Non-classical logic of classically universal measurement-based quantum computation

Leon Loveridge*1, Raouf Dridi†1 and Robert Raussendorf‡1

1Department of Physics and Astronomy, University of British Columbia.

August 5, 2014

Abstract

We report first steps towards elucidating the relationship between contextuality, measurement-based quantum computation (MBQC) and the non-classical logic of a topos associated with the computation. We show that in a class of MBQC, classical universality requires non-classical logic, which is “consumed” during the course of the computation, therefore pinpointing another potential quantum computational resource.

1 Introduction

The quantum mechanical description of the world has startling features which are quite alien from a classical point of view. Epitomising the structural differences from classical physics includes the existence of entangled states, non-commutative observable algebras and the necessary disturbances caused by measurement. Less well known is the impossibility of assigning values to quantum observables whilst preserving some basic functional relations – a trait known as contextuality and a central concept in this paper.

An upshot of the mathematical structure of quantum theory is the possibility of attaining certain advantages over classical physics in regard to computation; there now exist numerous examples of quantum protocols which far outperform their classical analogues, which are well documented in the literature. However, the origin of the quantum advantage remains unclear; “largeness” of Hilbert space, superposition, interference, and entanglement have been suggested as candidates in the past. Whilst being supported in a variety of situations [1–4], each of these has also met with objection [4–7]. Recently, contextuality has been
proposed as a contender for the source of the speedup in quantum computation; it has been observed that for quantum computation with a restricted gate set and injection of magic states [8], contextuality is necessary for both quantum computational universality and the hardness of classical simulation of quantum computation [9, 10].

Contextuality also plays a role in measurement-based quantum computation (MBQC). If an MBQC on qubits evaluates a non-linear (Boolean) function (in which case the computation is classically universal) with high probability of success, this computation is also contextual [11]. Therefore, for MBQC, contextuality is important not only for what can be computed efficiently, but for what can be computed at all.

The simplest example of this is the execution of an OR-gate using Pauli measurements on a 3-qubit Greenberger-Horne-Zeilinger (GHZ) state [12]. This gate is Mermin’s proof [13] of the Kochen-Specker theorem in Hilbert space-dimension 8, recast as a simple quantum computation.

In this paper we offer a perspective related to contextuality but distinct from it: that a quantum-over-classical advantage arises from the non-classical internal logic of the given computation (we shall treat “classical” and “Boolean” as synonyms). Specifically, we associate a particular topos to the computation which comes equipped with a natural logical structure, and show that the topos logic is non-Boolean whenever contextuality is present. With [11] we find that if the topos logic is Boolean, the MBCQ may only compute linear functions. Hence non-Booleanness is a necessary condition for quantum computational advantage in the class of computations we discuss.

Boolean logic was devised in the first instance as a formalisation of the “Laws of Thought” [14], i.e., as a way of consistently reasoning about the (classical) world. Many years have passed since Boole’s seminal contribution; a modern connection to Boolean logic is the theory of (classical) computation. The quantum analogue—the relationship between quantum computation and “quantum logic”—has thus far remained largely unexplored (though there are exceptions; see [15] for a version of “quantum computational logic”, and the work of Abramsky, Coecke and coworkers (e.g., [16])). In this paper we make some inroads into this territory.

Soon after the mathematical structure of quantum mechanics was essentially crystalised it was realised that the logical structure of the theory was fundamentally different from that found in classical physics [17]. Though there are now many candidates for the “logic of quantum theory” (see, for example, [15]), we choose to follow the topos approach initiated by Isham and Butterfield and developed by others (see, e.g., [18]). Our reasons for this choice are manifold. The logic of a topos is distributive, in contrast to the (propositional) logic ingeniously fashioned from projections by Birkhoff and von Neumann [17], which seems to have permanently acquired the name “quantum logic”. Moreover, topos quantum logic is a first order predicate logic, thus reaching well beyond

---

1 We denote this by ℓ-2 MBQC; see Section 4.
2 Adelman and Corbett [19] seem to have been the first on the scene of “topos quantum mechanics”, however we do not follow their approach here.
the propositional quantum logic and allowing for the expression of a much larger class of statements (involving quantifiers, for instance). It is in the topos approach that the connection between logic and contextuality is most clearly seen; we have a simple argument demonstrating that wherever there is contextuality there is non-Boolean topos logic, and that this applies to both state-independent and state-dependent versions of contextuality.

2 Survey of Results

Before proceeding to the provision of the mathematical and physical frameworks within which our work is carried out, we believe it helpful to survey the main results of this paper, in part as useful reference material and summary, and in part as a guide for what follows.

Following the pioneering work of Isham, Butterfield and Döring, we begin by discussing the Kochen-Specker theorem in terms of the “spectral presheaf” $\Sigma$, which associates to each abelian observable algebra (or context) a classical phase space, viewed as the space of valuations of the given observables. The Kochen-Specker theorem provides a negative answer to the question “is it possible that observables in quantum mechanics have predetermined measurement outcomes which are preserved under functional relations between these observables?”

The statement of the Kochen-Specker theorem can be recast in terms of the (non-)existence of global sections of $\Sigma$. We are also able, through the pseudostate $w\vert\psi\rangle$, to give state-dependent Kochen-Specker proofs from within the presheaf perspective, providing a simple version of a proof of Mermin in the new language. We note that what is required for such a proof is a specific subposet $W(H)$ of the poset $V(H)$ of all abelian subalgebras of $B(H)$ - the space of all linear operators on a finite dimensional Hilbert space $H$.

Understanding how $\Sigma$ and $w\vert\psi\rangle$ relate to their “environment” amounts to constructing the topos $\hat{W}(H)$ of all set-valued presheaves on $V(H)$. A topos is a set-like universe; from a logical perspective any topos behaves similarly to the category of sets but fails in two crucial respects: there are many possible truth values, arranged in a so-called Heyting algebra, and the law of excluded middle fails. The latter is equivalent to the statement that the internal logic of the given topos is non-Boolean. Moreover, the axiom of choice fails in most topoi and, by a theorem of Diaconescu, choice and excluded middle are related; in any topos choice implies excluded middle and hence Booleanness. In the topos of interest to us, namely the topos of presheaves on a poset, the above implication is promoted to an equivalence: Boolean logic is equivalent to the axiom of choice. By considering the appropriate categorical formulation of choice, we arrive at our first main observation: the presence of state-dependent or state-independent contextuality implies non-Boolean logic in $\hat{W}(H)$.

---

Sheaf theoretic methods in contextuality and non-locality have since been employed to great effect by Abramsky and coworkers (e.g., [20, 21]), who demonstrate that contextuality can be displayed by an operational consideration of measurement outcomes, without recourse to the quantum formalism.
Through the intermediary of contextuality, the relationship between MBQC and logic is considered. Anders and Browne [12] noticed that the state-dependent Kochen-Specker proof of Mermin can be recast as an MBQC OR-gate, for which they observe that the contextuality is a necessary requirement. For a general $\ell$-2 MBQC (see section 4), it has been shown [11] that non-linear function evaluation implies contextuality in the given computation, i.e., the existence of a Kochen-Specker proof. By constructing a poset canonically associated to the MBQC and identifying the corresponding topos, we may call upon the results stated in the previous paragraph to demonstrate that:

For the computation of non-linear functions in $\ell$-2 MBQC, the associated topos is necessarily non-Boolean.

In other words, just as entanglement, superposition and contextuality may be understood to be computational resources, we see that non-Boolean topos logic may be viewed similarly. By considering the post-measurement state in the Anders-Browne example, we show that the non-Booleanness is indeed depleted by the computation, and that this situation is also generic in the class of $\ell$-2 MBQC we consider.

The rest of this paper is organised as follows. In section 3 we give definitions of state-dependent and state-independent contextuality in terms of $\Sigma$ and $\mathbf{w}^*(\rho)$ respectively, including Mermin’s state-dependent proof from this perspective. Section 4 provides the definition of $\ell$-2 MBQC as well as Anders and Browne’s contextual OR-gate. We then turn to topoi and logic. Motivating the notion a Heyting algebra from the propositional structure governed by the open sets of a topological space, we then provide details of the topos $\mathbf{Sets}$ required for understanding the logical structures of a general topos which will be important in later sections. We provide some important definitions in the general theory of toposi and give the topos version of the axiom of choice.

A consideration of the topos $\mathbf{P}$ of presheaves on a generic poset $P$ comprises section 6. The crucial fact is that this topos is equivalent to the topos of sheaves $\mathbf{Sh}(P)$ on a topological space $P$ constructed from the poset $P$. The logical structure of the topos $\mathbf{Sh}(P)$ is clearly seen here; we provide the so-called subobject classifier $\Omega$ (or truth-value object) which generalises the set $\{0, 1\}$, and, following standard material, provide conditions under which $\mathbf{Sh}(P)$ is Boolean. By considering the truth values in $\Omega$ in $\mathbf{Sh}(P)$ we are able to directly discern whether $\mathbf{P}$ is Boolean, which comes of use in section 7. There we return to the quantum case and, building on work of previous sections, give our main result that non-Boolean topos logic is a necessary condition for non-linear function evaluation in $\ell$-2 MBQC. We analyse the consumption of the non-Booleanness during the course of the computation.
3 Contextuality in terms of $\Sigma$ and $w^{(\varphi)}$

We work in a complex Hilbert space $\mathcal{H}$ for which $\dim \mathcal{H} > 2$, equipped with the standard inner product $\langle \cdot | \cdot \rangle : \mathcal{H} \times \mathcal{H} \to \mathbb{C}$, linear in the second argument, pure states being given as unit vectors in $\mathcal{H}$. In order to obviate various technical topological issues we also assume that $\dim \mathcal{H} < \infty$. This is also justified on physical grounds; the quantum computational protocols we consider all take place in the finite dimensional setting.

