Thesis report for the BSc Applied Physics and BSc Applied Mathematics

A Critique of Topos Logic in Measurement-Based Quantum Computation

Storm Diephuis

Delft University of Technology

Supervisors

Dr. K.P. Hart　　Dr. D. Elkouss

Other committee members

Dr. E. Coplakova　　Dr. M. Blaauboer

July, 2020　　Delft

Abstract

Topos theory and quantum mechanics are both known for having a logic that is different from ordinary logic. With this in mind, much work has been done on unifying these two fields. Loveridge, Dridi and Raussendorf apply this unification to measurement-based quantum computation [14], revealing links between computation, contextuality and the failure of the law of excluded middle in the topoi associated with each computation. We review their work, fill in gaps, follow their research suggestion and have some criticism. Our main original finding is a formula, in the formal language of the topos associated with a computation, that expresses that the computation is deterministic.

Contents

Chapter 1

Introduction

Topos theory was initiated by Grothendieck in the 1950s and is based on category theory, which was developed only a decade earlier by Eilenberg and Mac Lane. Topoi (the Greek plural of "topos") are a generalisation of set theory. We speak of objects instead of sets, and of arrows or morphisms instead of functions. In a topos, objects are indeed similar to sets: there is a subobject relation and we can construct unions, products and power objects from given objects, among other things. Of course, there are differences with sets too. Most importantly, an object is no longer defined by its elements, in the way that sets are. In a certain sense, some non-trivial objects do not even have any elements! Another consequence of the generalisation is that the logic is altered. Not all of our familiar tautologies apply to a topos, but only those of *intuitionistic* logic, in which, for example, the law of excluded middle no longer holds: $p \vee \neg p$ is not valid for all propositions p,

It is well known that ordinary logic is not always suitable for quantum mechanics. For this and other reasons, attempts have been made to apply topos theory to quantum mechanics. It seems that Adelman and Corbett were the first to publish on this matter in 1995 [1]. Arguably the most influential publication, however, is *'What is a Thing?': Topos Theory in the Foundations of Physics* by Döring and Isham, which appeared only in 2008 [7]. They use topoi for "a fundamentally new way of constructing theories of physics", not even assuming that measurement outcomes have to be real-valued. By now, *topos quantum theory* can be called an actual field of study. Introductions to it can be found in [8] or in the twelfth chapter of [13].

So far, applications of topos theory specifically to quantum information and computation have been scarce. In this report, we will focus on the paper by Loveridge, Dridi and Raussendorf [14], which deals with so-called measurement-based quantum computation (MBQC). Another publication on topos theory and quantum information theory is [6]. The authors of [14] have two main messages. Firstly, they review how *contextuality*, a feature of quantum theory, manifests itself in topoi [10] and in MBQC [18], and unify these two views. Secondly, they expound some relations between MBQC and the logic of associated topoi. Our focus is on this second subject, but the first one will be touched on as well. The paper [14] also poses a research suggestion: properties of an MBQC may be represented internally in its associated topos.

The next three chapters will provide all prerequisites for understanding [14]. Chapter 2 reviews the basics of quantum theory and introduces *contexts* and *valuations*. Chapter 3 defines the setting of measurement-based quantum computation. Chapter 4 introduces the required parts of topos theory. Chapter 5 comprises the core of this report. It retells the ideas occurring in [14], while filling some gaps. We also work on the research suggestion. Our main result is indeed a formula in the language of a topos whose truth is equivalent to the determinism of the underlying MBQC. Chapter 5 also gives some criticism of the claims in [14]. Finally, our findings are summarised in Chapter 6. There is a list of symbols at the end of this document.

Chapter 2

Quantum theory preliminaries

In this chapter we first review the most important ingredients of quantum theory relevant for this report. This serves merely to fix notation and refresh the knowledge of quantum theory, and should not be read as an introduction to quantum theory. Secondly, we introduce *contexts* and *valuations*, and derive some properties that will be useful later on.

2.1 Basics

Throughout this report, we will only work with finite dimensional complex Hilbert spaces $\mathcal{H}$, as is usual for quantum computation. This means that, without loss of generality, we can always assume that the Hilbert space is of the form $\mathbb{C}^n$, that we can use matrix notation and that the inner product is the dot product.

A state, that is, a vector in the Hilbert space with norm one, may be represented by a Greek letters like ϕ or the *ket* $|\phi\rangle$, using bra-ket notation. In bra-ket notation, the *bra* $\langle\phi|$ is the Hermitian transpose of $|\phi\rangle$, so that the inner product can be conveniently written as $\langle\psi|\phi\rangle$. If ϕ is a vector of the Hilbert space $\mathcal{H}_1$ and ψ of $\mathcal{H}_2$ then the expressions $\phi \otimes \psi$, $|\phi\rangle \otimes |\psi\rangle$, $|\phi\rangle\,|\psi\rangle$ and $|\phi\psi\rangle$ all denote the same vectors in the tensor product space space $\mathcal{H}_1 \otimes \mathcal{H}_2$.

Whenever we speak of an *operator* on a Hilbert space $\mathcal{H}$, we mean a *linear operator*. Strictly speaking, an *observable* is a physical quantity that can be represented by a self-adjoint linear operator on $\mathcal{H}$. However, in our abstract approach we shall abuse the term and call any self-adjoint linear operator an observable. By the spectral theorem, an observable $A\colon \mathcal{H} \to \mathcal{H}$ can be written[1] as $A = \sum_i \mu_i P_i$, where the μ_i's are distinct eigenvalues of A and the P_i's are projections. We call each P_i an *eigenprojection* of A and its corresponding subspace of $\mathcal{H}$ an *eigenspace* of A. We shall call subspaces of an eigenspace eigenspaces as well, and similar for projections.

Suppose that a system is represented by a state ϕ. If we perform a measurement of the physical quantity corresponding to an observable A, then, in general, the system changes and is represented by a new state ψ. This new state is chosen randomly and must be an eigenstate of A. ψ is (the normalised version of) $P_i\,|\phi\rangle$ with probability $\langle\phi|P_i|\phi\rangle$, and in that case the measurement outcome is μ_i, the corresponding eigenvalue. So if ϕ is orthogonal to the eigenprojection P_j, the outcome of a measurement of A will never be μ_j. From now on, whenever we speak of a measurement, we only mean the mathematical process of choosing a particular new state and obtaining the corresponding eigenvalue as the outcome.

[1] Note that here we use the tacit assumption of the Hilbert space being finite dimensional. From now on, we will not always explicitly mention this assumption.

2.2 Qubits

In quantum computation, qubits are commonly the building blocks. A qubit can be implemented using a large number of physical setups, but can always represented by the Hilbert space $\mathbb{C}^2$. Three important observables are the Pauli matrices:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

We designate their eigenstates by $|+\rangle$ and $|-\rangle$ for X, by $|\uparrow\rangle$ and $|\downarrow\rangle$ for Y and by $|0\rangle$ and $|1\rangle$ for Z, each corresponding respectively to the eigenvalues 1 and -1.

Suppose that we have two qubits that are in a state $\phi = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \in \mathbb{C}^2 \otimes \mathbb{C}^2$. The qubits are entangled, so we cannot view them as completely separate physical systems. But we could still measure Z for the first qubit, disregarding the second one. It is not immediately clear how this changes the overall state. However, we could interpret "doing nothing" as measuring I, the identity operator. So measuring Z for the first qubit and doing nothing with the second qubit amounts to measuring $Z \otimes I$ for the ensemble. Projecting ϕ onto the eigenspaces of $Z \otimes I$, we see that the state must collapse to either $|00\rangle$ or $|11\rangle$, with equal probability, and with respective measurement outcomes 1 and -1. The above generalises to larger ensembles and other positions of the one-qubit observable in the tensor product[2].

2.3 Contexts and valuations

If a state ϕ is an eigenstate of an observable A, then A has a definite value for ϕ, namely the eigenvalue of ϕ. If we keep measuring A we always get the same outcome. On the other hand, if an observable B shares no eigenvectors with A, they cannot measured simultaneously. If we first measure A, then B and then A again, we may get a different outcome for A on both occasions. If two or more observables do have a common eigenbase (a set of eigenvectors that span the space), we call them compatible. Evidently, compatible observables can be measured simultaneously. It can be shown that observables are compatible if and only if they commute. This leads to the following definition.

Definition 2.1. *If $\mathcal{H}$ is a finite dimensional Hilbert space, then $B(\mathcal{H})$ is the C*-algebra of all the linear operators on $\mathcal{H}$. In addition, $\mathcal{V}(\mathcal{H})$ is the set of all unital Abelian subalgebras of $B(\mathcal{H})$. An element of $\mathcal{V}(\mathcal{H})$ is called a (measurement) context.*

A *C*-algebra* is a vector space equipped with an additional multiplication and adjoint (*) operation on the space, satisfying certain requirements. In this case the multiplication is given by composition of operators (i.e. matrix multiplication), and the *-operation is given by taking the adjoint of an operator (i.e. the Hermitian transpose of a matrix). $\mathbb{C}$, with standard multiplication and complex conjugation as the *-operation, is a C*-algebra as well. A *subalgebra* of $B(\mathcal{H})$ is a subset of $B(\mathcal{H})$ that is closed under all four operations of $B(\mathcal{H})$ (and thus is a C*-algebra itself). It is *unital* when it contains the unit operator I on $\mathcal{H}$ and it is *Abelian* when all its elements commute under composition.

The observables in a context commute and therefore are compatible. This is why it is called a context. We may not be able to assign values to every observable of $B(\mathcal{H})$ in a consistent manner, but we can certainly do so in a particular context. The merit of the extra structure that comes with a context becomes clear from the following elegant definition

[2] This reasoning is actually a bit sloppy, since, for example, measuring $X \otimes X$ is *not* the same as first measuring X for the first qubit and then for the second one.

Definition 2.2. A *valuation* of a context V is a *-homomorphism $\lambda\colon V \to \mathbb{C}$: a function that preserves the unit element and all four C*-algebra operations. $\Sigma(V)$ is the set of all valuations of V.

It will turn out, perhaps surprisingly, that a valuation assigns only eigenvalues to observables. Indeed, a common eigenstate ϕ of a context V determines a corresponding valuation that takes each observable to its eigenvalue for ϕ. To prove this, we need the following proposition.

