurements on a resource

state, is naturally suited to analysis in terms of contextuality. In the circuit-based model, it is *transformations* of a system that performs the computational work which adds a layer of conceptual obstacles to a fine-grained analysis of how contextuality powers computation. Nevertheless, the salience of the logical perspective survives in the complex setting of quantum computation.

4.1 Future work

We indicate questions for future work in two main directions: along purely logical lines towards developing a structural understanding of how contextuality enables computational advantage, and along concretely quantum computational lines.

The most immediate task is to precisely delineate the mechanism by which paradoxes aid in achieving computational advantage. This is most clearly done in a purely logical setting, without the complications and excessive assumptions of choosing a physical theory. By interpreting these results within quantum theory, such logical insights can be practically applied. As this work takes place in the circuit model of quantum computing which explicitly involves transformations of a physical system (in contrast to the measurement-based setting of previous work) this raises the question of how to incorporate dynamical aspects into frameworks of contextual logic. Given the adaptivity of measurements in measurement-based computational models, there is the need to incorporate causality into frameworks of contextual logic. One might then ask: what is the interaction between causal structures on measurements and the aforementioned dynamical aspects? Furthermore, can the distillation of weak contextuality into strong computational resources, exemplified in the quantum setting by the magic state distillation protocol, be understood at a logical level?

At a concrete level, our work leaves open the question of a complete classification of quantum paradoxes in qudit stabilizer mechanics. It also raises questions about the exact nature of the mutual relationships between the Clifford hierarchy, quantum resources for deterministic injection, and strong contextuality. For example, it is reasonable to conjecture that every strongly contextual two-qudit state admits a deterministic injection protocol enabling universal quantum computation. It remains open whether these magic state-based paradoxes admit cohomological witnesses [7, 50] or whether it is possible to relate the contextual fraction of a magic state to the difficulty or length of its associated protocols for distillation/injection.

Acknowledgments

References

[1] S. Abramsky, R. S. Barbosa, G. Carú, N. de Silva, K. Kishida, and S. Mansfield. 2017. Minimum quantum resources for strong non-locality. In *Theory Quant. Comp. Comm. Crypt. (TQC) 2017*.

[2] S. Abramsky, R. S. Barbosa, N. de Silva, and O. Zapata. 2017. The quantum monad on relational structures. In *Math. Found. Comp. Sci. (MFCS) 2017*, Vol. 83. 35:1–35:19.

[3] S. Abramsky, R. S. Barbosa, K. Kishida, R. Lal, and S. Mansfield. 2016. Possibilities determine the combinatorial structure of probability polytopes. *J. Math. Psych.* 74 (2016), 58–65.

[4] S. Abramsky, R. S. Barbosa, and S. Mansfield. 2017. Contextual fraction as a measure of contextuality. *Phys. Rev. Lett.* 119 (2017), 050504.

[5] S. Abramsky and A. Brandenburger. 2011. The sheaf-theoretic structure of non-locality and contextuality. *New J. Phys.* 13, 11 (2011), 113036.

[6] S. Abramsky and L. Hardy. 2012. Logical Bell inequalities. *Phys. Rev. A* 85, 6 (2012), 062114.

[7] S. Abramsky, R. S. Barbosa, K. Kishida, R. Lal, and S. Mansfield. 2015. Contextuality, cohomology and paradox. In *Comp. Sci. Logic (CSL) 2015*, Vol. 41. 211–228.

[8] A. Acín, T. Fritz, A. Leverrier, and A. B. Sainz. 2015. A combinatorial approach to nonlocality and contextuality. *Comm. Math. Phys.* 334, 2 (2015), 533–628.

[9] J. Anders and D. E. Browne. 2009. Computational power of correlations. *Phys. Rev. Lett.* 102, 5 (2009), 050502.

[10] A. Aspect, P. Grangier, and G. Roger. 1982. Experimental Realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment. *Phys. Rev. Lett.* 49 (1982), 91–94.

[11] A. Atserias, P. G. Kolaitis, and S. Severini. 2017. Generalized satisfiability problems via operator assignments. In *Fund. Comp. Theory (FCT) 2017*, Vol. 10472. 56–68.