Let $B(\mathcal{H})$ denote the algebra of all linear mappings $\mathcal{H} \to \mathcal{H}$, and $\mathcal{V}(\mathcal{H})$ the collection of all unital abelian subalgebras of $B(\mathcal{H})$, (partially) ordered by inclusion. To each $V \in \mathcal{V}(\mathcal{H})$ ($V$ viewed as a $C^*$ algebra) we associate the set of characters;

$$\Sigma(V) := \{ \lambda_V : V \to \mathbb{C} | \lambda_V \text{ is linear and } \lambda_V(ab) = \lambda_V(a)\lambda_V(b) \}$$  \hspace{1cm} (1)

Following Isham et al. (e.g., [18]) we also define how $\Sigma$ acts on inclusion relations between different abelian subalgebras: for $\lambda_V \in \Sigma(V)$, if $U \subseteq V$, define

$$\Sigma(U \subseteq V)(\lambda_V) := \lambda_V|_U \text{ (as function restriction)}$$ \hspace{1cm} (2)

$$\lambda_V \mapsto \lambda_V|_U;$$ \hspace{1cm} (3)

the mapping $\Sigma(U \subseteq V)$ is called a restriction map. It is clear that, if $U \subseteq V \subseteq W$ (all abelian),

$$\Sigma(V \subseteq W) \circ \Sigma(U \subseteq V) = \Sigma(U \subseteq W);$$ \hspace{1cm} (4)

in other words, it makes no difference if one restricts in stages, or “all at once”. In mathematical terms, $\Sigma$ is then referred to as a contravariant, set-valued functor (or presheaf), called the spectral presheaf.\footnote{\textsuperscript{5}} It is the version of “state space” introduced in [22] and suitable for our work.

For each $V \in \mathcal{V}(\mathcal{H})$, $\Sigma(V)$ can be viewed both topologically and logically as a classical phase space. It is topologically compact and Hausdorff, and the algebra of observables $V$ can be recovered as the space of (continuous) complex valued functions $\Sigma(V) \to \mathbb{C}$ (in other words, $V \cong C(\Sigma(V))$) and the isomorphism is isometric; this is the Gelfand duality arising from the Gelfand transform $A \mapsto A$; $\lambda(A) := A(\lambda)$. The algebra of physical propositions is given by the clopen (closed and open) subsets of $\Sigma(V)$ which is necessarily Boolean, reflecting the propositional structure we are all used to utilising when reasoning about (classical) physical systems. We will eventually see that $\Sigma$ itself carries a logical structure - a crucial property given its role as a state space.

\footnote{We also demand that $\lambda_V \neq 0$.}

\footnote{Presheaves on a category are sometimes called variable sets; one can view a presheaf as a collection of sets, parametrised by the objects of the domain category, and compatible with the morphisms. Presheaf categories are likewise dubbed “categories of variable sets”.}
3.1 Valuations and Sections

The set $\Sigma(V)$—the Gelfand spectrum of $V$—is in bijection with the set of simultaneous eigenvectors of self-adjoint operators in $V$, and therefore for any self-adjoint $a \in V$ and any $\lambda_V \in \Sigma(V)$, $\lambda_V(a)$ is an eigenvalue of $a$ (we call this condition SPEC). Furthermore, any $\lambda_V$ obeys the functional constraint $f(\lambda_V(a)) = \lambda_V(f(a))$ for any (continuous) function $f : \mathbb{R} \to \mathbb{R}$ and self-adjoint $a$ in $V$. Hence $\lambda_V$ acting on $V$ satisfies the “functional composition principle” $\text{FUNC}$ (see [23], chapter 5 for details) and can therefore be viewed as a valuation of the self-adjoint operators in $V$ (and the collection of all $\lambda_V$ are all the valuations). Such valuations are called local sections (above $V$). $\text{FUNC}$ states that if an observable $a$ (energy, for example) has value $a_0$, then $f(a)$ has value $f(a_0)$ (i.e., the value of the square of the energy should be the square of its value, for instance), and is (along with the spectrum requirement SPEC) an ostensibly mild condition even when considered on the whole of $B(\mathcal{H})$. However, $\mathcal{V}(\mathcal{H})$ is woven together in a complicated way (recall the partial order) and, as we shall see, this prohibits the existence of “global” valuations, i.e., those defined on all observables in $B(\mathcal{H})$.

The existence of a valuation on $B(\mathcal{H})$ is of clear importance in attempts to restore any kind of realism to quantum theory: if observables can be said to have values prior to and independently of measurement, the status of measurement can be downgraded to mere revelation of values/properties “held” by the quantum object in question. If such a valuation were to exist, quantum theory would then retain some essence of classical physics where all observables have values in all states, and where propositions about a physical system are either true or false. To reiterate, a valuation $\lambda : B(\mathcal{H}) \to \mathbb{C}$ must satisfy:

- For $a = a^*$, $\lambda(A) \in \sigma(a)$ (i.e., the value must be an eigenvalue) (SPEC)
- For $a = a^*$ and $f : \mathbb{R} \to \mathbb{R}$, $f(\lambda(a)) = \lambda(f(a))$ (FUNC);

any such valuation is necessarily linear and multiplicative on commuting operators and corresponds to sections above abelian algebras. It is automatic, of course, that for a projection $P$, $\lambda(P) \in \{0, 1\}$.

If such a global value assignment $\lambda$ existed, we would be able to choose for each $V \in \mathcal{V}(\mathcal{H})$ a point $\lambda_V$ in $\Sigma(V)$ in such a way that for any $U \subseteq V$, $\Sigma(U \subseteq V)(\lambda_V) = \lambda_U$. From equation (4), we see that local valuations, on $U$, say, are not sensitive to which other abelian algebras $U$ is contained in if they come from a global valuation, intuitively corresponding to a non-contextuality requirement.

3.2 The Kochen-Specker theorem

As we have seen, a global assignment $\lambda$ would specify an eigenvalue of each self-adjoint operator in $B(\mathcal{H})$ (SPEC) whilst respecting functional relations (FUNC). Keeping the same notation we now view $\lambda$ as giving rise to a local section above each $V$, in such a way as to respect the inclusions in $\mathcal{V}(\mathcal{H})$;
Definition 1 A global section $\lambda$ of $\Sigma$ is an assignment of a point $\lambda(V) \equiv \lambda_V \in \Sigma(V)$ for each $V \in \mathcal{V}(\mathcal{H})$, such that for $U \subseteq V$, $\Sigma(U \subseteq V)(\lambda_V) = \lambda_V|_U = \lambda_U$.

There is a categorical description in which a global section looks like a “point” of a set. Consider the singleton set $\{\ast\}$—the terminal object in the category $\text{Sets}$ of abstract sets and functions—characterised by the property that for any set $A$ (including the empty set $\emptyset$), there is precisely one map $A \to \{\ast\}$. Clearly any point of a set $A$ can be given as a map $\{\ast\} \to A$, and the collection of all such maps determines $A$ completely.

Now consider the (constant) presheaf $1 : \mathcal{V}(\mathcal{H}) \to \text{Sets}$ for which $1(V) = \{\ast\}$ for each $V$ (and on inclusions $1(U \subseteq V)(\{\ast\}) = \{\ast\}$). In the category of all presheaves $\mathcal{V}(\mathcal{H}) \to \text{Sets} =: \mathcal{E}$ (which is also a topos - more on this later), $1$ is a terminal object; for any presheaf $A$ in $\mathcal{E}$ there is precisely one map (natural transformation) $A \to 1$. Hence one can view a (generalised) point, or element of $\Sigma$ as a map (natural transformation) $1 \to \Sigma$ and this map is precisely $\lambda$. Hence a global section of an object $A$ in $\mathcal{E}$ is a generalised element of $A$.

In this language the Kochen-Specker theorem 7 (or the existence of contextuality) reads 7.

Theorem 1 (Kochen-Specker, Isham-Butterfield) For $\Sigma : \mathcal{V}(\mathcal{H}) \to \text{Sets}$, there exists no global section $1 \to \Sigma$,

and hence $\Sigma$ has no points at all in a generalised sense! An alternative view presents itself. For sets, surjective maps are right cancellable; if $g_1 \circ f = g_2 \circ f$ then $g_1 = g_2$. This provides the categorical version of a surjective map, called an epic map, or an epimorphism or an epimorphism. Just as any function $A \to \{\ast\}$ is surjective, in any topos of presheaves the map $A \to 1$ is an epimorphism. Hence one may view the section $1 \to \Sigma$ as the “cross-section” 8 (i.e., right inverse) of an epimorph $\Sigma \to 1$; following standard terminology (e.g., 7) we also call this map a section (indeed, this is the reason for calling $1 \to \Sigma$ a section in the first place). As shall become evident, the nonexistence of such a section is not only critical for a realist description of quantum theory, it is also of crucial importance to logic. Considering any subposet $\mathcal{W}(\mathcal{H})$ of $\mathcal{V}(\mathcal{H})$ we may make the following definition:

Definition 2 $\mathcal{W}(\mathcal{H})$ is contextual if $\Sigma : \mathcal{W}(\mathcal{H}) \to \text{Sets}$ has no global section. 8

---

6 Let $F, G : \mathcal{V}(\mathcal{H}) \to \text{Sets}$ be two presheaves. A natural transformation $\tau : F \to G$ is a map of presheaves, given context-wise as $\tau_V : F(V) \to G(V)$, which for each $U \subseteq V$, $\tau_U \circ F(U \subseteq V) = G(U \subseteq V) \circ \tau_V$.