Proposition 2.3. *Let $V \in \mathcal{V}(\mathcal{H})$ and $A \in V$. Then A is normal, has orthogonal eigenspaces and the projection for each eigenspace of A is in V as well.*

Proof. First of all, $A^* \in V$ and A is normal (i.e. $AA^* = A^*A$), because V is an Abelian subalgebra. Since A is normal, it has orthogonal eigenspaces (by the spectral theorem).

Now let $\mu_1, \ldots, \mu_n$ be an enumeration of all the (distinct) eigenvalues of A (this is possible since $\mathcal{H}$ is finite dimensional). We will show that $P = \alpha \prod_{i \neq m}(A - \mu_i I)$ is the eigenprojection belonging to eigenvalue μ_m, for a suitable $\alpha \in \mathbb{C}$. Since $A, I \in V$ and since V is closed under all operations used in the construction of P, also $P \in V$.

Let ψ be an arbitrary vector and write it as a linear combination of eigenvectors of A: $\psi = a_1\phi_1 + \cdots + a_k\phi_k$, where ϕ_i is an eigenvector with eigenvalue μ_i. Each $(A - \mu_i I)$ is orthogonal to ϕ_i, so P filters out ϕ_m: $P\psi = a_m\beta\phi_m$. Here, $\beta = \prod_{i \neq m}(\mu_m - \mu_i)$, so $\beta \neq 0$ (because the eigenvalues are distinct). Therefore, we can set $\alpha = \beta^{-1}$, turning $P \in V$ into the desired projection. □

Proposition 2.4. *For any $A \in V \in \mathcal{V}(\mathcal{H})$ and valuation λ of V, we have that $\lambda(A) \in \sigma(A)$, the spectrum of eigenvalues of A.*

Proof. For any projection $P \in V$, $\lambda(P) = \lambda(PP) = \lambda(P)^2$, so $\lambda(P) = 0$ or $\lambda(P) = 1$. Since A is normal and since its orthogonal eigenprojections P_i are in V, we can write $A = \sum_i \mu_i P_i$. Because $\sum_i P_i = I$ and $1 = \lambda(I) = \lambda(\sum_i P_i) = \sum_i \lambda(P_i)$, it must be that only one $\lambda(P_j)$ is nonzero. Therefore, $\lambda(A) = \lambda(\sum_i \mu_i P_i) = \sum_i \mu_i \lambda(P_i) = \mu_j \in \sigma(A)$. □

Valuations behave in the way we want them to: they assign eigenvalues (and therefore, possible measurement outcomes) to observables. The fact that they assign values to other operators too does not mean much, because those operators never correspond to physical quantities. But including operators that are not self-adjoint in contexts does not hurt and even makes our proofs simpler.

2.4 Contextuality

One of the counter-intuitive consequences of quantum mechanics is that some physical quantities do not have a definite value, even when we know that a system is in a particular state. This happens when the state is not an eigenvector of an observable, so that we cannot associate just one eigenvalue with it. However, a measurement of such a quantity still always yields a single value. It is natural to wonder whether the quantities have definite values prior to measurement after all, and that we just do not know everything about the state of a system — that we are missing certain *hidden variables*. A theory that accommodates this idea is called a *non-contextual hidden variable theory*. One approach to such a theory is trying to find a valuation for each context, in such a way that the valuations do not contradict each other. To see how valuations of different contexts are related, we note that $\mathcal{V}(\mathcal{H})$ has some extra structure, namely a partial order:

Definition 2.5. A *partially ordered set*, or a *poset*, is a pair $P = \langle |P|, \leq \rangle$ such that $\leq$ is a reflexive, antisymmetric and transitive relation on $|P|$. For ease of notation, we shall use the same symbol for a poset and its underlying set, i.e. write P instead of $|P|$.

Antisymmetry means that $p \leq q$ and $q \leq p$ imply $p = q$. So a poset is similar to a linearly ordered set, except that not all elements need to be comparable. A standard example of a poset is the powerset $\mathscr{P}(X)$ ordered by inclusion (the subset relation), for any set X.

We can order $\mathcal{V}(\mathcal{H})$ by inclusion as well, turning it into a poset. If $U \subseteq V$ are contexts, then any valuation λ_V of V determines one of U, namely the restriction of λ_V to the domain U. Thus for two contexts V and W, we could ask ourselves: are there valuations of V and W that coincide on $V \cap W$? Even more general, we define the following.

Definition 2.6. A *global valuation* of $\mathcal{V}(\mathcal{H})$ is a function with domain $\mathcal{V}(\mathcal{H})$ that assigns a valuation λ_V to each context V, such that, if $U \subseteq V$, then $\lambda_U = \lambda_V|_U$, the restriction of λ_V to the domain U.

It is a corollary of the Kochen-Specker[3] theorem [12] that, if the dimension of $\mathcal{H}$ is at least 3, no global valuations of $\mathcal{V}(\mathcal{H})$ exist. This feature is called *contextuality* and makes it particularly hard to maintain a realist's view of hidden but definite values. As we will see in Chapter 5, contextuality can be formulated very neatly using topos theory.

2.5 Some more properties of contexts and valuations

Looking at the proofs of Propositions 2.3 and 2.4, it seems that there is an intimate relation between a valuation and the projections that get value 1. To investigate this relation we consider a structure containing all projections of a context.

Definition 2.7. A *lattice* L is a poset such that every two elements $a, b \in L$ have a least upper bound $a \vee b$ (called the *join*) and a greatest lower bound $a \wedge b$ (called the *meet*). *Least upper bound* means that that $a \leq a \vee b$ and $b \leq a \vee b$ and, if $a \leq c$ and $b \leq c$, then $a \vee b \leq c$. *Greatest upper bound* is similarly defined.

As an example, the powerset poset from before is a lattice as well. The join of two sets turns out to be their union, and the meet their intersection. The projections in a context form a lattice as well.

Definition 2.8. For any subalgebra V of $B(\mathcal{H})$, the *lattice of projections* $\mathcal{P}(V)$ is defined as follows.

- Its elements are all the projections in V.
- $P \leq Q$ if and only if the image of P is included in the image of Q.
- $P \wedge Q$ is the projection that has as image the intersection of the images of P and Q.
- $P \vee Q$ is the projection that has as image the span of the images of P and Q.

It is easily shown that this indeed satisfies the definition of a lattice. Note that $P \wedge Q = PQ$ and that $P \vee Q = (I - (I - P)(I - Q)) = P + Q - PQ$, so that the lattice operations do not lead out of V.

[3] This theorem was in fact proven by the eponymous authors only a year after J. S. Bell had proven it [4], but it should not be confused with Bell's other famous theorem of non-locality [3].

Definition 2.9. Let $V \in \mathcal{V}(\mathcal{H})$. We define $M_V \subseteq \mathcal{P}(V)$ to be the set of minimal elements of $\mathcal{P}(V) \setminus \{ 0 \}$. So if $P \in M_V$, $Q \in \mathcal{P}(\mathcal{V})$ and $Q \leq P$, then $Q = P$ or $Q = 0$.

It is known that, given a set of commuting observables, a common eigenstate specifies a value for each observable, that is, a valuation. Conversely, if the set of commuting observables is refined enough, then a valuation unambiguously specifies a state. The following result generalises this.

Theorem 2.10. *Let $V \in \mathcal{V}(\mathcal{H})$. Then there is a bijection $\tau_V \colon \Sigma(V) \to M_V$ such that $A\tau_V(\lambda) = \lambda(A)\tau_V(\lambda)$ for each $\lambda \in \Sigma(V)$ and $A \in V$.*

Proof. First, we construct τ_V in a few steps and prove that it satisfies the eigenvalue equation. Afterwards, we prove that this τ_V is indeed a bijection.

- We show that the projections in M_V are pairwise orthogonal. Let $P, Q \in M_V$. $PQ \leq P$ and $PQ \leq Q$, but $PQ \in \mathcal{P}(V)$ and P and Q are minimal in $\mathcal{P}(V) \setminus \{ 0 \}$, so either $P = Q$ or $PQ = 0$. Therefore, distinct projections in M_V are orthogonal.

- We show that M_V generates $\mathcal{P}(V)$ under the lattice operations. We want to write any $P \in \mathcal{P}(V)$ as an iterated join of projections in M_V. If $P \in M_V$ we are done. If not, P is not minimal, and there must be a $Q_1 \in M_V$ such that $Q_1 \leq P$. Construct $P' = P - Q_1$. Since Q_1 and P' are orthogonal, $P = Q_1 + P' = Q_1 \vee P'$. If $P' \in M_V$ we are done. If not, repeat what we did with P for P'. Since $\mathcal{H}$ is finite dimensional, this process stops at some point with $P = Q_1 \vee (Q_2 \vee (\cdots \vee Q_k) \cdots)) = Q_1 + \cdots + Q_k$, with each $Q_i \in M_V$.

- From this follows that $I = \sum M_V$ so, just as in the proof of Proposition 2.4, for any valuation λ only one projection Q_λ in M_V gets value 1 and all the others get value 0. Therefore, let $\tau_V \colon \lambda \mapsto Q_\lambda$, the unique projection in M_V to which λ assigns the value 1.

- Because of point 2 and Proposition 2.3, we can write each $A \in V$ as $A = \sum_{P \in M_V} \mu_P P$. Let $\lambda \in \Sigma(V)$. Now $A\tau_V(\lambda) = \mu_{\tau_V(\lambda)}\tau_V(\lambda)$, because $\tau_V(\lambda) \in M_V$ is orthogonal to all other projections in M_V. Moreover, $\lambda(A) = \sum_{P \in M_V} \mu_P \lambda(P) = \mu_{\tau_V(\lambda)}$. Hence $A\tau_V(\lambda) = \lambda(A)\tau_V(\lambda)$, as desired.

We still need to show that τ_V is invertible. (In fact, we have not even shown that there exist any valuations at all.) Let $Q \in M_V$. We have seen in the last step that Q is an eigenprojection for every $A \in V$. So let $\tau_V^{-1}(Q) \colon A \mapsto \mu_Q$, the eigenvalue of A for Q. We need to show that the function $\lambda = \tau_V^{-1}(Q)$ is a valuation, i.e., a *-homomorphism. To this end, let $A, B \in V$ and $\alpha \in \mathbb{C}$ be arbitrary.