[12] J. Barrett, A. Kent, and S. Pironio. 2006. Maximally nonlocal and monogamous quantum correlations. *Phys. Rev. Lett.* 97, 17 (2006), 170409.

[13] J. S. Bell. 1964. On the Einstein-Podolsky-Rosen paradox. *Physics* 1, 3 (1964), 195–200.

[14] J. S. Bell. 1966. On the problem of hidden variables in quantum mechanics. *Rev. Mod. Phys.* 38, 3 (1966), 447.

[15] S. Bravyi and A. Kitaev. 2005. Universal quantum computation with ideal Clifford gates and noisy ancillas. *Phys. Rev. A* 71, 2 (2005), 022316.

[16] J. Briët, H. Buhrman, T. Lee, and T. Vidick. 2013. Multipartite entanglement in XOR games. *Quant. Inf. & Comp.* 13, 3-4 (2013), 334–360.

[17] A. Cabello, S. Severini, and A. Winter. 2014. Graph-theoretic approach to quantum correlations. *Phys. Rev. Lett.* 112, 4 (2014), 040401.

[18] E. T. Campbell. 2014. Enhanced fault-tolerant quantum computing in d-level systems. *Phys. Rev. Lett.* 113, 23 (2014), 230501.

[19] R. Cleve, P. Hoyer, B. Toner, and J. Watrous. 2004. Consequences and limits of nonlocal strategies. In *Proc. 19th IEEE Computational Complexity*. 236–249.

[20] R. Cleve and R. Mittal. 2014. Characterization of binary constraint system games. In *ICALP 2014*. 320–331.

[21] C. Cormick, E. F. Galvão, D. Gottesman, J. P. Paz, and A. O. Pittenger. 2006. Classicality in discrete Wigner functions. *Phys. Rev. A* 73, 1 (2006), 012301.

[22] T. S. Cubitt, D. Leung, W. Matthews, and A. Winter. 2010. Improving zero-error classical communication with entanglement. *Phys. Rev. Lett.* 104, 23 (2010), 230503.

[23] S. X. Cui, D. Gottesman, and A. Krishna. 2017. Diagonal gates in the Clifford hierarchy. *Phys. Rev. A* 95, 1 (2017), 012329.

[24] N. de Silva. 2017. Graph-theoretic strengths of contextuality. *Phys. Rev. A* 95, 3 (2017), 032108.

[25] N. Delfosse, P. Allard Guerin, J. Bian, and R. Raussendorf. 2015. Wigner function negativity and contextuality in quantum computation on rebits. *Phys. Rev. X* 5, 2 (2015), 021003.

[26] N. Delfosse, C. Okay, J. Bermejo-Vega, D. E. Browne, and R. Raussendorf. 2017. Equivalence between contextuality and negativity of the Wigner function for qudits. *New J. Phys.* 19, 12 (2017), 123024.

[27] L. E. Dickson. 1896. The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group. *Ann. Math.* 11 (1896), 65–120.

[28] A. Einstein, B. Podolsky, and N. Rosen. 1935. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.* 47 (1935), 777–780.

[29] A. C. Elitzur, S. Popescu, and D. Rohrlich. 1992. Quantum nonlocality for each pair in an ensemble. *Phys. Lett. A* 162, 1 (1992), 25–28.

[30] A. Fine. 1982. Hidden variables, joint probability, and the Bell inequalities. *Phys. Rev. Lett.* 48, 5 (1982), 291.

[31] E. F. Galvão. 2005. Discrete Wigner functions and quantum computational speedup. *Phys. Rev. A* 71, 4 (2005), 042302.

[32] K. S. Gibbons, M. J. Hoffman, and W. K. Wootters. 2004. Discrete phase space based on finite fields. *Phys. Rev. A* 70, 6 (2004), 062101.

[33] D. Gottesman. 1997. *Stabilizer codes and quantum error correction*. Ph.D. Dissertation. Caltech.

[34] D. Gottesman. 1998. Theory of fault-tolerant quantum computation. *Phys. Rev. A* 57 (1998), 127–137.

[35] D. Gottesman and I. Chuang. 1999. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature* 402, 6760 (1999), 390–393.