7 We treat “the Kochen-Specker theorem” and “the existence of contextuality” as synonymous here. One can find a variety of meanings of the word “contextual” in the literature, ranging from the broad notion in Bohr’s “philosophy” that quantum phenomena must be understood only in reference to a concrete experimental arrangement/“context” (see, e.g., 17), to explicit statements about joint measurements, i.e., when it may arise that $A = f(B) = g(C)$ but $[B, C] \neq 0$, in which case one must take into account the “context” when stipulating values of $A$ and $B$ or, in measurement terms, whether $A$ is measured jointly with $B$ or with $C$.

8 This is the term commonly used in bundle theory for instance; see 26.

9 We always refer to $\Sigma$ despite the different domains; the context should make clear the poset to which we refer.
This allows us to look for contextual “scenarios”, i.e., instances of contextuality, by considering a small number of observables, constructing the corresponding subposet of $\mathcal{V}(\mathcal{H})$, and looking for global sections of $\Sigma$ there.

Theorem 1 does not depend on any choice of (pure) state; there are numerous examples of so-called “state-dependent” proofs of the Kochen-Specker theorem which do invoke a particular state, physically interpreted as the impossibility of observables possessing values in that given state. Such proofs can also be displayed in terms of sections of the “pseudostate” $w(\varphi) : \mathcal{V}(\mathcal{H}) \to \text{Sets}$ (or subposets of $\mathcal{V}(\mathcal{H})$ thereof) - this provides a unified perspective of state-dependent and state-independent versions of the Kochen-Specker theorem. With $P(V)$ denoting the projection lattice of $V$ (seen as a von Neumann algebra) and with $\varphi \in \mathcal{H}$ fixed, we first define the presheaf $S_{\varphi}$ (neglecting the restrictions) by

$$S_{\varphi}(V) := \bigwedge \{ P \in P(V) \mid P \geq |\varphi\rangle \langle \varphi| \}, \quad (5)$$

viz. the smallest projector $P \in P(V)$ which dominates $|\varphi\rangle \langle \varphi|$. The Gelfand transform $P \mapsto \bar{P}$, defined as $\lambda_V(P) = \bar{P}(|\varphi\rangle \langle \varphi|)$, dictates that $\bar{P}$ can be viewed as the characteristic function on $\Sigma(V)$ of those $\lambda_V$ for which $P(\lambda_V) = 1$. This motivates the definition of $w(\varphi)$, given by

$$w(\varphi)(V) = \{ \lambda_V \in \Sigma(V) \mid \lambda_V(P) = 1 \}, \quad (6)$$

which is manifestly a subset of $\Sigma(V)$ for each $V$, and hence $w(\varphi)$ is a subobject of $\Sigma$ (the restriction maps for $w(\varphi)$ are of course the same as for $\Sigma$; $w(\varphi)(U \subseteq V)(\lambda_V) = \lambda_U$). Continuing to write $\mathcal{W}(\mathcal{H})$ for some fixed subposet of $\mathcal{V}(\mathcal{H})$, we have the following definition:

**Definition 3** state-dependent contextuality is present for $(|\varphi\rangle \in \mathcal{H}, \mathcal{W}(\mathcal{H}))$ if there is no global section $1 \to w(\varphi)$.

The following simple observation demonstrates the relationship between state-dependent and state-independent contextuality:

**Proposition 1** For any $\mathcal{W}(\mathcal{H})$, if $\Sigma$ has no global section then there does not exist a $|\varphi\rangle \in \mathcal{H}$ for which $w(\varphi)$ has a global section.

Since $w(\varphi)$ picks out a subset of all possible sections above each $V \in \mathcal{W}(\mathcal{H})$, the proof is clear.

### 3.3 Mermin’s state-dependent proof

We let $\mathcal{H} \equiv \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \mathcal{H}_3 := \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$ with the Pauli operators $\sigma_x, \sigma_y, \sigma_z$ having the standard definitions, and write $X_1 \equiv \sigma_x \otimes 1 \otimes 1$, $Y_2 \equiv 1 \otimes \sigma_y \otimes 1$, etc. Consider the following putative valuation:

---

10We could thus also refer to state-independent contextuality when $\Sigma$ has no section. We shall do this only when distinction from the state-dependent case is required.
By definition $\lambda$ is multiplicative on commuting operators. The product of the four terms on the left hand sides of (7) - (10) is 1, whereas the product of the four values on the right hand side is $-1$, thus ruling out the mapping $\lambda$ as a viable valuation.

The values taken by $\lambda$ on the right hand side of (7) - (10) are precisely those given by (expectation values in) the GHZ state $|\Psi\rangle \equiv 1/\sqrt{2} (|000\rangle + |111\rangle)$ (11) (the 0’s and 1’s correspond to eigenvalues of $\sigma_z$, see [28], and [29] for Mermin’s state-dependent Kochen-Specker proof). The GHZ state is not multiplicative on the given observables and therefore does not satisfy the definition of a section.

In order to prove that we are in the presence of state-dependent contextuality in the language of this paper, i.e., in accordance with definition 3, it must be shown that $w|\Psi\rangle$ has no global section, i.e., that the local sections, compatible with the constraints imposed by the GHZ state, cannot be appropriately “glued” to give a global section with the required restrictions.

Let $\tilde{\lambda}_V : \{\ast\} \to w(|\Psi\rangle)$ denote a hypothetical global section of $w(|\Psi\rangle)$, and define $V_1$ to be the observable algebra generated by $\{X_1, X_2, X_3\}$ and, following equations (7) - (10), mutatis mutandis, do the same for $V_2, V_3$ and $V_4$. We denote by $V_{X_1}$ the algebra generated by $X_1$ (which is contained in $V_1$), etc. We have that $\tilde{\lambda}_{V_i} : \{\ast\} \to w(|\Psi\rangle)(V_i)$ so that $\tilde{\lambda}_{V_i}(\{\ast\})$ is a local section of $w(|\Psi\rangle)$ above $V_i$ for $i \in \{1..4\}$. Hence we have the constraints:

\[
\begin{align*}
\tilde{\lambda}_{V_1}(\ast)(X_1)\tilde{\lambda}_{V_1}(\ast)(X_2)\tilde{\lambda}_{V_1}(\ast)(X_3) &= +1 \\
\tilde{\lambda}_{V_2}(\ast)(X_1)\tilde{\lambda}_{V_2}(\ast)(Y_2)\tilde{\lambda}_{V_2}(\ast)(Y_3) &= -1 \\
\tilde{\lambda}_{V_3}(\ast)(Y_1)\tilde{\lambda}_{V_3}(\ast)(X_2)\tilde{\lambda}_{V_3}(\ast)(Y_3) &= -1 \\
\tilde{\lambda}_{V_4}(\ast)(Y_1)\tilde{\lambda}_{V_4}(\ast)(Y_2)\tilde{\lambda}_{V_4}(\ast)(X_3) &= -1.
\end{align*}
\]

For convenience we write $\lambda_{V_i} := \tilde{\lambda}_{V_i}(\ast)$. The local sections $\lambda_{V_i}$ have restrictions, for example $\lambda_{V_1}|_{V_{X_1}} = \lambda_{V_{X_1}}$ etc. It is thus required that the compatibility conditions hold: $\lambda_{V_1}|_{V_{X_1}} = \lambda_{V_2}|_{V_{X_1}}, \lambda_{V_1}|_{V_{X_2}} = \lambda_{V_3}|_{V_{X_2}}$ and so on. These are manifestly requirements of non-contextuality. Appropriate substitution back into (12) gives rise to the same contradiction found on $\lambda$ in (7) - (10).

The following Hasse diagram illustrates the poset structure of the GHZ scenario:

---

\[\text{Strictly, of course, } \lambda \text{ acts on the algebra generated by the given qubit observables.}\]
4 Measurement Based Quantum Computation

4.1 $\ell$-2 MBQC

Measurement based quantum computation (MBQC) employs single particle (qubit or qudit, projective or positive operator valued) measurements on a fixed initial state to achieve a computational output. The state is altered by the local measurements (in particular any entanglement is destroyed); the initial state is thus viewed as a resource, and for suitable choices such as cluster states \([30,31]\), MBQC is universal for quantum computation.

The measurements generating the computation have individually random but correlated outcomes, and the computational result depends crucially on these correlations. In addition, the observables to be measured must typically be adjusted according to previous measurement outcomes. Therefore, classical side-processing is required both to direct the computation and to produce the desired output. This classical processing is typically limited, and is not universal for classical computation. For example, in the universal scheme of \([32]\), only addition modulo 2 is permitted.

We note that universal MBQC schemes with different classical side-processing, different resource states and different sets of allowed measurements have been devised; see, e.g., \([33–38]\). However, for the present purpose, we consider MBQC on quantum states of multiple qubits, where the classical side-processing is restricted to addition modulo 2, see \([11,12,32]\).

The relevant Hilbert space for our work is $\mathbb{C}^{2^n} \cong \bigotimes_{k=1}^{n} \mathbb{C}^2$ and measured observables are non-trivial on only one factor in the tensor product; these are referred to as local observables. Local measurements are defined in the obvious way. We now give a brief definition of $\ell$-2 MBQC and refer to \([11]\) for details; for clarity of exposition we restrict attention to the case where there is only one output bit, though our results pertain to the general case. We also restrict ourselves to computations which are temporally flat, i.e., joint measurements of local observables or, in other words, where the choice of measured local observable does not depend on the outcome of a previous measurement.