- It immediately follows from the definition that $\lambda(0) = 0$ and $V(I) = 1$.

- $\lambda(A^*) = \lambda(A)^*$, because the eigenvalues of A^* are those of A conjugated.

- $\lambda(\alpha A) = \alpha\lambda(A)$, because the eigenvalues of αA are those of A multiplied by α.

- Write $A = \sum_{P \in M_V} \mu_P P$ and $B = \sum_{P \in M_V} \nu_P P$. Then $A + B = \sum_{P \in M_V} (\mu_P + \nu_P) P$ so $\lambda(A + B) = \mu_Q + \nu_Q = \lambda(A) + \lambda(B)$.

- Similarly, $AB = \sum_{P \in M_V} (\mu_P \nu_P) P$ so $\lambda(AB) = \mu_Q \nu_Q = \lambda(A)\lambda(B)$.

Therefore τ_V^{-1} yields a valuation for each $P \in M_V$ and it clearly inverts τ_V. So τ_V is a bijection with the desired property. □

It is important to notice that not all common eigenprojections of a context V are in V themselves. For example, if V has a rank-2 common eigenprojection P and $Q \leq P$ is rank-1, then there is no $A \in V$ that distinguishes Q and $P - Q$ by eigenvalue, so Q cannot be constructed as in Proposition 2.3. From this it follows that M_V could be described as the set of largest common eigenprojections of V: if $P \in M_V$ and $P < Q$, then Q is not an eigenprojection of every $A \in V$, while if $Q < P$, then $Q \notin M_V$.

The upshot of this section is that a context V and its valuations are completely determined by M_V, the 'minimal' projections in V (barring 0). Finally, the following construction is useful for generating contexts.

Definition 2.11. Given $S \subseteq B(\mathcal{H})$, the *commutant* of S is $S' = \{ X \mid AX = XA \text{ for all } A \in S \}$. So S' is the set of operators that commute with every operator in S. S'' is called the *bicommutant* of S.

Proposition 2.12. *If $S \subseteq B(\mathcal{H})$ is a set of commuting linear operators that is closed under taking adjoints, then its bicommutant S'' is a context, $S \subseteq S''$, and S and S'' have the same common eigenspaces.*

Proof. To show that S'' is a context is to show that it is a unital Abelian subalgebra of $B(\mathcal{H})$.

- Let $A, B \in S''$ and $\alpha \in \mathbb{C}$ be arbitrary. Clearly αA, $A + B$ and AB also commute with every operator of S', so S'' is closed under these operations.
- Let $X \in S'$. Then X commutes with $O^* \in S$ for any $O \in S$, so $OX^* = (XO^*)^* = (O^*X)^* = X^*O$. Thus X^* commutes with every operator in S: $X^* \in S'$. This shows that S' is closed under taking adjoints. The same holds for S''. Combining this with the previous item, we see that S'' is a C*-algebra.
- Since I commutes with every operator, $I \in S''$; S'' is unital.
- Since every $A \in S$ commutes with every other operator of S, also $A \in S'$ and hence $S \subseteq S'$. So the operators in S'' also commute with the operators in S, and therefore $S'' \subseteq S'$. From this follows that the operators of S'' commute, i.e. S'' is Abelian.

Clearly every operator in S commutes with every operator in S', so $S \subseteq S''$. Hence every common eigenspace of S'' is also a common eigenspace of S. For the other direction, suppose that P is a common eigenprojection of S. This means that any $X \in S$ acts as a scaled identity on the image of P: for any operator A, $XPAP = PAPX$ and thus $PAP \in S'$. Any $O \in S''$ has to commute with every PAP as well, but this is only possible if O too is a scaled identity on the image of P. Hence, P is a common eigenprojection of S''. We conclude that S and S'' have the same eigenspaces. □

From this it follows that if S is a set of observables, and if all observables in S are measured, the outcomes uniquely determine a valuation of S''. Therefore, from now on we can speak of *measuring a context*, by which we mean measuring the observables in the context, and of *getting the valuation λ as an outcome.*

Chapter 3

Quantum computation

Quantum computation can be implemented using many different schemes (or at least in theory), exploiting different quantum-mechanical phenomena. Following [14], we concern us with so-called *measurement-based quantum computation* (abbreviated *MBQC*), or better yet, a restricted version of it. The goal of this chapter is to explain, simplify and formalise this type of computation.

3.1 Description

General MBQC was introduced in [19]. One computation simply outputs a string of (classical) bits, given an input of bits. This is effected by a series of measurements on an ensemble of qubits, which start off in a predetermined, entangled state. The output is calculated from the measurement outcomes. Which measurements are done depends on the input and on the intermediate measurements results. This second dependence is useful, because it allows to counteract the stochastic nature of measurements.

The measurements are *local*: only one qubit is measured at a time. The idea is that this is more feasible in practice than many-qubit measurements. Once a qubit is measured, it is no longer entangled with the other qubits. The computation destroys the entanglement. That is why the authors of [19] call it a *one-way quantum computer*. Of course, the initial entangled state can be created anew by another form of processing, but not with just the local measurements of MBQC.

In [14], only a specific type of MBQC is dealt with, called $\ell 2$-MBQC, which was introduced in [18]. It has three restrictions:

- For each qubit, only two different observables are allowed to be measured, encoded by 0 and 1.
- The observables have two different outcomes (and therefore are non-degenerate) which are encoded by 0 and 1.
- All classical side processing is linear.

The classical side processing is what computes which observables are measured and calculates the final output from all the measurement results. Linearity means that it can only use addition modulo 2 of bits. For example, given that the input is a string of bits $(i_1, \ldots, i_n)$, which observable is measured for the first qubit is determined by something of the form $i_{k_1} \oplus \cdots \oplus i_{k_l}$, where "$\oplus$" is addition modulo 2. Similarly, the output must be calculated as a sum modulo 2 of the measurement results.

This is $\ell 2$-MBQC as it is defined in [18]. There, it is proven that this scheme is universal for quantum computation: it can compute any Boolean function, and (potentially) has the same speedup over classical computations as other quantum based computations have. Specifically, there are certain problems (like the prime factorisation of a natural number) for which the best known classical algorithms have a (sub)exponential complexity, while the number of qubits needed to solve the problem with $\ell 2$-MBQC only depends polynomially on the input size of the problem.

Before formalising $\ell 2$-MBQC mathematically, we make two more simplifications. The first one is that all observables have eigenvalues 1 and -1, and that those eigenvalues are encoded as 0 and 1 respectively. This imposes no restriction on the computational power. To see this, diagonalise an arbitrary non-degenerate qubit observable as $A = UDU^{-1}$. If we replace D by Z or $-Z$, then the resulting observable has the same effect on states when measured, and the eigenvalue encoding is conveniently absorbed into the sign. In light of this, we define the following:

Definition 3.1. $\iota\colon \{1,-1\} \to \{0,1\}$ maps 1 to 0 and -1 to 1.

We could even call this little function a homomorphism, because $\iota(ab) = \iota(a) \oplus \iota(b)$ for all $a, b \in \{1,-1\}$. The second simplification is that the two observables belonging to a qubit do not share any eigenstates. We will explain this simplification later and show that it not a severe restriction.

3.2 Definition

The mathematical formulation of an $\ell 2$-MBQC is now as follows.

Definition 3.2. An $\ell 2$-MBQC consists of the following:

- Positive integers d, n and m, corresponding respectively to the resource state size (in number of qubits) and the in- and output sizes (in number of bits).
- An initial resource state $\psi \in \mathcal{H} = \mathbb{C}^{2^d}$.
- For each qubit $k \in \{1,\dots,d\}$, two self-adjoint linear operators $O_k(0)$ and $O_k(1)$ on $\mathbb{C}^2$, with eigenvalues in $\{1,-1\}$, that share no eigenstates. For the corresponding observables on the ensemble of qubits, we write A_k^0 and A_k^1. For example, $A_2^0 = I \otimes O_2(0) \otimes I \otimes \cdots \otimes I \in B(\mathcal{H})$.
- A $d \times n$ matrix Q and a $d \times d$ matrix T, both with elements in $\{0,1\}$, such that T is lower triangular with zeroes on the diagonal.
- An $m \times d$ matrix R with elements in $\{0,1\}$.

The choice of observables is represented by $\mathbf{q} = (q_1,\dots,q_d) \in \{0,1\}^d$, so that $O_k(q_k)$ is measured for each qubit k. The outcome μ after measuring qubit k (whether using $O_k(0)$ or $O_k(1)$) is represented by $s_k = \iota(\mu)$, yielding a vector of measurement results $\mathbf{s} = (s_1,\dots,s_d) \in \{0,1\}^d$. Given an input $\mathbf{i} = (i_1,\dots,i_n) \in \{0,1\}^n$, the choice of measurements is determined by

$$\mathbf{q} = T\mathbf{s} + Q\mathbf{i} \pmod 2.$$

Because of the shape of T, $\mathbf{q}$ can be calculated one element at a time (we need q_k before we can get s_k, and in general we need s_k before we can get q_{k+1}). After all measurements have been performed, the final output is calculated using

$$\mathbf{o} = (o_1,\dots,o_m) = R\mathbf{s} \pmod 2.$$

The (mod 2) in the vector equations should be interpreted row-wise. Note that the observables on different qubits, regarded as observables on the ensemble, commute, so that it would not matter in which order the qubits are measured.

The linearity of side processing seems like an arbitrary demand. But in [18], where $\ell 2$-MBQC was introduced, it was an essential assumption for some proofs. For us, it will mostly be a convenience in notation, but not indispensable at all.

An $\ell 2$-MBQC can have the following special properties:

Definition 3.3. An $\ell 2$-MBQC is called *temporally flat* if $T = 0$. In this case, $\mathbf{q}$ can be calculated all at once there is no restriction on the order in which the qubits are measured.

Definition 3.4. An $\ell 2$-MBQC is called *deterministic for input* $\mathbf{i} \in \{ 0,1 \}^n$ if there is only one possible output $\mathbf{o}$ the input $\mathbf{i}$.

Definition 3.5. An $\ell 2$-MBQC is called *deterministic* if it is deterministic for each input. In this case, we can write the output as a function $\mathbf{o}(\mathbf{i})$.