[36] D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger. 1990. Bell's theorem without inequalities. *Am. J. Phys.* 58, 12 (1990), 1131–1143.

[37] D. Gross. 2006. Hudson's theorem for finite-dimensional quantum systems. *J. Math. Phys.* 47, 12 (2006), 122107.

[38] A. Grudka, K. Horodecki, M. Horodecki, P. Horodecki, R. Horodecki, P. Joshi, W. Kłobus, and A. Wójcik. 2014. Quantifying contextuality. *Phys. Rev. Lett.* 112 (2014), 120401.

[39] B. Hensen et al. 2015. Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. *Nature* 526, 7575 (2015), 682–686.

[40] X. Hou. 2015. Permutation polynomials over finite fields—a survey of recent advances. *Finite Fields and Their Applications* 32 (2015), 82–119.

[41] M. Howard and E. Campbell. 2017. Application of a resource theory for magic states to fault-tolerant quantum computing. *Phys. Rev. Lett.* 118, 9 (2017), 090501.

[42] M. Howard and J. Vala. 2012. Qudit versions of the qubit $\pi/8$ gate. *Phys. Rev. A* 86, 2 (2012), 022316.

[43] M. Howard, J. Wallman, V. Veitch, and J. Emerson. 2014. Contextuality supplies the 'magic' for quantum computation. *Nature* 510, 7505 (2014), 351–355.

[44] K. Kishida. 2016. Logic of local inference for contextuality in quantum physics and beyond. In *ICALP 2016*, Vol. 55. 113:1–113:14.

[45] M. Kleinmann, O. Gühne, J. R. Portillo, J. Larsson, and A. Cabello. 2011. Memory cost of quantum contextuality. *New J. Phys.* 13, 11 (2011), 113011.

[46] A. A. Klyachko, M. Ali Can, S. Binicioğlu, and A. S. Shumovsky. 2008. A simple test for hidden variables in spin-1 system. *Phys. Rev. Lett.* 101, 2 (2008), 020403.

[47] S. Kochen and E. P. Specker. 1967. The problem of hidden variables in quantum mechanics. *J. Math. Mech.* 17 (1967), 59–87.

[48] A. Mari and J. Eisert. 2012. Positive Wigner functions render classical simulation of quantum computation efficient. *Phys. Rev. Lett.* 109, 23 (2012), 230503.

[49] N. D. Mermin. 1993. Hidden variables and the two theorems of John Bell. *Rev. Mod. Phys.* 65, 3 (1993), 803.

[50] C. Okay, S. Roberts, S. D. Bartlett, and R. Raussendorf. 2017. Topological proofs of contextuality in quantum mechanics. *Quant. Inf. & Comp.* 17, 13-14 (2017), 1135–1166.

[51] H. Pashayan, J. J. Wallman, and S. D. Bartlett. 2015. Estimating outcome probabilities of quantum circuits using quasiprobabilities. *Phys. Rev. Lett.* 115, 7 (2015), 070501.

[52] A. Peres. 1999. All the Bell inequalities. *Found. Phys.* 29, 4 (1999), 589–614.

[53] S. Popescu and D. Rohrlich. 1994. Quantum nonlocality as an axiom. *Found. Phys.* 24, 3 (1994), 379–385.

[54] R. Raussendorf. 2013. Contextuality in measurement-based quantum computation. *Phys. Rev. A* 88, 2 (2013), 022322.

[55] R. Raussendorf and H. J. Briegel. 2001. A one-way quantum computer. *Phys. Rev. Lett.* 86, 22 (2001), 5188.

[56] W. van Dam. 1999. *Nonlocality & communication complexity*. Ph.D. Dissertation.

[57] V. Veitch, C. Ferrie, D. Gross, and J. Emerson. 2012. Negative quasi-probability as a resource for quantum computation. *New J. Phys.* 14, 11 (2012), 113011.

[58] V. Veitch, H. Mousavian, D. Gottesman, and J. Emerson. 2014. The resource theory of stabilizer quantum computation. *New J. Phys.* 16, 1 (2014), 013009.

[59] W. K. Wootters. 1986. The discrete Wigner function. *Ann. N. Y. Acad. Sci.* 480, 1 (1986), 275–282.