**Definition 4** A temporally flat, deterministic $\ell$-2 MBQC $M$ consists of a resource state $|\Psi\rangle \in \mathbb{C}^{2^n}$, classical input $i \in \mathbb{Z}_2^m$ and classical output $o : \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2$. 
\(i \mapsto o(i)\), a collection of local observables \(\{O_k(q_k)|k \in \{1\ldots n\}; q_k \in Z_2\}\) for which the measurement outcomes of a given \(O_k(q_k)\) are labelled \(s_k(q_k) \in \{0, 1\}\) for each \(k\). The computed output \(o(i) = \sum_k s_k(q_k) \mod 2\), and, with \(q = (q_1\ldots q_n)\), the measured observable \(O_k(q_k)\) is related to the outcome \(s_k(q_k)\) by \(q = Qi\) where \(Q : Z_2^n \rightarrow Z_2^n\).

Since all the computations we consider are of the above form, for brevity we occasionally omit the qualifiers “deterministic” and “temporally flat”, and only refer to such conditions when necessary.

Given \(B(\mathbb{C}^2^n)\), we must construct the poset \(\mathcal{W}(\mathbb{C}^2^n)\), yielding a diagram similar to (13). We proceed by considering all strings \(\{(O_1(q_1), ... , O_n(q_n))\}\) for which \(O_1(q_1) \otimes ... \otimes O_n(q_n) |\Psi\rangle = (-1)^{o(i)} \). Given such a string \((O_1(q_1), ... , O_n(q_n))\) the abelian algebra (context) is generated by the local observables, written \(\{O_1(q_1), ... , O_n(q_n)\}''\) The collection of all such algebras form the “top layer” of the poset, with the second layer given as the algebras generated by local observables appearing in the strings, furnished by the obvious inclusion relations. We also note here that any algebra \(\{O_1(q_1), ... , O_n(q_n)\}''\) is a maximal abelian subalgebra (masa) of \(B(\mathbb{C}^2^n)\), that is, there is no larger abelian algebra containing it. This follows since the set \(\{O_1(q_1), ... , O_n(q_n)\}\) generates \(2^n\) mutually orthogonal projections, and the algebra generated by these projections coincides with \(\{O_1(q_1), ... , O_n(q_n)\}''\).

The main result of [11] reads:

**Theorem 2** [11] *Every \(\ell\)-2 MBQC which deterministically computes a non-linear Boolean function is contextual.*

We conclude this subsection with two remarks. Firstly, there are quantum algorithms with super-polynomial speed-up in the class of deterministic MBQCs, exhibiting contextuality. Specifically, the quantum algorithm for the “discrete log” problem [40] breaks a crypto system. It is deterministic in the circuit model [41], and can be converted into deterministic MBQC by standard techniques [32]. Secondly, the condition of determinism in theorem 2 can be relaxed. For probabilistic function evaluation, for every given non-linear function there is a threshold in the success probability above which the corresponding MBQC is contextual. This threshold can be low; for the bent functions [12] it approaches 1/2 in the limit of large number of input bits [11].

### 4.2 Anders and Browne’s OR-gate

The first and simplest example that illustrates the connection between contextuality and non-linear function evaluation in MBQC is the OR-gate of Anders and Browne [12], which is directly constructed from Mermin’s state-dependent proof of the Kochen-Specker theorem (see subsection 3.3).

---

**Footnotes:**

12This is simply the double commutant, see, e.g., [39] theorem 5.3.1.

13The version of contextuality used in [11] is the “strong contextuality” of [20], which, though different from our definition, coincides with it in the cases we consider.

11
In order to consider computation, it is necessary to rewrite the proof of contextuality arising from the GHZ state in computational variables. Consider once more the “GHZ-valuation” $\lambda$ given in (7) - (10). Define $\lambda(X_i) = (-1)^{x_i}$ and $\lambda(Y_i) = (-1)^{y_i}$. Direct substitution into (7) - (10) yields the following constraints (with all sums modulo 2):

$$
\begin{align*}
    x_1 + x_2 + x_3 &= 0, \\
    x_1 + y_2 + y_3 &= 1, \\
    y_1 + x_2 + y_3 &= 1, \\
    y_1 + y_2 + x_3 &= 1,
\end{align*}
$$

resulting, once again, in an insoluble set of equations (this time seen by summing the left hand side of (14), summing the right hand side, and comparing). The above proof of the Kochen-Specker theorem can be adapted to MBQC. There is no contradiction if in (7) - (10), or equivalently their computational counterparts in (14), the $x_i, y_i$ are regarded as actual measurement outcomes rather than predetermined (noncontextual) values.

The right hand side of (14) can be viewed as the output of an OR-gate in $\ell$-2 MBQC (recall definition [4]) as follows. The input $i = (i_1, i_2) \in Z_2 \times Z_2$ and $o(i) \in Z_2$. If $q_k = 0$, $X_k$ is measured, if $q_k = 1$, $Y_k$ is measured. The outcomes $s_k(q_k)$ are written $s_k(0) = x_k$, $s_k(1) = y_k$. The map $Q$ effects $q_1 = i_1, q_2 = i_2, q_3 = i_1 + i_2 \mod 2$. Hence $o(i) = s_1(q_1) + s_2(q_2) + s_3(q_3)$ so, for instance, if $(i_1, i_2) = (0, 0), q(0, 0) = s_1(0) + s_2(0) + s_3(0) = x_1 + x_2 + x_3 = 0.$

Computing the outputs for the remaining inputs verifies that $o(i_1, i_2) = \text{OR}(i_1, i_2)$, and, given equation (14), we see how the above Kochen-Specker proof gives rise to an OR-gate in $\ell$-2 MBQC.

The OR-gate has the property of being a non-linear Boolean function (compare $\text{OR}(1, 1) + \text{OR}(0, 1)$ with $\text{OR}(1, 0)$) which, as theorem [2] shows, implies the presence of contextuality. While not of practical use, the ability to evaluate an OR-gate within MBQC is of fundamental relevance. The classical control computer in $\ell$-2 MBQC is limited to addition mod 2, and is thus by itself not classically universal. Access to a GHZ state and Pauli measurements promotes it to classical universality, vastly increasing its computational power.

5 Topoi and logic

5.1 Introduction to topoi

Topos theory emerged from two distinct places (a good history can be found in the introduction of [43]): Grothendieck’s work on sheaves and Lawvere and Tierney’s work on categorical set theory and the foundations of mathematics. Only in the last 20 years or so have people begun to apply this rich and powerful subject to problems in quantum mechanics. We avoid excessive detail here (and refer to [44] and for the brave [43] for topos theory, and [18], [45] for the quantum case) and opt instead for a brief discussion of the main points, focussing on the logical aspects.
A topos resembles a “universe of sets”, that is, abstract sets and functions between them. The defining feature of topoi (or toposes) is that certain universal constructions available for sets (for example the cartesian product of sets is a set, the collection $B^A$ of all functions $A \to B$ is a set called the exponential and so on) are available in any topos. Of crucial importance is that one may represent subobjects by suitable mappings. In set theory one may uniquely identify a subset $A \subseteq X$ with the characteristic map $\chi_A : X \to \{0, 1\}$; via such a mapping one may confirm (1) or deny (0) whether a given subset or element of $X$ lies inside $A$.

The situation in topos theory is similar; there exists a bijection between subobjects and their characteristic mappings. However, general topos objects do not have elements (global sections) as we have already seen, and the “truth value set” $2 \equiv \{0, 1\}$ must be replaced by a truth object $\Omega$ in the topos, called the subobject classifier. The collection of global sections $\Gamma \Omega$ of $\Omega$ (and there may be many!) represent the “truth values” that a given statement can take. In general $\Gamma \Omega$ is not a Boolean algebra - it is what is called a Heyting algebra, to be introduced in the next section.

5.2 Logic and Heyting algebras

Just as the power set of a given set is Boolean, the open sets of a topological space carry their own logical structure, providing the prototypical Heyting algebra. With (the lattice of) open sets $O(X)$ of a space $X$ representing propositions, there is no difficulty in interpreting the logical “and” ($\land$) and “or” ($\lor$) as set theoretical intersection $\cap$ and union $\cup$ (these preserve openness). However, whereas the operation $\neg$ is given by complementation ($\cdot^c$) in the power set, this is not available in a topological space since complementation need not preserve openness. Instead, $\neg U$ (we do not distinguish the logical proposition $U$ from the corresponding open set) is given as the interior $intU^c$ of $U^c$, i.e., $\neg U$ is given as $intU^c \equiv int(X \setminus U)$. This is clearly open; however $U^c$ cannot be interpreted as a true complement of $U$, since $(U^c)^c = intclU$ (the interior of the closure of $U$) which may properly contain $U$. Logically, one has $\neg \neg U \geq U$ and

$$U \lor \neg U \leq 1.$$ 

In other words, the law of excluded middle does not hold in the Heyting algebra of open sets of a topological space. Logical implication $\implies$ is a derived operation involving $\neg$ (recall that in the Boolean power set $U \implies V = U^c \cup V \equiv \neg U \lor V$), and in a Heyting algebra of open sets $U \implies V$ takes the form $\neg U \lor V \equiv int(X \setminus U) \cup V$.

Though the lattice of open sets always forms a Heyting algebra, there are others, and so we need a general definition. First notice that the logical operations can be given in terms of the lattice operations, for instance $\neg U = \bigvee \{W | W \cap U = \emptyset\}$. We have

\[\text{Technically the subobject classifier also comprises an arrow } true : 1 \to \Omega; \text{ details to follow.}\]
Definition 5  A Heyting algebra $\mathcal{H}$ is a bounded distributive lattice (like a Boolean algebra) with a top element 1, a bottom element 0, and a binary operation $\Rightarrow$ which satisfies, for all $a, b, c$ in $\mathcal{H}$, $c \leq a \Rightarrow b$ if and only if $(c \land a) \leq b$.

$\neg a$ is defined by $a \Rightarrow 0$; it is called the pseudo-complement (of $a$) and is manifestly the greatest element of $\mathcal{H}$ for which $a \land \neg a = 0$, which we have already seen in the case of topological spaces.