3.3 Example

The following example, which occurs frequently in [14], is based on an article by Anders and Browne [2], who in turn got the idea from Mermin's alternative proof [17] of the Kochen-Specker theorem [12].

Example 3.6. An $\ell 2$-MBQC for the Anders and Browne OR-gate is given by

- $d = 3$, $n = 2$ and $m = 1$.
- $\psi = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$.
- $O_k(0) = X$ and $O_k(1) = Y$ for each k.
- $Q = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{pmatrix}$, $T = 0$.
- $R = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$.

This MBQC does what you think it does: it deterministically performs the OR operation on the two input bits. We describe one possible execution of the MBQC. Let the input be 00. In this case, we will measure X for each qubit. We can rewrite $\psi = \frac{1}{2\sqrt{2}}(|+\rangle (|00\rangle + |11\rangle) + |-\rangle (|00\rangle - |11\rangle))$. Suppose that after measuring X for the first qubit, the outcome is 1. The ensemble of qubits is then represented by the state $\psi' = \frac{1}{\sqrt{2}} |+\rangle (|00\rangle + |11\rangle)$. Suppose that after measuring X for the second qubit, the outcome is -1. Then the new state must be $\psi'' = \frac{1}{\sqrt{2}} |+\rangle |-\rangle (|0\rangle - |1\rangle) = |+--\rangle$. The non-entangled state of the third qubit is now an eigenstate of X, and the last measurement outcome must also be -1. Therefore, the outcome vector is $\mathbf{s} = (0,1,1)$ and the final output is $o = Z\mathbf{s} = 0$. Indeed, $0 \vee 0 = 0$.

To show that this $\ell 2$-MBQC always computes the OR operation, it helps to apply our theory of contexts and valuations. Each input $\mathbf{i}$ determines a $\mathbf{q} \in \{ 0,1 \}^d$, and therefore a set $S_\mathbf{i}$ of observables. By Proposition 2.12, measuring $S_\mathbf{i}$ fixes a valuation λ of the context $S_\mathbf{i}''$. The outcome of the MBQC is $o = \iota(\lambda(A_1^{q_1})) \oplus \iota(\lambda(A_2^{q_2})) \oplus \iota(\lambda(A_3^{q_3}))$. But we can rewrite this as $\iota(\lambda(A_1^{q_1} A_2^{q_2} A_3^{q_3}))$! Next, $A_1^{q_1} A_2^{q_2} A_3^{q_3}$ is $X \otimes X \otimes X$ for input 00, $X \otimes Y \otimes Y$ for input 01, $Y \otimes X \otimes Y$

for input 10 and $Y \otimes Y \otimes X$ for input 11. The resource state is an eigenstate of each of these observables, with respective eigenvalues 1, -1, -1 and -1, and only a valuation that assigns these values can be obtained as a measurement outcome. After applying ι, those are precisely the outputs of the OR operation. A valuation of $S''_{\mathbf{i}}$, gained by measuring the resource state, always assigns the appropriate eigenvalue to $A_1^{q_1} A_2^{q_2} A_3^{q_3}$. We conclude that the above ℓ2-MBQC works as desired.

In general, for any ℓ2-MBQC, $\mathbf{q}$ determines a context to be valuated, and each row of R determines an observable for that context, the value of which is one of the elements in the output vector (after applying ι). This elegant correspondence is thanks to the linearity of the side processing and other conditions for ℓ2-MBQC. The resource state and the ways in which we can 'arrive' at each context (restricted by the matrices Q and T) limit the 'accessible' valuations. In the OR gate example, the context corresponding to input 00 has eight valuations, but four are not compatible with the resource state, and only the other four are accessible. Furthermore, $q = \{ 0, 0, 1 \}$ is not in the range of $T\mathbf{s} + Q\mathbf{i} \pmod 2$, so the context containing $X \otimes X \otimes Y$ has no accessible valuations at all.

In Chapter 5, we will see that we can collect the accessible valuations of an ℓ2-MBQC in something called a presheaf. The logic that the topos of all presheaves (on a certain poset) supplies, allows us, among other things, to formulate the conditions under which the ℓ2-MBQC is deterministic.

3.4 No common eigenstates

Before we get to topos theory, we need to wrap up one thing. We added a custom restriction to ℓ2-MBQC: that the two observables of each qubit cannot share any eigenstates. This will turn out to be an essential assumption later on, but we have to prove that it does not impede computational power.

Let an ℓ2-MBQC be given, but with the assumption dropped. Suppose that $O_k(0)$ and $O_k(1)$ share an eigenstate. There is only one state that is orthogonal to this eigenstate. This second state must therefore be the other eigenstate of both observables. And since they are non-degenerate and their eigenvalues are in $\{ 1, -1 \}$, we must have that $O_k(0) = \pm O_k(1)$. If $O_k(0) = O_k(1)$, then no harm is done if we only ever measure $O_k(0)$ and replace $O_k(1)$ by an arbitrary observable. If $O_k(0) = -O_k(1)$, then both observables still have the same effect on the ensemble state of the qubits. Measuring $O_k(1)$ instead of $O_k(0)$ is the same as measuring $O_k(0)$ and inverting all the output bits that depend on s_k. But inversion can be achieved by adding a constant 1, modulo 2.

We accomplish this by appending two qubits $d+1$ and $d+2$ to the ensemble. They start in the state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ (or any other maximally entangled state). Choose $O_{d+1}(0)$ and $O_{d+1}(1)$ arbitrarily but sharing no eigenstates. Set $O_{d+2}(0) = O_{d+1}(0)$ and $O_{d+2}(1) = -O_{d+1}(1)$. The rows in T and Q for q_{d+1} and q_{d+2} are the same as q_k used to have, but we set the rows corresponding to q_k to zero. Copy the row belonging to s_k in R for s_{d+1} and s_{d+2}. If $q_{d+1} = 0$, then we measure either twice 0 or twice 1 (after applying ι), and their sum modulo 2 is 0, so nothing is changed. If $q_{d+1} = 1$, then the measurement outcomes are opposite, yielding a constant 1, and an inversion in each output that depends on s_k, so that we have the same behaviour as before. If we repeat this protocol for each pair of observables that violates the assumption, we obtain an equivalent ℓ2-MBQC that does satisfy the complete definition.

Chapter 4

Topos theory

4.1 Category theory

This section is based on [15].

Definition 4.1. A *category* is a collection of *objects* and *arrows* (also called *morphisms*). Every arrow f has an object a as its *domain* and an object b (possibly the same one) as its *codomain*, which we denote as $f\colon a \to b$. There is a special arrow $1_a\colon a \to a$ for each object a, which we call the identity. Finally, a composition $g \circ f\colon a \to c$ must be defined for each pair of compatible arrows $f\colon a \to b$ and $f\colon b \to c$. The identities and composition must satisfy the following:

1. Associativity: $f \circ (g \circ h) = (f \circ g) \circ h$ for all arrows of the form $f\colon a \to b$, $g\colon b \to c$ and $h\colon c \to d$.

2. Identity: $1_b \circ f = f$ and $g \circ 1_b = g$ for all objects b and arrows $f\colon a \to b$ and $g\colon b \to c$.

Any category can be imagined as a special directed multigraph. The nodes are objects and there can be multiple directed arrows between two objects.

Example 4.2. The universe of sets form a category **Set**. In it, objects are sets and arrows are functions. The domain and codomain of an arrow are the obvious objects. The identity arrow is the identity function on a set, and the composition of arrows is simply the composition of functions. It is readily verified that the axioms are satisfied.

Example 4.3. We can construct the category **Hilb** of all finite dimensional Hilbert spaces. Its objects are finite dimensional Hilbert spaces and its arrows are linear transformations. $1_{\mathcal{H}}$ is the identity operator on $\mathcal{H}$, and the composition of arrows is again simply the composition of linear transformations, satisfying the axioms.

Example 4.4. A poset P (see Definition 2.5) can be made into a category. The objects of the category are the elements of P. For every $p, q \in P$, create one arrow $p \to q$ if $p \leq q$ (we shall sometimes designate such an arrow simply by "$p \leq q$"). For each $p \in P$, $p \leq p$, so let the identity arrow 1_p be the only arrow $p \to p$. If $f\colon p \to q$ and $g\colon q \to r$ are arrows, then $p \leq q$ and $q \leq r$, so by transitivity, $p \leq r$: we choose $g \circ f\colon p \to r$ to be the arrow corresponding to the relation $p \leq r$. Again, the axioms are satisfied.

Definition 4.5. An arrow $m\colon a \to b$ in a category $\mathcal{C}$ is called *monic* if it is left cancellable: for any two arrows $f_1, f_2\colon d \to a$, we have that $m \circ f_1 = m \circ f_2$ if and only if $f_1 = f_2$.

Example 4.6. Identity arrows are always monic. In **Set**, an arrow is monic if and only if it is injective as a function. In a poset category, every arrow is a monic. In fact, there can never be two distinct parallel arrows $a \to b$ in such a category.

Definition 4.7. Two objects a and b of a category $\mathcal{C}$ are called *isomorphic* if there exist two arrows $f\colon a \to b$ and $g\colon b \to a$ such that $g \circ f = 1_a$ and $f \circ g = 1_b$. In that case we write $a \cong b$ and call f and g *isomorphisms.*

Definition 4.8. Given two categories $\mathcal{C}$ and $\mathcal{D}$, a *functor* $T\colon C \to D$ is a pair of mappings, one on objects and one on arrows. For every object a of $\mathcal{C}$, it gives an object $T(a) = Ta$ of $\mathcal{D}$, and for every arrow $f\colon a \to b$ of $\mathcal{C}$, it gives an arrow $T(f) = Tf\colon Ta \to Tb$ of $\mathcal{D}$. Furthermore, it must preserve identities and compositions:

$$T(1_a) = 1_{Ta}, \quad T(g \circ f) = Tg \circ Tf$$

for all objects a and arrows $f\colon b \to c$ and $g\colon c \to d$ of $\mathcal{C}$.

A functor $T\colon \mathcal{C} \to \mathcal{D}$ gives a sort of image of $\mathcal{C}$ in $\mathcal{D}$, although some objects could merge (indeed, one could define a notion of injectivity for functors).