As already stated, there is no excluded middle available in a general Heyting algebra. This is the principal difference between Heyting algebras and Boolean algebras. Indeed (see [46], proposition 1.2.11 and the accompanying proof),

Proposition 2  A Heyting algebra $\mathcal{H}$ is Boolean if, and only if, for each $a \in \mathcal{H}$, $\neg \neg a = a$, i.e., if each element has a complement/negation, which holds if and only if for all $a \in \mathcal{H}$, $a \lor \neg a = 1$.

In a Heyting algebra one still has $a \land \neg a = 0$.

A statement formulated in a topos $\mathcal{E}$ can be “partially true”, depending on which global element of the Heyting algebra $\Gamma\Omega$ the statement is mapped to. Just as ordinary mathematical statements (“$M$ is a manifold”, “$f$ is a continuous function”, etc.) can be formulated in first order predicate calculus, statements in topos theory can be formulated in terms of first order intuitionistic logic (see, e.g., [47]). A topos represents a nonstandard “universe” in which one may reason. Proof by contradiction is ruled out in general, as is the axiom of choice, to which we turn our attention shortly.

5.3 The topos Sets

Naturally, (perhaps) the simplest topos is $\textbf{Sets}$ itself - the collection of sets with functions between them. Recall that $\textbf{Sets}$ comes equipped with a logical structure relating to how subsets “fit inside each other”. In order to properly incorporate the categorical philosophy into the discussion of sets, the specification of a subset of a given set must refer only to functions to or from that set, and make no reference to the internal structure. However, to build intuition before proceeding to the abstract setting where objects may not have elements, we provisionally allow ourselves to talk of elements so that the generalisation is convincing.

Two distinct notions of what a subset $S$ of some set $A$ “is”, given in terms of functions and which capture the ordinary definition (i.e., elements of $S$ which also belong to $A$), immediately present themselves: an injective map $s : S \hookrightarrow A$, and a function $A \rightarrow \{0, 1\}$ which takes the value 1 whenever a given point in $A$ is also in $S$.

In the former, it is common, and not improper, to sometimes identify the image $s(S)$ with $S$ itself, since $s$ provides a faithful “picture” of $S$ inside $A$; thus, up to a clear equivalence, one can think of injective maps (or their domains) with codomain $A$ as subsets of $A$. In the latter, one can think of a map $u : A \rightarrow$...
{0, 1} \cong 2 as (giving rise to) a subset of A - simply think of the inverse image \( u^{-1}(1) \), i.e., the set of elements of A which get mapped to 1, or “true” under \( u \). Such a map \( u \) can be written \( \chi_S \), i.e., the characteristic function of the set \( S \), where \( \chi_S(x) = 1 \) if \( x \in S \) and 0 otherwise. These two perspectives on subsets “agree”, that is, there is a bijective correspondence between (equivalence classes of) injective maps with codomain \( A \), and mappings \( A \to 2 \), written \( 2^A \). Hence, we have the bijection (with \( \mathcal{P} \) denoting power set)

\[ \text{sub}_A \cong \mathcal{P}(A) \cong 2^A. \] (16)

This feature is preserved in a general topos; one can formulate the required characteristic maps without ever referring to points, which is crucial in a topos where objects (\( \Sigma \) for example) may have no points but many subobjects. Equation (16) yields immediately that \( \text{sub}\{\ast\} \cong \mathcal{P}\{\ast\} \cong 2^{\{\ast\}} \), which can also be seen by direct inspection; \( \{\ast\} \) has two subsets given by the empty map and the identity, thereby setting up the bijection \( \text{sub}\{\ast\} \cong \{0, 1\} \cong 2 \).

The set 2 represents a (very simple!) Boolean algebra in two obvious ways: firstly, \( \text{sub}(2) \) is the power set \( \mathcal{P}(2) \) which is always Boolean. The elements \( \Gamma_2 = \{0, 1\} \) of 2, given by the maps \( \{\ast\} \to 2 \), also carry the structure of a Boolean lattice under \( 1 > 0 \), which represents the algebra of truth values in \( \text{Sets} \). In a general topos \( \mathcal{E} \), the subobject classifier \( \Omega \) also has two Heyting structures; \( \text{sub}\Omega \) and \( \Gamma\Omega \), where the latter represents generalised “truth values”, and in general neither \( \text{sub}\Omega \) nor \( \Gamma\Omega \) are Boolean.

We now give the formal definition of the subobject classifier (or subset classifier, in this case) for \( \text{Sets} \) which provides the prototype for all other topoi.

**Definition 6** (Subobject classifier for \( \text{Sets} \)) Let \( \text{true} : \{\ast\} \to \{0, 1\} =: 2 \) take the value \( \text{true}(\ast) = 1 \). A subobject classifier is a set \( \Omega \equiv 2 \) together with a function \( \text{true} : 1 \to 2 \) such that for every set \( A \in \text{Sets} \) and every injective map \( s : S \hookrightarrow A \), there is a unique function \( \chi_S : A \to 2 \) for which the following square commutes:

\[
\begin{array}{cc}
S & \to & \{\ast\} \\
\downarrow s & & \downarrow \text{true} \\
A & \to & 2 \\
& \chi_S & \\
\end{array}
\]

and, furthermore, that for any \( X \to A \), there is a unique map \( X \to S \) (this says that the above square is a pullback - an example of a universal property).

It must be stressed that none of the above is chosen arbitrarily - the subobject classifier is **unique** (up to isomorphism). We also reiterate that since the above diagram can be understood by only considering objects (sets) and morphisms (functions) and does not require one to look “inside” sets (though one can, of course, describe points of a set \( A \) by maps \( \{\ast\} \to A \)), it is immediately ready for generalisation to arbitrary categories which have “enough” in common with \( \text{Sets} \) to make sense of the concepts appearing in the definition, namely a
terminal object which generalises \{\ast\}, the availability of diagrams of the above form (pullbacks) and a suitable truth value object \(\Omega\). Along with some other requirements, which will not be needed in this paper, these are the essential ingredients needed for the definition of a topos.

### 5.4 General topoi

We now discuss more general features of topoi by abstracting further some notions appearing in the case of \textbf{Sets} given in the previous section. We omit the full definition of a topos (see, e.g., [46] chapter 5), which is technical, and instead stress the similarities to \textbf{Sets}, focussing on the logic. The crucial components in that respect that make up part of the definition of a topos is the existence of a terminal object 1 and a subobject classifier \(\Omega\). With \(\mathcal{E}\) an arbitrary topos, we have the following important definitions.

**Definition 7** A subobject \(A\) of an object \(B\) in \(\mathcal{E}\) is defined as a monic arrow \(A \rightarrow B\), where monic means “right cancellable”.

Of course, “monic” is the category version of “injective” in \textbf{Sets}. The definition of the subobject classifier in a topos \(\mathcal{E}\) is identical to that given for sets, with the replacement in definition 8 of 2 by an object \(\Omega\) in \(\mathcal{E}\), subsets by subobjects, and \{\ast\} by the terminal object 1, and hence:

**Definition 8** Let \(\mathcal{E}\) be a topos. A subobject classifier is an object \(\Omega\) together with a morphism \(\text{true} : 1 \rightarrow \Omega\) such that for every object \(A \in \mathcal{E}\) and every monic \(s : S \rightarrow A\), there is a unique morphism \(\chi_S : A \rightarrow \Omega\) such that the following square is a pullback (i.e., commutes and is universal among such squares):

\[
\begin{array}{ccc}
S & \rightarrow & 1 \\
\downarrow s & & \downarrow \text{true} \\
A & \rightarrow & \Omega \\
\chi_S & \downarrow & \\
& & \\
\end{array}
\]  

(18)

This sets up a Heyting algebra isomorphism between subobjects of some object \(X\) and characteristic morphisms \(X \rightarrow \Omega\):

\[
\text{sub}X \cong \text{Hom}(X, \Omega) \cong X^\Omega
\]  

(19)

where \(\text{Hom}(X, \Omega)\) denotes the set of maps (morphisms) \(X \rightarrow \Omega\). We state without proof the following fact, referring the reader to [46], proposition 6.2.1:

**Proposition 3** For any object \(X\) in \(\mathcal{E}\), \(\text{sub}X\) is a Heyting algebra.

Replacing \(X\) by 1—the terminal object in \(\mathcal{E}\)—immediately yields

\[
\text{sub}(1) \cong \Gamma\Omega,
\]

(20)
demonstrating at once that the global elements of $\Omega$ have the structure of a Heyting algebra, given as the subobjects of the terminal object $1$.

**Definition 9** $\mathcal{E}$ is called Boolean if $\text{sub}_\Omega$ (the lattice of subobjects of $\Omega$) is a Boolean algebra.

**Definition 10** If every epimap in $\mathcal{E}$ has a section, then we say the axiom of choice (AC) holds in $\mathcal{E}$.

This is a straightforward generalisation from the standard scenario (of set theory) where it is usually maintained that AC holds. This much studied condition takes many forms, the simplest of which is the seemingly innocuous statement “the product of nonempty sets is non-empty”. Closer in spirit to the topos case is “every surjective function has a section” (i.e., a right inverse). AC fails in “most” topoi, and has a surprising connection to logic.

Due to a theorem of Diaconescu, the implication “AC $\implies$ Boolean” holds in any topos, though the converse fails in general. Crucially, in certain special (localic) topoi, of which the topos of presheaves on a poset—the situation to be encountered in our investigation—is an example, the converse of Diaconescu’s theorem does hold. Thus we may conclude that the nonexistence of a global section of an epimap ($\Sigma \to 1$ or $\psi \to 1$, for example) in our quantum topoi, which ensures the failure of the axiom of choice, also ensures the non-Booleanness of the given topos, thus intimately tying contextuality to non-Boolean topos logic.