Example 4.9. We can define a “forgetful” functor $F\colon$ **Hilb** $\to$ **Set**, which sends a Hilbert space to its set of vectors (forgetting all vector space structure etc.) and a linear transformation to itself, seen as just a function. Clearly, (co)domains, identities and compositions are preserved this way.

Definition 4.10. A *contravariant functor* $T\colon \mathcal{C} \to \mathcal{D}$ is similar to a normal functor, but it differs in that it reverses arrow directions. So for every arrow $f\colon a \to b$ of $\mathcal{C}$, it gives an arrow $Tf\colon Tb \to Ta$ of $\mathcal{D}$. For compatibility, it must also reverse compositions:

$$T(g \circ f) = Tf \circ Tg$$

for all arrows $f\colon b \to c$ and $g\colon c \to d$ of $\mathcal{C}$.

To distinguish normal functors from contravariant functors, they are sometimes called *covariant functors.*

Definition 4.11. A *presheaf* on a poset P is a contravariant functor $X\colon P \to$ **Set**, where P is regarded as a category. We call the sets Xp (for each $p \in P$) the component sets, or simply the components, of X. We sometimes denote the arrows $X(p \leq q)\colon Xq \to Xp$ by X_{pq}.

Example 4.12. There are many presheaves on a poset. Consider for example the poset P_3 with three elements $p \leq q \leq r$. A presheaf $X\colon P_3 \to$ **Set** picks out three sets, Xp, Xq and Xr, three functions $X_{pq}\colon Xq \to Xp$, $X_{qr}\colon Xr \to Xq$ and $X_{pr}\colon Xr \to Xp$ that compose as $X_{pr} = X_{pq} \circ X_{qr}$, and of course the identity functions on the sets. Conversely, *any* two functions $f\colon A \to B$ and $g\colon B \to C$ can be made into a presheaf $X\colon P_3 \to$ **Set**:

- $Xp = C$, $Xq = B$, $Xr = A$
- $X_{pq} = g$, $X_{qr} = f$
- $X_{pr} = g \circ f$
- $X(1_p)$ is the identity function on C, etc.

Because of the shape of P, in this case, it would not have mattered much if we considered *covariant* functors instead. Even though the reversions are confusing, the *contravariant* functors will be more useful in our application later on.

Definition 4.13. Let $S, T \colon \mathcal{C} \to \mathcal{D}$ be two contravariant functors. A *natural transformation* $\tau \colon S \to T$ is a mapping that sends each object c of $\mathcal{C}$ to an arrow $\tau_c \colon Sc \to Tc$ of $\mathcal{D}$, such that

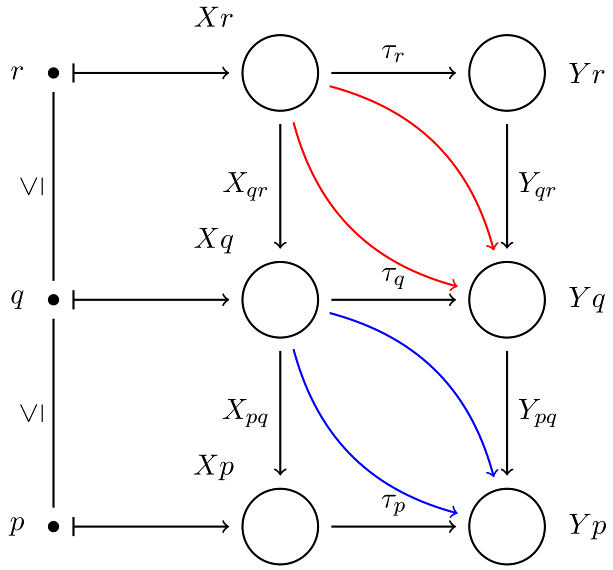
$$(Tf) \circ \tau_c = \tau_d \circ (Sf) \tag{4.1}$$

for every arrow $f \colon d \to c$ of $\mathcal{C}$. We call τ_c a *component* of τ.

Earlier we have said that a (covariant) functor $S \colon \mathcal{C} \to \mathcal{D}$ gives a sort of image of $\mathcal{C}$ in $\mathcal{D}$. A contravariant functor does the same, but reverses the arrows. A natural transformation transforms one such image into another. But the images given by S and T do not need to have the exact same shape.

Normally, a natural transformation is defined for covariant functors first, but for the sake of brevity, we restrict our attention to the contravariant version.

Example 4.14. Let X and Y be two presheaves of the three element poset P_3 defined in Example 4.12. A natural transformation $\tau \colon X \to Y$ can be depicted like in the following figure.



Condition 4.1 of Definition 4.13 says that the composition of functions along paths of same colour must yield the same result. The figure is not complete. For example, X_{pr} and Y_{pr} are missing, together with the condition $\tau_p \circ X_{pr} = Y_{pr} \circ \tau_r$.

4.2 The topos of presheaves

A topos is a category that is much like **Set**. For example, in **Set**, we could identify a product set $A \times B$ by only looking at the arrows between $A \times B$, A and B. We could test this categorical description of the product in other categories. If a category $\mathcal{C}$ has an object c_{ab} for each pair of objects a and b that satisfies this description, we say that $\mathcal{C}$ has products and define $a \times b = c_{ab}$. We will see the formal definition of products on page 19.

Of course, **Set** is a topos itself. We will not define completely what a topos is. It would take many pages and still be hard to grasp. Rather, we consider a special type of topoi, and exhibit only the features we will need in the next chapter.

Definition 4.15. Let P be a poset. The category $\widehat{P}$ of presheaves on the poset P has as objects all presheaves on P and as arrows all natural transformations between them. If S is a presheaf, the identity natural transformation 1_S sends $p \in P$ to 1_p. Clearly $(Sf) \circ 1_p = Sf = 1_q \circ (Sf)$ for every object p and arrow $f \colon q \to p$ of P, so this is indeed a natural transformation. Composition of natural transformations is done componentwise. If $\rho \colon R \to S$ and $\tau \colon S \to T$ are natural transformations, then for any arrow $f \colon q \to p$ of P,

$$\begin{aligned}(Tf) \circ (\tau_p \circ \rho_p) &= ((Tf) \circ \tau_p) \circ \rho_p = (\tau_q \circ (Sf)) \circ \rho_p \\ &= \tau_q \circ ((Sf) \circ \rho_p) = \tau_q \circ (\rho_q \circ (Rf)) \\ &= (\tau_q \circ \rho_q) \circ (Sf)\end{aligned}$$

so that condition 4.1 of Definition 4.13 is satisfied: the components $(\tau \circ \rho)_p = \tau_p \circ \rho_p$ make up a natural transformation. The composition on the whole is easily seen to be associative. Finally, the identity natural transformation 1_S satisfies $\tau \circ 1_S = \tau$ and $1_S \circ \rho = \rho$. We conclude that $\widehat{P}$ is indeed a category.

For the rest of this chapter, let P be any poset and $\widehat{P}$ its category of presheaves. It can be shown that $\widehat{P}$ is a topos. We will only show that $\widehat{P}$ has the following features:

- A terminal object 1, that is like the one element set $\{ * \}$.
- Product objects $a \times b$ and product arrows $\langle f, g \rangle$ that are like product sets and product functions.
- Subobjects, with operations $\cup$ and $\cap$, that are like subsets, unions and intersections.
- An object called the subobject classifier Ω, that is like the set of classical truth values $\{ 0, 1 \}$. An arrow $a \to \Omega$ specifies a subobject of a in a way similar to how a proposition $\pi(x)$ specifies a subset $\{ x \in A \mid \pi(x) \}$.

4.2.1 The terminal object

Definition 4.16. An object 1 in a category is called *terminal* if, for every object a, there is exactly one arrow $!_a \colon a \to 1$. An arrow $1 \to a$ is called a *global element*[1] of a.

Every topos has a terminal object 1. In **Set**, the singleton set $\{ * \}$ is terminal. For any set A, there is only one function to $\{ * \}$. On the other hand, there are $|A|$ functions from $\{ * \}$ to A, i.e. global elements of A. Each function selects one element from the set A!

Definition 4.17. In $\widehat{P}$, the presheaf 1 is defined as $1p = \{ * \}$ on objects $p \in P$ and as $1_{pq} \colon * \mapsto *$ on morphisms $p \leq q$.

Proposition 4.18. 1 *is terminal in* $\widehat{P}$.

Proof. Let T be any presheaf on P. We define the natural transformation $\tau \colon T \to 1$. It sends p to the unique function $\tau_p \colon Xp \to 1p = \{ * \}$ (and we immediately see that τ would be the only possible natural transformation). Evidently, $(1f) \circ \tau_p = \tau_q \circ (Tf)$ for any arrow $q \leq p$, since the only outputs of those functions are $*$. So τ is indeed a natural transformation, and it is unique. Since there is exactly one arrow $1 \to T$ for object T of $\widehat{P}$, 1 is terminal. □

Interestingly enough, unlike in **Set**, not every object of $\widehat{P}$ needs to have global elements.

[1] It is called a *global* element because of its correspondence to global sections in sheaf theory, from which topos theory stems historically.

Example 4.19. Suppose that P has three elements and is ordered as $r \geq p \leq s$. Let X be the presheaf defined on objects as $Xr = \{ u \}$, $Xs = \{ v \}$ and $Xp = \{ u, v \}$ and on arrows as $X_{pr} \colon u \mapsto u$ and $X_{ps} \colon v \mapsto v$. Then X has no global element. Suppose that $\tau \colon 1 \to X$ is a natural transformation. Then $1r$ must select u (i.e. $\tau_r \colon * \mapsto u$) and $1s$ must select v. If $1p$ selects u, then $\tau_p \circ (1_{ps}) \colon * \to u$ but $(X_{ps}) \circ \tau_s \colon * \to v$, so in that case, τ cannot be a natural transformation. It goes similarly goes wrong when $1p$ selects v. We conclude that X has no global elements.

Like many aspects of a topos, a global element is defined after its counterpart in set theory. But global elements are much less important in topoi than in set theory. Nonetheless, we will soon see that certain global elements play the role of truth values.

4.2.2 Products

Definition 4.20. In any category $\mathcal{C}$, we say that an object $a \times b$ is the product of objects a and b if there exists arrows $\pi \colon c \to a$ and $\rho \colon c \to b$ (called the projections) such that for any two arrows $f \colon c \to a$ and $g \colon c \to b$, there exists a unique arrow $\langle f, g \rangle \colon c \to a \times b$ such that $f = \pi \circ \langle f, g \rangle$ and $g = \rho \circ \langle f, g \rangle$.

Every topos has a product for every pair of objects. In **Set**, the ordinary Cartesian product $A \times B$ is a categorical product of the sets A and B.

Proposition 4.21. *$\widehat{P}$ has a product $X \times Y$ for each pair of objects X and Y.*

Proof. We write Z instead of $X \times Y$. We define the product componentwise: $Zp = Xp \times Yp$ (the Cartesian product) and $Z_{pq} = \langle X_{pq}, Y_{pq} \rangle \colon Xq \times Yq \to Xp \times Yp$ (the ordinary pair of functions). Next, we define the projections. The natural transformation $\pi \colon Z \to X$ is given by its components

$$\begin{aligned} \pi_p \colon Zp = Xp \times Yp &\to Xp \\ \langle x, y \rangle &\mapsto x \end{aligned}$$

It is not hard to see that this is a natural transformation. The other projection $\rho \colon Z \to Y$ is defined similarly.

Now suppose that $\sigma \colon W \to X$ and $\tau \colon W \to Y$ are natural transformations. We define $\langle \sigma, \tau \rangle \colon W \to Z$ componentwise too:

$$\langle \sigma, \tau \rangle_p = \langle \sigma_p, \tau_p \rangle$$

(recall that $\sigma_p \colon Wp \to Xp$ and $\sigma_p \colon Wp \to Yp$ are simply functions in **Set**; we are again using pairing of functions). Certainly $\pi_p \circ \langle \sigma, \tau \rangle_p = \pi_p \circ \langle \sigma_p, \tau_p \rangle = \sigma_p$ for each $p \in P$, so $\sigma = \pi \circ \langle \sigma, \tau \rangle$. Similarly, $\tau = \rho \circ \langle \sigma, \tau \rangle$. Moreover, no other definition of $\langle \sigma, \tau \rangle$ could satisfy this: it is unique. We conclude that Z is a product of X and Y. □

In $\widehat{P}$, the components of $1 \times X$ are $(1 \times X)_p = \{ * \} \times Xp = \{ \langle *, p \rangle \mid x \in Xp \}$. There is a natural transformation $\tau \colon X \to 1 \times X$ with components $\tau_p \colon x \mapsto \langle *, x \rangle$, with an evident inverse, so that X and $1 \otimes X$ are isomorphic: 1 is a unit for the product. It can also be shown that the product is associative up to isomorphisms, i.e. $X_1 \times (X_2 \times X_3) \cong (X_1 \times X_2) \times X_3$ so that it makes sense to define arbitrary finite products $X_1 \times \cdots \times X_n$. It will be useful to define the empty product as 1.

4.2.3 Subobjects

Recall that a monic arrow is left cancellable and coincides with the notion of injection in **Set**. An injection $f\colon A \to B$ specifies a subset of B, namely $f[A]$, the range of f. Conversely, if $A \subseteq B$, then the inclusion function $f\colon A \to B, \quad x \mapsto x$ is injective. We can identify a subset by the equivalence class of corresponding injections, and do the same for subobjects and monic arrows.

Definition 4.22. In any category $\mathcal{C}$, we call two monic arrows $m\colon a \to d$ and $n\colon b \to d$ *isomorphic* if there exists an isomorphism $f\colon a \to b$ such that $m = n \circ f$.

A *subobject* of d is an isomorphism class of monic arrows with codomain d. (By an isomorphism class we mean an equivalence class for the equivalence relation "m is isomorphic to n".)

We shall often represent a subobject by a single monic arrow. If $f\colon a \to d$ and $g\colon b \to d$ are both monic arrows, we write $f \subseteq g$ if and only if there exists an arrow $k\colon a \to b$ such that $f = g \circ k$.

Example 4.23. In $\widehat{P}$, the 'range' of a monic arrow $\tau\colon Y \to X$ actually determines a special presheaf. Suppose that τ is a monic arrow: $\tau \circ \sigma_1 = \tau \circ \sigma_2$ always implies $\sigma_1 = \sigma_2$. This is only possible if all of the components of τ are injections. We define the presheaf Z by $Zp = \tau_p[Yp]$ and $Z_{pq} = X_{pq}|_{Zq}$, the restriction of the function X_{pq} to the domain Zq. We need to verify that Z_{pq} takes Zq into Zp, otherwise Zp cannot be the (categorical) codomain of Z_{pq}. $Z_{pq}[Zq] = (Z_{pq} \circ \tau_q)[Yq]$ since τ_q is a bijection between Yq and Zq. But $Z_{pq} \circ \tau_q = \tau_p \circ Y_{pq}$ by naturality of τ. Therefore $Z_{pq}[Zq] = (\tau_p \circ Y_{pq})[Yq] \subseteq \tau_p[Yp]$. So X_{pq} takes Zq into Zp and we conclude that Z is indeed a presheaf.

Conversely, any presheaf Z with $Zp \subseteq Xp$ and $Z_{pq} = X_{pq}|_{Zq}$ determines a monic arrow $\tau\colon Z \to X$, which we call the inclusion arrow. τ_p is the inclusion function of Zp in Xp. By injectivity, $X_{pq} \circ \tau_q = \tau_p \circ Z_{pq}$ so τ is indeed a natural transformation. τ in turn determines an isomorphism class of monic arrows, that is, a subobject of X.

We call a presheaf Z like in this example a *subpresheaf* of X and write $Z \subseteq X$. We shall use this more intuitive representation of a subobject often. However, the subpresheaf Z constructed from a monic arrow $Y \to X$ can in no way be distinguished from Y by arrows alone. The category sees no difference between them; it does not understand that the elements that occur somewhere in Z also occur in X. It is only from our external perspective that we think of Z as more canonical than Y.

Definition 4.24. We define the operations $\cup$ and $\cap$ on subobjects in $\widehat{P}$. If we represent two subobjects of X as subpresheaves of X, then $Y \cup Z$ is defined by $(Y \cup Z)p = Yp \cup Zp$ and $(Y \cup Z)_{pq} = X_{pq}|_{(Y \cup Z)q}$. Like before, $Y \cup Z \subseteq X$ is a presheaf and we can convert it back to a subobject. The definition of $Y \cap Z$ is similar.

4.2.4 Subobject classifier

We have seen that in **Set** we can represent a subset $A \subseteq D$ by a monic arrow (an injection). We can represent it in another way, namely by the characteristic function χ_A of A: $\chi_A(x) = 1$ if $X \in A$ and $\chi_A(x) = 0$ if $X \notin A$. This function is of course also an arrow $\chi_A\colon D \to \{\, 0, 1 \,\}$ in **Set**. We can interpret $\chi_A(x)$ as a proposition, which is true if it gets value 1 and false if it gets value 0. In that case we can write $A = \{\, x \in D \mid \chi_A(x) \,\}$. We call $\Omega = \{\, 0, 1 \,\}$ the set of truth values.

As propositions, characteristic arrows have logical operators like "$\wedge$", "and", and "$\Rightarrow$", "implies". If $B \subseteq D$ as well, then $\{\, x \in D \mid \chi_A(x) \wedge \chi_B(x) \,\} = \{\, x \in D \mid \chi_A(x) \,\} \cap \{\, x \in D \mid \chi_B(x) \,\}$.

Moreover, $A \subseteq B$ if and only if $\chi_A(x) \Rightarrow \chi_B(x)$ has value 1 for all $x \in D$. These operators are themselves arrows $\wedge, \Rightarrow \colon \Omega \times \Omega \to \Omega$ in **Set**.

In a topos, we can do something similar, and in particular in $\widehat{P}$. We will only describe this and not give explicit definitions. In any topos, there is a *truth value object* Ω, such that to every monic arrow $f \colon Z \to X$ corresponds a certain special characteristic arrow $\chi_f \colon X \to \Omega$. $\widehat{P}$ has an arrow $\wedge \colon \Omega \times \Omega \to \Omega$ such that (if $g \colon Y \to X$ is another monic arrow) the character of $f \cap g$ (as defined in Definition 4.24) is $\chi_{f \cap g} = \wedge \circ \langle \chi_f, \chi_g \rangle$, which we will abbreviate as $\chi_f \wedge \chi_g$. Similarly, there is an operator $\vee$, "or", that corresponds to $\cup$.

In any topos, Ω also has a special global element $\top \colon 1 \to \Omega$, which we call the *truth arrow.* Together, Ω and $\top$ make up the *subobject classifier.* In **Set**, $\top$ is the function $* \mapsto 1$. In $\widehat{P}$, we call an arrow $\chi \colon X \to \Omega$ valid if it "factors through" $\top$: if $\chi = \top \circ !_X$, where $!_X$ is the unique arrow $X \to 1$. Finally, $\widehat{P}$ contains an arrow $\Rightarrow \colon \Omega \times \Omega \to \Omega$, for which it holds that $\Rightarrow \circ \langle \chi_f, \chi_g \rangle$ is valid if and only if $f \subseteq g$. Again, we write $\chi_f \Rightarrow \chi_g$ instead of $\Rightarrow \circ \langle \chi_f, \chi_r \rangle$.

We have tried to give an intuitive description of the subobject classifier. We hope the idea is clear: we can represent subobjects either as monic arrows, subpreheaves or characteristic arrows, between which we can switch freely, and there are corresponding operations and relations in each domain. Subpresheaves will be the easiest to use for explicit constructions in the next chapter. However, using the characteristic arrows, we will be able to create formulas in a formal language.

We have chosen not to give a formal definition of the subobject classifier, nor its explicit form in $\widehat{P}$. They are too lengthy to exhibit here can be found in standard literature on topoi, for example [16] or [9].

4.3 Internal logic of a topos

Now that we have a truth value object and logical operators, we are going to use them. First, we will inspect the structure of the collection of global elements of the subobject classifier. In the second part of this section, we will glimpse at a formal language in which we can express internal propositions of a topos.