## 6 Presheaves on a poset

We consider a generic poset $(P, \leq)$, which we abbreviate by $P$. The logic of the topos $\text{Sets}^{\text{op}} \equiv \hat{P}$ is essentially determined by the structure of $P$ or, more precisely, the nature of a topological space $\hat{P}$ naturally associated with $P$. Since $\hat{\mathcal{W}(\mathcal{H})}$ is a topos of presheaves on a poset, it is worth first investigating the structure of $\hat{P}$.

**Definition 11** Consider the poset $P$. A down-set $A$ on $P$ is a subset $A \subseteq P$ for which $x \in A$ and $y \leq x$ implies $y \in A$.

The down-sets $\downarrow P$ on $P$ form the open sets of a topological space called the Anti-Alexandrov topology on $P$; we write $\hat{P}$ for this space.

As well as presheaves we must consider sheaves; we only need sheaves on a topological space and so omit the categorical definition, opting for the “classical” one instead.

---

$^{16}$Note that $\Gamma \Omega$ may still have more than two elements even if $\Omega$ is Boolean. However, any Boolean topos can be turned into a Boolean topos in which $\Gamma \Omega$ does have two elements without changing anything essential - see [44], chapter 6, Proposition 6.

$^{17}$Any category $\text{Sets}^{\text{op}} \equiv \hat{C}$, with $C$ a small category, is a topos.

$^{18}$We note that $P$ can be recovered up to equivalence from $\hat{P}$. 

17
Definition 12 Let $X$ be a topological space and $\mathcal{F} : \mathcal{O}(X) \to \text{Sets}$ a presheaf on the open sets $\mathcal{O}(X)$. $\mathcal{F}$ is a sheaf if for any open set $U$ and any open cover $U = \bigcup U_i$ of $U$ and each collection $v_i \in F(U_i)$ (of local sections) for which $f_i|_{U_i \cap U_j} = f_j|_{U_i \cap U_j}$, there exists a unique $f \in F(U)$ such that $f|_{U_i} = f_i$ for each $i$.

We denote the collection of (set-valued) sheaves on $X$ by $\text{Sh}(X)$. It turns out (e.g., [48]) that the presheaves on $P$ seen as a poset are exactly the sheaves on $P$.

Proposition 4 $\hat{P} \cong \text{Sh}(P)$ where $\cong$ denotes equivalence of categories.

Furthermore (see [44], chapter II, proposition 4), with 1 denoting the terminal object in $\text{Sh}(X)$

$$\mathcal{O}(X) \cong \text{sub}(1) \quad (21)$$

which, in combination with equation (20) and proposition 4 shows that the global elements of $\Omega$ are precisely the down-sets in $P$. We state it as a proposition:

Proposition 5 $\downarrow P \cong \Gamma \Omega$.

This enables us to understand the logical structure of the truth values $\Gamma \Omega$ in $\mathcal{E}$ by directly looking at the poset $P$, which will be of use when we consider the topoi involved in quantum computation. The next theorem demonstrates, among other things, that $\text{Sh}(X)$ is Boolean if and only if $X$ is Boolean as a topological space; first we require a definition:

Definition 13 Let $A'$ be a subobject of $B$ in $\hat{P}$, i.e., for each $p \in P$, $A'(p) \subseteq B(p)$. A complement of $A'$ in $B$ is an $A''$ for which $A''(p) \subseteq B(p)$ (i.e., $A'' \to B$) for each $p$ and for which $A' \cup A'' \cong B(p)$ ($\cong$ denotes a bijection, $\cup$ denotes union; it is required that $A'(V)$ and $A''(p)$ are always disjoint if they are to be complements).

Theorem 3 Let $\mathcal{E}$ be a topos of the form $\mathcal{E} = \text{Sh}(X)$ for $X$ a topological space [19]. The following are equivalent ([46], proposition 7.55 and [43], proposition 5.14):

1. $\Omega$ is a Boolean Algebra (i.e., $\mathcal{E}$ is Boolean);
2. AC holds in $\mathcal{E}$;
3. All subobjects have complements;
4. $\mathcal{O}(X)$ is a complete Boolean algebra.

[19] All that is actually required for parts 1 and 2 of theorem 3 is that $X$ is a locale, or “point-free topological space”. 

18
Equation (21) gives $\mathcal{O}(P) \cong \Gamma \Omega$ in the topos $\text{Sh}(P)$ which, by item 4 in theorem 3, shows that $\text{Sh}(P)$ is a Boolean topos precisely when $\Gamma \Omega$ is a Boolean algebra, i.e., it is enough that $\Gamma \Omega$ is Boolean to conclude that $\Omega$ (and hence $\mathcal{E}$) itself is. By proposition 4 we therefore observe that $\hat{P}$ is Boolean precisely when $\mathcal{O}(P) \cong \downarrow P$ (by proposition 5) is a Boolean algebra, thus yielding a direct means by which to decide if the presheaf topos on a given poset is a Boolean algebra. This will be of use when we consider the logical situation after the completion of a computation in subsection 7.2.

6.1 The quantum topos

The topos $\text{Sets}$ captures the logical structure of classical physics, where Boolean logic plays a fundamental role both in the structure of propositions (i.e., distinguished subsets of the phase space) and in the truth evaluation of the given propositions - any such proposition is true or false, and the two truth values are arranged as a Boolean algebra. It has been argued by Isham and collaborators that one should use topoi other than $\text{Sets}$ for construction of physical theories in general. Isham and Döring in [18] provide a thorough discussion of the topos $\hat{\mathcal{V}}(\mathcal{H})$ (which we recall is the topos of presheaves on the poset of abelian von Neumann subalgebras of $B(\mathcal{H})$). The spectral presheaf $\Sigma$ carries a logical structure of its own and represents the phase space in the topos $\hat{\mathcal{V}}(\mathcal{H})$.

The topos $\hat{\mathcal{W}}(\mathcal{H})$ of interest to us is a subtopos of $\hat{\mathcal{V}}(\mathcal{H})$ and these topoi have many features in common. We may view $\hat{\mathcal{W}}(\mathcal{H})$ as the restriction to a specific physical situation of interest, with the given logical structure as the logic governing that situation. It is therefore of crucial importance to understand the logic of $\hat{\mathcal{W}}(\mathcal{H})$ and when this logic is non-Boolean, thus dictating that we are in a situation fundamentally different from that of classical physics.

Consider once more the poset $\mathcal{W}(\mathcal{H}) \subseteq \mathcal{V}(\mathcal{H})$ and the topos $\hat{\mathcal{W}}(\mathcal{H})$. Combining definition 10 with theorem 3 we thus immediately see that demonstrating that $\mathcal{E}$ is non-Boolean amounts to finding an epimap in $\mathcal{E}$ which has no sections. We thus have as a corollary of theorem 1 one of our main observations:

**Corollary 1** Let $\mathcal{E} = \hat{\mathcal{W}}(\mathcal{H})$ and let $\Sigma$ and $\nu$ have the given definitions. If $\Sigma$ has no global section or if there exists a $|\varphi\rangle \in \mathcal{H}$ for which $\nu(|\varphi\rangle)$ has no global section, then the logic of $\mathcal{E}$ is non-Boolean.

Therefore we see that

**Corollary 2** state-dependent or state-independent contextuality implies non-Boolean logic in $\mathcal{E}$.

Therefore, state-dependent or independent contextuality may be viewed as a sufficient condition for the given topos to be non-Boolean. This may come as no surprise - the Kochen Specker theorem rules out a class of hidden variables which are in some sense classical. However, we are now able to demonstrate a tight link between the Kochen Specker theorem and the logic of a topos closely
related to a physical situation. The observation that this comes via the axiom of choice is perhaps a surprise. We also make the following remark: in general, contextuality is not a necessary requirement for non-Booleanness. It may occur that both $\mathfrak{m}^{|\psi\rangle}$ and $\Sigma$ have global sections, but there exist other presheaves in $\mathcal{E}$ which do not, therefore yielding a non-Boolean topos without the presence of contextuality. We now explore the connection between the non-classical logic of a topos and the promotion of non-universal to universal computation in MBQC.

7 Non-Boolean logic and quantum computation

Before analysing the role played by non-Boolean topos logic in the class of $\ell$-2 MBQC of interest, we briefly summarise the various topics that have been presented thus far, and how they are related. The state-dependent and state-independent Kochen-Specker theorem was rephrased in terms of the non-existence of global sections of the presheaves $\mathfrak{m}^{|\psi\rangle}$ and $\Sigma$ respectively, both defined on a poset $W(\mathcal{H}) \subseteq V(\mathcal{H})$, the latter representing the collection of abelian von Neumann algebras of $\mathcal{B}(\mathcal{H})$, ordered by inclusion, and we presented Mermin’s state-dependent proof in this language. Temporally flat deterministic $\ell$-2 MBQC was introduced, with emphasis on a result in [11] that demonstrates the necessity of contextuality in the evaluation of non-linear Boolean functions, and we presented the simple example of Anders and Browne’s OR-gate [12].

The connection to logic was then made by introducing some basic machinery of topos theory, where the Boolean logic of set theory is replaced by (the non-Boolean) intuitionistic logic, with Heyting algebras governing the structure of the multivalued truth object and the structure of subobjects of the “phase space” $\Sigma$. The special case of (the topos of) presheaves on a poset, which encompasses the quantum case, was then analysed in greater detail, and we delineated conditions under which such a topos is Boolean. Via the topos version of the axiom of choice, we then established the major link between contextuality and logic: by constructing the topos $\hat{W}(\mathcal{H})$ from the poset $W(\mathcal{H})$, we showed (corollary 2) that contextuality implies non-Boolean logic in $\hat{W}(\mathcal{H})$.