4.3.1 Truth values

We have seen that the truth value object Ω of a topos has logical operators and a global element $\top$. It has another global element, $\bot$, which takes the role of falsehood. There may be more global elements. We call the global elements of Ω truth values. The truth values can be partially ordered. For two truth values $f, g \colon 1 \to \Omega$ we define: $f \leq g$ if and only if $f \wedge g = f$. Under this ordering, the global elements of Ω constitute a Heyting algebra:

Definition 4.25. A *Heyting algebra* **HA** is a lattice (see Definition 2.7) with a greatest element $\top$, a least element $\bot$, and another operation $\Rightarrow$ called the *relative pseudo-complementation* that satisfies

$$(x \wedge a) \leq b \text{ if and only if } x \leq (a \Rightarrow b) \tag{4.2}$$

for all $x, a, b \in \mathbf{HA}$.

$\top$ being the greatest element means that for every $x \in \mathbf{HA}$, $x \leq \top$. The least element is similarly defined.

Proposition 4.26. *For any topos, the set of truth values of Ω under the relation $\leq$ form a Heyting algebra, with the operations as given.*

We call this Heyting algebra $\Gamma\Omega$. For a proof, we again refer to [16] and [9]. For any Heyting algebra **HA**, we can define a *pseudo-complement* $\neg x$ of x as $x \Rightarrow \bot$. A Heyting algebra then satisfies many of the familiar tautologies of classical propositional logic, but not necessarily all of them. Most notoriously, the law of excluded middle does not always obtain: it might be that $x \vee \neg x \neq \top$. This is why we call it a *pseudo*-complement. The formulas that are true in every Heyting algebra can be axiomatised. The result is *intuitionistic logic*.

Even though we have not given Ω explicitly for $\widehat{P}$, its Heyting algebra is not too difficult to describe. A truth value is an arrow $f\colon 1 \to \Omega$. But by definition of the subobject classifier, this must correspond to a monic arrow $g\colon X \to 1$ as $f = \chi_g$. A monic arrow in $\widehat{P}$ is a natural transformation with injective component functions. But the component sets of 1 are simply $\{\,*\,\}$. An injective function to $\{\,*\,\}$ can have an empty domain[2] or a domain with just one element. So the component sets of X must be empty or singleton. However, a function cannot have a nonempty domain and an empty codomain. So if $p \leq q$ in P, and $Xq \neq \emptyset$, then it must be that $Xp \neq \emptyset$, since there is a function $X_{pq}\colon Xq \to Xp$. We see that X defines a lower set A of P, where $p \in A$ if and only if $Xp \neq \emptyset$:

Definition 4.27. A subset A of a poset P is called a *lower set* of P if for every $p \in A$ and $q \in P$ with $q \leq p$, also $q \in A$. The set of all lower sets of P is denoted by $\downarrow\!P$.

If $f\colon a \to 1$ and $g\colon b \to 1$ are monic arrows and if $f \subseteq g$, then the lower set defined by f is a subset of the lower set defined by g, and conversely. So $\downarrow\!P$ ordered by inclusion has the same partial order as the Heyting algebra of the global elements of Ω. In it, $\top = P$, $\bot = \emptyset$, $A \vee B = A \cup B$ and $A \wedge B = A \cap B$. $A \Rightarrow B$ is more complicated. If $X, A, B \subseteq P$ were arbitrary sets, then $X \cap A \subseteq B$ if and only if $X \subseteq (P \setminus A) \cup B$. But this latter set might not be a lower set, so instead, $A \Rightarrow B$ is the largest lower subset of $(P \setminus A) \cup B$. This satisfies equation 4.2 in Definition 4.25.

In the next chapter, we deal a few times with presheaves Z of which all functions Z_{pq} are surjective. In this special situation of presheaves with surjective functions, we can understand what a lower set of P means as a truth value for $\widehat{P}$. So suppose that a presheaf X has two subpresheaves Y and Z that solely have surjective functions. We can wonder whether $Y \subseteq Z$. Now, assume that $p \leq q$ in P and $Yq \subseteq Zq$. $Yp = Y_{pq}[Yq] = X_{pq}[Yq]$ since $Y_{pq}\colon Yq \to Yp$ is surjective and a restriction of X_{pq}. Similarly, $Zp = X_{pq}[Zq]$. Since $Yq \subseteq Zq$, it necessarily follows that $Yp \subseteq Zp$. So the elements p of P for which $Yp \subseteq Zp$ form a lower set of P, and this lower set corresponds to a truth value of Ω. In other words, the proposition "$Y \subseteq Z$" gets a truth value in Ω. This idea, however, does not obtain for general presheaves.

4.3.2 A formal language

A *formal language* is a collection of symbols and a prescription of how to create well-formed terms and formulas from these symbols. A certain rich formal language, called the *Mitchell-Benabou language* (after its creators), can be constructed for a given topos $\mathcal{T}$. The topos $\mathcal{T}$ is an *interpretation* for this language: each symbol of the language has as its interpretation an arrow of $\mathcal{T}$. Moreover, intuitionistic tautologies can be formulated in this language, which are all true when interpreted in $\mathcal{T}$, so that we can use intuitionistic deductions.

In ordinary mathematics, we often use the variables n and x, and think of them as corresponding to the sets $\mathbb{N}$ and $\mathbb{R}$ respectively. We could say that n is of type $\mathbb{N}$ and that x is of type $\mathbb{R}$. In the Mitchell-Benabou language, this notion of types is made more explicit. Each term of the language has a type. We do not need the full strength of the Mitchell-Benabou language, whose definition can be found in [16]. Instead, we define a simpler language $\mathcal{L}(\mathcal{T})$ based on it.

[2] A function $h\colon A \to B$ is a special subset of $A \times B$. The empty subset of the empty product $\emptyset \times B$ is a function too!

Definition 4.28. For a given topos $\mathcal{T}$, we define what the terms of the language $\mathcal{L}(\mathcal{T})$ are. Every term has a type X, which is an object of $\mathcal{T}$, and an interpretation, which is an arrow with codomain X. The terms of $\mathcal{L}(\mathcal{T})$ are those that can be obtained by using the following rules.

1. For every object X of $\mathcal{T}$ there are symbols $x_1, x_2, \ldots$ which we call the *variables of type* X. Any variable of type X is also a term of type X. Its interpretation is the identity function $1_X \colon X \to X$.

2. If $f \colon X \to Y$ is an arrow of $\mathcal{T}$ and σ is a term of type X, with interpretation $\sigma \colon U \to X$, then $f\sigma$ is a term of type Y. Its interpretation is the arrow $f \circ \sigma \colon U \to Y$.

3. If σ is a term of type X and τ is a term of type Y, with interpretations $\sigma \colon U \to X$ and $\tau \colon V \to Y$, then $\langle \sigma, \tau \rangle$ is a term of type $X \times Y$, with interpretation $\langle \sigma, \tau \rangle \colon U \times V \to X \times Y$.

If σ is a term of type Ω, we call it a *formula.* It is *true* for the topos $\mathcal{T}$ if its interpretation $\sigma \colon X \to \Omega$ factors through $\top$: $\sigma = \top \circ !_X$, where $!_X$ is again the unique arrow $X \to 1$.

If σ and τ are formulas, then $\wedge\langle \sigma, \tau \rangle$ is also a formula, since $\wedge$ is an arrow $\Omega \times \Omega \to \Omega$. We shall abbreviate this formula as $\sigma \wedge \tau$, and similarly for the other logical operators.

We have seen before that, for two subobjects f and g of a presheaf X in $\widehat{P}$, $f \subseteq g$ if and only if the arrow $\chi_f \Rightarrow \chi_g$ is valid. We can convert this latter arrow into a formula of $\mathcal{L}(\widehat{P})$. If x is a variable of type X, then the formula $\chi_f x \Rightarrow \chi_g x$ is a term of type Ω of the language $\mathcal{L}(\widehat{P})$. Its interpretation is $\Rightarrow \circ \langle \chi_f \circ 1_X, \chi_g \circ 1_X \rangle = \chi_f \Rightarrow \chi_g$. So the formula $\chi_f x \Rightarrow \chi_g x$ is true if and only if the arrow $\chi_f \Rightarrow \chi_g$ is valid. For clarity, we will use $\chi_f(x)$ as a term instead of $\chi_f x$

The full Mitchell-Benabou language also has quantifiers $\forall$, $\exists$, relations $=$ and $\in$ and a sort of function evaluation, which all have interpretations similar to their familiar meanings. These interpretations are however much harder to define, and we will not be needing them, which is why they were omitted.

Chapter 5

The topos of an ℓ2-MBQC

This chapter is the core of this report. We will show that the fact that an ℓ2-MBQC 'works' can be expressed within a certain topos related to the ℓ2-MBQC. In doing this, we closely follow [14], but we will have some criticism as well.

5.1 The topos $\widehat{\mathcal{W}(\mathcal{H})}$

In Chapter 3 it has been suggested that we could understand an ℓ2-MBQC better by looking at the relevant contexts and valuations. First, we define $\mathcal{W}(\mathcal{H})$, a subposet of the poset of contexts $\mathcal{V}(\mathcal{H})$. We take the idea from [14], but our definition will be a bit more general.

Definition 5.1. Let an ℓ2-MBQC be given. We define

$$\mathcal{Q} = \{\, T\mathbf{s} + Q\mathbf{i} \pmod 2 \mid \mathbf{s} \in \{\, 0, 1\,\}^d, \quad \mathbf{i} \in \{\, 0, 1\,\}^n \,\}.$$

For the labelling $\mathbf{a} \in \mathcal{Q}$ of any choice of observables, we set $S_{\mathbf{a}} = \{\, A_1^{a_1}, \ldots, A_d^{a_k} \,\}$.

Definition 5.2. For a given ℓ2-MBQC, we define $\mathcal{W}(\mathcal{H})$, a subposet of $\mathcal{V}(\mathcal{H})$, as follows. Let $\mathcal{S} = \{\, S_{\mathbf{a}} \mid \mathbf{a} \in \mathcal{Q}\,\}$. $\mathcal{W}(\mathcal{H})_0$ is the poset generated by taking all possible intersections of elements in $\mathcal{S}$, excluding the empty set, and ordering by inclusion. $\mathcal{W}(\mathcal{H})$ is the poset gained by replacing each element S of $\mathcal{W}(\mathcal{H})_0$ by its bicommutant S'' and ordering by inclusion.

Every $S_{\mathbf{a}}$ determines a final context $S''_{\mathbf{a}}$ of the ℓ2-MBQC. The intersections of the $S_{\mathbf{a}}$'s determine intermediate contexts, which are 'visited' as the observables are chosen and measured one by one.