We are therefore presented with a link between non-Boolean logic and computation. With $\Phi$ a resource state for an $\ell$-2 MBQC $\mathcal{M}$ as defined in section 4, the main result of [11], in the language of this paper, reads

**Proposition 6** If $\mathcal{M}$ computes a non-linear Boolean function, then $\mathfrak{m}^{(|\Phi\rangle)}$ has no global section, i.e., there is state-dependent contextuality for $(|\Phi\rangle, W(\mathcal{H}))$.

Hence we immediately arrive at our main result:

**Theorem 4** If $\mathcal{M}$ computes a non-linear Boolean function then $\hat{W}(\mathcal{H})$ is a non-Boolean topos.

In other words, non-classical logic is a necessary condition for non-linear function evaluation, and hence universal classical computation in $\ell$-2 MBQC, the model of computation we consider. It does not seem unwarranted to view the
non-Boolean logic of $\hat{W}(H)$ as affording a new potential “resource” for quantum computation. Given other qualities previously mooted as computational resources—entanglement of $|\Phi\rangle$ for instance—we may view non-Booleanness in the same light - a view which is to be strengthened in subsection 7.1 where we will demonstrate the “consumption” of the non-Booleanness by the execution of the Anders and Browne OR-gate. Just as the state after the completion of an $\ell$-2 MBQC is necessarily a product, and is therefore unentangled, we will show that the “final topos” after the completion of the computation is necessarily Boolean.

We turn attention once more the example of Anders and Browne’s OR-gate, in order to demonstrate explicitly the non-Booleanness of the associated topos, and the consumption of non-Booleanness in the course of the computation. Our main conclusions, however, pertain also to any MBQC satisfying definition 4.

### 7.1 Anders and Browne’s OR-gate revisited

The poset $W(H)$ for Anders and Browne’s OR-gate is simply the Hasse diagram given in (13). With $|\Psi\rangle$ as the GHZ state, the pair $(|\Psi\rangle, W(H))$ is clearly contextual and therefore $\hat{W}(H)$ is a non-Boolean topos. It is instructive, however, to also provide a direct proof of the non-Booleanness of $\hat{W}(H)$, given in terms of (the nonexistence of) a complement of $w|\psi\rangle \ni \Sigma$. Recall from definition 13 that a complement of a subobject $A' \ni \Sigma$ is an $A'' \ni \Sigma$ for which $A' \cup A''(V) \sim \Sigma(V)$ for each $V$. We have

**Proposition 7** Let $\hat{W}(H)$ be the topos defined by Anders and Browne’s OR-gate. The subobject $w|\psi\rangle \ni \Sigma$ has no complement.

**Proof.** Consider the (abelian) algebra $V_{X_1}$ generated by the single observable $X_1$, and $V_1 \equiv \{X_1, X_2, X_3\}$. It must be that $w|\psi\rangle(V_{X_1}) = w|\psi\rangle(V_1)|_{V_{X_1}}$, and the putative complement, denoted using a tilde, must be $\tilde{w}|\psi\rangle(V_1)|_{V_{X_1}}$. Writing $\lambda_{\pm}$ as the sections above $V_{X_1}$ defined by $\lambda_{\pm}(a) = \langle \pm | a \pm \rangle$ for a self-adjoint $a \in V_{X_1}$, one finds that $w|\psi\rangle(V_{X_1}) = \{\lambda_+, \lambda_-\} = \tilde{w}|\psi\rangle(V_{X_1})$, which contradicts the definition of complement. ■

We also see in Anders and Browne’s OR-gate that the presheaf $w|\psi\rangle$ specifies the computation “internally” to the topos $\hat{W}(H)$. For the context $V_1$ for example, $w|\psi\rangle$ gives rise to the family of sections $\{\lambda_{+++}, \lambda_{++-}, \lambda_{+-+}, \lambda_{--+}\}$, each of which take value 1 on $X_1X_2X_3$ which coincides with the computed output. Identical behaviour occurs for the three remaining contexts (on $V_2$, for instance, we find the family of sections which evaluate $X_1X_2X_3$ as $-1$).

The above generalises quite naturally to deterministic, temporally flat $\ell$-2 MBQC. As we have seen, for non-linear function evaluation the topos associated to the MBQC must be non-Boolean, a fact which arises from the lack of global section of the relevant pseudostate, one can observe that the computational output can be specified internally to the given topos. This paves the way to a topos description of the computation and a better understanding of the non-Boolean
“internal working” of the computation. In order to justify the perspective that has been put forward, namely that non-Boolean logic is a quantum computational resource, it is paramount to consider the logical situation subsequent to the outcome of the computation being produced.

7.2 “Consumption” of the non-Booleanness $\ell$-2 MBQC

Again referring to the OR-gate, we observe that after the computation is complete, the post-measurement state written $|\Psi_f\rangle$ (whatever it may be) is a product with each factor an eigenstate of one of the six local observables listed in equations (7)-(10). Suppose, for example, that $|\Psi_f\rangle = |+++angle$ (i.e., is an eigenstate of $X_1 X_2 X_3$). We observe that $V_1$ is a maximal abelian subalgebra of $B(\mathbb{C}^8)$, and that clearly no other maximal subalgebra has $|\Psi_f\rangle$ as a local section/joint eigenstate. From the point of view of deterministic $\ell$-2 MBQC, we must therefore restrict attention to the poset (which is also a lattice) $V_1(\mathcal{H})$, i.e., with $V_{X_i} := \{X_i\}$ etc.,

![Diagram](image)

That the presheaf $w^{(\Psi_f)} : V_1(\mathcal{H}) \to \text{Sets}$ does have a global section $1 \to w^{(\Psi_f)}$ follows immediately from $V_1$ being abelian, or by simply noting that $\lambda_{++++}$ is such a global section. $\Sigma$ also has a global section $1 \to \Sigma$, which can be seen directly or via the contrapositive form of proposition 1. Thus we see immediately that there is no state-dependent contextuality with respect to $(\mathcal{H}, V_1(\mathcal{H}))$ or state-independent contextuality with respect to the poset $V_1(\mathcal{H})$. Consequently, only linear functions may be evaluated in deterministic $\ell$-2 MBQC, by theorem 2. Hence $|\Psi_f\rangle$ is clearly not a viable resource for “interesting” computations. Moreover,

**Proposition 8** The topos of presheaves $\hat{V}_1(\mathcal{H})$ is Boolean.

**Proof.** The down-sets $\downarrow V_1(\mathcal{H})$ give rise to the topological space $\mathcal{P}_{V_1}$. By inspection we see that $\mathcal{O}(\mathcal{P}_{V_1})$ is Boolean, since for each open set $U \in \mathcal{O}_{V_1}$, $\neg\neg U = U$. Equivalently we observe that the open sets $\mathcal{O}(\mathcal{P}_{V_1})$ of $(\mathcal{P}_{V_1})$ coincide with the power set of $S = \{V_1, X_1, X_2, X_3\}$. This is simply the discrete topology.

22
on $S$, which is a Boolean algebra. Hence by theorem $\mathbb{I}$ $\text{ShP}_V$ is a Boolean topos, and by proposition $\mathbb{4}$ $\text{Sh}(\mathcal{H})$ is Boolean. 

One could also arrive at this conclusion by noting that $\mathcal{O}(P_V)$ being Boolean entails that $\Gamma\Omega$ is Boolean in the topos $\mathcal{V}_1(\mathcal{H})$, which is enough to conclude that $\mathcal{V}_1(\mathcal{H})$ is Boolean. An identical argument holds for any post-computation state, with $V_1$ replaced by $V_i$ for $i \in \{2, 3, 4\}$; the corresponding topoi are always Boolean.

Not only has the state-dependent contextuality been exhausted by the computation, we may say that the pre-computation non-Booleanness has been “consumed” during its course. This situation clearly manifests also in any deterministic, temporally flat $\ell$-2 MBQC, demonstrating that our findings in the Anders and Browne OR-gate have a natural generalisation to the computations considered in this paper. The relevant post-computation poset in $\ell$-2 MBQC is of a similar form to that depicted in diagram (22), with $V_1$ replaced by $\{O_1(q_1), \ldots, O_n(q_n)\}$, with the $n$ local observables in the second row. It is simple to observe that the topological space consisting of the down-sets is also discrete (and therefore Boolean), thereby demonstrating the generality of our findings in the example of the Anders and Browne OR-gate. This also justifies the view presented here that we may view non-Boolean logic as a quantum computational resource, in the same sense as other resources mooted in the past. Understanding the full impact of this perspective remains a goal for the future. We believe it will be possible to eventually quantify “how much” non-Booleanness is present, both at different stages of a given computation, and the amount required to execute certain computational tasks. This requires mathematical techniques that lie beyond the scope of this paper and constitutes further work.

8 Concluding Remarks and Outlook

Classical logic and classical computation have had a close relationship since the advent of computation; logic delineates the rules of manipulation of computational symbols and allows for the expression of the truth of linguistic sentences. However, there has been little contact between the subjects of quantum computation and “quantum logic”, whichever flavour of the latter one wishes to consider. This paper offers the first footbridge between these thus far disparate disciplines. Interestingly, the specific logical rules which allow for the construction and truth evaluation of sentences in a topos have not been explicitly used. We have instead demonstrated that if one wishes to compute non-linear functions in $\ell$-2 MBQC, thereby possessing a classically universal scheme, a topos closely related to the computation must possess a logical structure fundamentally different from ordinary set theory, pointing to an essential difference between classical and quantum computation. Therefore further examination of the specific structure of the intuitionistic language in the topoi arising from MBQC, and what the language tells us about computation, seems a worthy goal.
Establishing that the ability of a class of quantum computations ($\ell$-2 MBQC) to deterministically compute non-linear functions necessitates that a topos associated to the computation must be non-Boolean, and that a Boolean topos results from the execution of a computation, constitutes a new perspective on the source of quantum-over-classical improvement in computation. Non-Booleanness appears to be a crucial resource for such an improvement - a resource that is depleted by the act of computation. The extent and scope of this view remains unknown.

Acknowledgments

Thanks are due to Chris Heunen and Rebecca Ronke for valuable feedback on an earlier draft of this manuscript.

References

[1] Cleve, R., Ekert, A., Macciavello, C. & Mosca, M. 1998 Quantum algorithms revisited. *Proc. R. Soc. A* 454, 339-354. (DOI 10.1098/rspa.1998.0164.)
[2] Vidal, G. 2003 Efficient Classical Simulation of Slightly Entangled Quantum Computations. *Phys. Rev. Lett.* 91. (DOI 0.1103/Phys-RevLett.91.147902.)
[3] van den Nest, M., Diir, W., Vidal, G. & Briegel, H.-J. 2007 Classical simulation versus universality in measurement-based quantum computation. *Phys. Rev. A* 75. (DOI 10.1103/PhysRevA.75.012337.)
[4] Gottesman, D. 1997 *Stabilizer Codes and Quantum Error Correction* Ph.D. thesis, California Institute of Technology, 8232.
[5] Bremner, M. J., Mora, C. & Winter, A. 2009 Are random pure states useful for quantum computation? *Phys. Rev. Lett.* 102. (DOI 10.1103/Phys-RevLett.102.190502.)
[6] Gross, D., Flammia, S. T. & Eisert, J. 2009 Most Quantum States Are Too Entangled To Be Useful As Computational Resources. *Phys. Rev. Lett.* 102. (DOI 10.1103/PhysRevLett.102.190501.)
[7] Van den Nest, M. 2013 Universal Quantum Computation with Little Entanglement. *Phys. Rev. Lett.* 110. (DOI 10.1103/PhysRevLett.110.060504.)
[8] Bravyi, S. & and Kitaev, A. 2005 Universal quantum computation with ideal Clifford gates and noisy ancillas. *Phys. Rev. A* 71. (DOI 10.1103/PhysRevA.71.022316.)
[9] Veitch, V., Ferrie, C., Gross, D., & Emerson, J. 2012 Negative quasi-probability as a resource for quantum computation. *N. J. Phys.* **14**. (DOI 10.1088/1367-2630/14/11/113011.)

[10] Howard, M., Wallman, J. J., Veitch, V. & Emerson, J. 2014 Contextuality supplies the magic for quantum computation. *Nature* **510**, 351-355. (DOI 10.1038/nature13460.)

[11] Raussendorf, R. 2013 Contextuality in measurement based quantum computation. *Phys. Rev. A* **88** (DOI 10.1103/PhysRevA.88.022322.)

[12] Anders, J. & Browne, D. 2009 Computational Power of Correlations. *Phys. Rev. Lett.* **102** (DOI 10.1103/PhysRevLett.102.050502.)

[13] Mermin, N. D. 1993 Hidden variables and the two theorems of John Bell. *Rev. Mod. Phys.* **65** (DOI 10.1103/RevModPhys.65.803.)

[14] Boole, G. 1958 *An Investigation of the Laws of Thought*, New Edition. Dover.

[15] Dalla Chiara, M., Giuntini, R. & Grecchle, R. 2004 *Reasoning in Quantum theory*, Springer.

[16] Abramsky, S. & Coecke, B. 2004 A categorical semantics of quantum protocols. *Proceedings of the 19th IEEE conference on Logic in Computer Science (LiCS’04).* IEEE Computer Science Press. (DOI 10.1109/LICS.2004.1)

[17] Birkhoff, G. & von Neumann, J. 1936 The Logic of Quantum Mechanics. *Ann. Math.* **37**, 823843.

[18] Isham, C. J. & Döring, A. 2011 ‘What is a thing’?: Topos Theory in the Foundations of Physics. In *New Structures for Physics*, Springer Lecture Notes in Physics (ed. Bob Coecke). **813**, pp. 753-940. Springer, Heidelberg.

[19] Adelman, M. & Corbett, J. 1995 A sheaf model for intuitionistic quantum mechanics. *App. Cat. Str.* **3**, 79-104. (DOI 10.1007/BF00872949.)

[20] Abramsky, S. & Brandenburger, A. 2011 The sheaf-theoretic structure of non-locality and contextuality. *N. J. Phys.* **13**. (DOI 10.1088/1367-2630/13/11/113036.)

[21] Abramsky, S., Mansfield, S. & Barbosa, R. S. 2012 The Cohomology of Non-Locality and Contextuality. *Proceedings 8th International Workshop on Quantum Physics and Logic Nijmegen, Netherlands* **95**, 1-14. Op. Pub. Ass. (DOI 10.4204/EPTCS.95.1.)

[22] Isham, C. J., Butterfield, J. & Hamilton, A. 2000 Topos Perspective on the Kochen-Specker Theorem: III. Von Neumann Algebras as the Base Category. *Int. J. Th. Phys.* **39**, 1413-1436. (DOI 10.1023/A:1003667607842.)
[23] Redhead M. 1993 *Incompleteness, Nonlocality and Realism*, Reprint Edition. Clarendon Press.

[24] Kochen, S. & Specker, E. P. 1967 The problem of hidden variables in quantum mechanics. *J. Math. Mech.* 17, 59-87.

[25] de Muynck, W. M. 2002 *Foundations of Quantum Mechanics, An Empiricist Approach*. Springer.

[26] Kobayashi, S. & Nomizu, K. 1996 *Foundations of Differential Geometry, Vol.1*. Wiley.

[27] Lawvere, W. & Rosebrugh, R. 2003 *Sets for Mathematics*. CUP.

[28] Greenberger, D. M., Horne, M. A. & Zeilinger, A. 1989 Going Beyond Bells Theorem. In *Bell’s Theorem, Quantum Theory, and Conceptions of the Universe* (ed. M. Kafatos), pp. 69 - 72. Kluwer, Dordrecht.

[29] Mermin, N. D. 1990 Quantum Mysteries Revisited. *Am. J. Phys.* 58, 731. (DOI 10.1119/1.16503)

[30] Briegel, H.-J. & Raussendorf, R. 2001 Persistent Entanglement in Arrays of Interacting Particles. *Phys. Rev. Lett.* 86, 910. (DOI 10.1103/PhysRevLett.86.910.)

[31] Schlingemann, D. & Werner, R. F. 2001 Quantum error-correcting codes associated with graphs. *Phys. Rev. A* 65. (DOI 10.1103/PhysRevA.65.012308.)

[32] Raussendorf, R. & Briegel, H.-J. 2001 A one-way quantum computer. *Phys. Rev. Lett.* 86. (DOI 10.1103/PhysRevLett.86.5188.)

[33] Leung, D. W. 2004 Quantum Computation by Measurements. *Int. J. Quant. Inf.* 2. (DOI 10.1142/S0219749904000055.)

[34] Gross, D. & Eisert, J. 2007 Novel Schemes for Measurement-Based Quantum Computation. *Phys. Rev. Lett.* 98. (DOI 10.1103/PhysRevLett.98.220503.)

[35] Chen, X., Duan, R., Ji, Z. & Zeng, B. 2010 Quantum State Reduction for Universal Measurement Based Computation. *Phys. Rev. Lett.* 105. (DOI 10.1103/PhysRevLett.105.020502.)

[36] Miyake, A. 2011 Quantum computational capability of a 2D valence bond solid phase. *Ann. Phys.* 326, 16561671 (DOI 10.1016/j.aop.2011.03.006.)

[37] Wei, T. C., Affleck, I. & and Raussendorf R. 2011 Affleck-Kennedy-Lieb-Tasaki State on a Honeycomb Lattice is a Universal Quantum Computational Resource. *Phys. Rev. Lett.* 106. (DOI 10.1103/PhysRevLett.106.070501.)
[38] Else, D. V., Schwarz, I., Bartlett S. D. & Doherty, A. C. 2012 Symmetry-
Protected Phases for Measurement-Based Quantum Computation. Phys.
Rev. Lett. 108. (DOI 10.1103/PhysRevLett.108.240505.)

[39] Kadison, R. V. & Ringrose, J. R. 1997 Fundamentals of the theory of opera-
tor algebras volume I: elementary theory. American Mathematical Society.

[40] Shor, P. 1994 Algorithms for quantum computation: discrete logarithms
and factoring. Proceedings of the 35th Annual Symposium on Foundations
of Computer Science, Santa Fe, NM, 124-134. IEEE Press, New York. (DOI
10.1109/SFCS.1994.365700.)

[41] Mosca, M. & Zalka, C. 2004 Exact quantum Fourier transforms
and discrete logarithm algorithms. Int. J. Quant. Inf., 91-100. (DOI
10.1142/S0219749904000109.)

[42] MacWilliams, F. J. & Sloane, N. A. 1977 The Theory of Error-Correcting
Codes. North-Holland.

[43] Johnstone, P. 2013 Topos Theory, Reprint Edition. Dover.

[44] Moerdijk, I. & Mac Lane, S. 1992 Sheaves in Geometry and Logic, A First
Introduction to Topos Theory, 1st edn. Springer.

[45] Flori, C. 2013 A first course in topos quantum theory. Springer.

[46] Borceux, F. 2008 Handbook of categorical algebra 3 Categories of Sheaves.
CUP.

[47] Bell, J. & Machover, M. 1977 A Course in Mathematical Logic. North
Holland.

[48] Johnstone, P. 2002 Sketches of an Elephant: A Topos Theory Compendium
vol. II. OUP.