If $A \subseteq B$, then an operator that commutes with all elements of B also commutes with all elements of A. Hence $B' \subseteq A'$ and therefore $A'' \subseteq B''$. By the definition of ℓ2-MBQC, $O_k(0)$ and $O_k(1)$ do not have the same eigenspaces, so $A'' \neq B''$ whenever A and B are distinct elements of $\mathcal{W}(\mathcal{H})_0$, and no merging occurs. Therefore $\mathcal{W}(\mathcal{H})$ has precisely the same order as $\mathcal{W}(\mathcal{H})_0$.

We see that we can construe $\mathcal{W}(\mathcal{H})$ as the poset of all contexts *relevant* to the computation. No observables will be measured other than those appearing somewhere in $\mathcal{W}(\mathcal{H})$. Strictly speaking, $\mathcal{W}(\mathcal{H})$ might still be too large. It is possible that not every outcome of measurements $\mathbf{s}$ is actually feasible for every input $\mathbf{i}$, and that therefore not every $\mathbf{a}$ in the range of $T\mathbf{s} + Q\mathbf{i}$ (mod 2) will be encountered. This (non)issue will be discussed later.

Example 5.3. We consider $\mathcal{W}(\mathcal{H})$ for the OR-gate of Example 3.6. For convenience, we write $X_1 = X \otimes I \otimes I$, $X_2 = I \otimes X \otimes I$, and so forth. Since $T = 0$, the contexts are determined only by the input and not by the intermediate measurement results. The following are all the elements of $\mathcal{S}$: $S_1 = \{ X_1, X_2, X_3 \}$, $S_2 = \{ X_1, Y_2, Y_3 \}$, $S_3 = \{ Y_1, X_2, Y_3 \}$ and $S_4 = \{ Y_1, Y_2, X_3 \}$. We see that their intersections are singletons (or the empty set). So let $V_i = S_i''$ and $V_{X_1} = \{ X_1 \}''$, etc. Then $\mathcal{W}(\mathcal{H})$ is given by the diagram in Figure 5.3. In it, a line connecting p and q, such that p lies lower than q, means $p \leq q$. This kind of diagrams for posets are called Hasse diagrams.

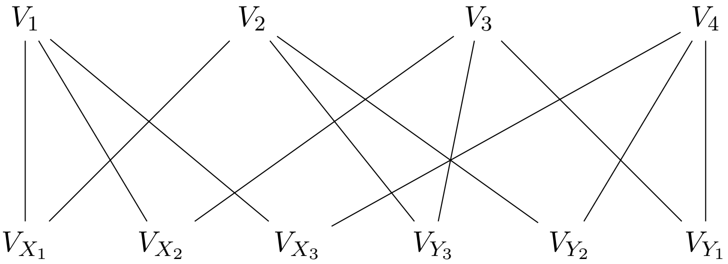


Figure 5.1: The poset $\mathcal{W}(\mathcal{H})$ of the OR-gate ℓ2-MBQC.

We can now consider the topos of presheaves on $\mathcal{W}(\mathcal{H})$, designated $\widehat{\mathcal{W}(\mathcal{H})}$. The poset $\mathcal{W}(\mathcal{H})$ of the OR-gate has only two layers, so in each presheaf, there are no compositions other than with the identity morphisms. This means that there are really no restrictions for a presheaf F; $F(U \subseteq V)$ can be any function between the arbitrary sets $F(V)$ and $F(U)$.

5.2 The spectral presheaf

We can structure the valuations of the contexts in $\mathcal{W}(\mathcal{H})$ neatly in a presheaf.

Definition 5.4. Given a poset of contexts $\mathcal{W}(\mathcal{H})$, the *spectral presheaf* $\Sigma\colon \mathcal{W}(\mathcal{H}) \to \mathbf{Set}$ is defined on objects by

$$\Sigma(V) = \{ \lambda\colon V \to \mathbb{C} \mid \lambda \text{ is a valuation of } V \}$$

and on morphisms by

$$\begin{aligned} \Sigma(U \subseteq V)\colon \Sigma(V) &\to \Sigma(U) \\ \lambda &\mapsto \lambda|_U, \end{aligned}$$

the restriction of λ to the domain U. It is easily seen that Σ satisfies the definition of a contravariant functor; namely that it inverts – but preserves – compositions:

$$\Sigma((V \subseteq W) \circ (U \subseteq V)) = \Sigma(U \subseteq V) \circ \Sigma(V \subseteq W)$$

Example 5.5. We consider what Σ looks like for the OR-gate ℓ2-MBQC. Using Proposition 2.12, we can identify the valuations of $V_1 = \{ X_1, X_2, X_3 \}''$ with the common eigenprojections of $\{ X_1, X_2, X_3 \}$. But X only has eigenstates $|+\rangle$ and $|-\rangle$. It readily follows that the common eigenprojections are those belonging to the states $|{+}{+}{+}\rangle$, $|{+}{+}{-}\rangle$, etc. Therefore V_1 has eight valuations, which we designate λ_{+++} (which gives X_1, X_2 and X_3 value 1), λ_{++-} (which gives X_3 value -1), etc.

Similarly, the eigenstates of Y are $|{\uparrow}\rangle$ (with value 1) and $|{\downarrow}\rangle$ (with value -1), so $V_2 = \{ X_1, Y_2, Y_3 \}''$ has common eigenstates like $|{+}{\uparrow}{\uparrow}\rangle$ and $|{-}{\uparrow}{\downarrow}\rangle$. Its valuations are $\lambda_{+\uparrow\uparrow}$, $\lambda_{+\uparrow\downarrow}$, etc. For $V_{X_1} = \{ X_1 \}''$ the situation is even simpler. The eigenprojections of X_1 are $|+\rangle\langle+| \otimes I \otimes I$ and $|-\rangle\langle-| \otimes I \otimes I$. The corresponding valuations of V_{X_1} are $\lambda_{+\cdot\cdot}$ and $\lambda_{-\cdot\cdot}$.

The picture is similar for the other contexts. For example, V_{Y_2} has valuations $\lambda_{\cdot\uparrow\cdot}$ and $\lambda_{\cdot\downarrow\cdot}$. The function $\Sigma(V_{X_1} \subseteq V_1)$ sends valuations of the form λ_{+**} to $\lambda_{+\cdot\cdot}$ and λ_{-**} to $\lambda_{-\cdot\cdot}$, where each '$*$' is '$+$' or '$-$'. The other functions work in a similar fashion.

Recall from Chapter 2 that a global valuation of $\mathcal{H}$ selects a valuation for each context in $\mathcal{V}(\mathcal{H})$, in such a way that the valuations do not contradict each other. We can straightforwardly extend this definition of a global valuation to any subposet of $\mathcal{V}(\mathcal{H})$. Now suppose that we have a global valuation of $\mathcal{W}(\mathcal{H})$. It selects for each $V \in \mathcal{W}(\mathcal{H})$ a valuation λ_V in $\Sigma(V)$. If $U \subseteq V$, then it must be that $\lambda_U = \lambda_V|_U$ (this is just the definition of a global valuation). Put differently, it must be that $\Sigma(U \subseteq V)(\lambda_V) = \lambda_U$. But this is precisely what a global element $1 \to \Sigma$ would do. Actually, Σ for the OR-gate ℓ2-MBQC does have global elements (even though the Hilbert space is contextual), because it is defined on too small a poset, or because it has too many valuations. For example, the valuations λ_{+++}, $\lambda_{+\uparrow\uparrow}$, $\lambda_{\uparrow+\uparrow}$ and $\lambda_{\uparrow\uparrow+}$ of the contexts V_1 through V_4 do not contradict each other, and, together with the corresponding valuations on the lower contexts, they make up a global element of Σ. Soon we shall see a subpresheaf of Σ that does not have a global element.

5.3 Intermezzo

The authors of [14] prove a few relations between properties of an ℓ2-MBQC and properties of the logic of the corresponding topos $\widehat{\mathcal{W}(\mathcal{H})}$. They suggest that one could go a bit further and show that the Mitchell-Benabou language contains formulas that, when interpreted in the topos, say something about the computation directly. In particular, they claim that "the Anders and Browne OR-gate takes the form of a theorem" within the language. We want to investigate this matter.

First we will have to address one pressing question: what could they possible mean by "the Anders and Browne OR-gate takes the form of a theorem"? Surely this hypothetical theorem must assert something provable (and hopefully meaningful) about the ℓ2-MBQC corresponding to the OR-gate. It seems that the only sensible things we can say about this ℓ2-MBQC are that it is deterministic and that it in fact computes the OR operation. But even these two assertions are not completely separable. The determinism of an ℓ2-MBQC largely depends on the output matrix R. For example, any ℓ2-MBQC with $R = 0$ is deterministic. Evidently, in proving determinism, we are working with the intended output.

And now it gets interesting: in [14], $\mathcal{W}(\mathcal{H})$ is only defined for temporally flat, *deterministic* ℓ2-MBQCs! What is the point of trying to prove determinism using a structure that only exists by virtue of that determinism? Of course, it may still provide insights, but in any case, our definition of $\mathcal{W}(\mathcal{H})$ applies to *any* ℓ2-MBQC. It can be shown that this definition coincides with that of [14] for a temporally flat, deterministic ℓ2-MBQC. Regardless whatever the original intention of the authors of [14] was, our goal will be to find, for any ℓ2-MBQC, a formula in the topos language that asserts that the ℓ2-MBQC is deterministic.

5.4 Propositions and pseudo-states

This section introduces the physics related notions to which the topos logic applies. The definitions in this section are based on [7] and [8], the only difference being that they are adapted for any subposet $\mathcal{W}(\mathcal{H})$ instead of all of $\mathcal{V}(\mathcal{H})$.

5.4.1 Quantum propositions

In physics, basic propositions are of the form "$A \in \Delta$", where A is a physical quantity and $\Delta \subseteq \mathbb{R}$. In a classical system in a certain state, such a proposition is either true of false. This is because every state specifies a particular value for every observable. For a quantum system, the situation is more complex. If the state ϕ is not an eigenstate of A (seen as an observable), we associate multiple (eigen)values with A for ϕ. If some of these values are in Δ, and others are not, then it makes no sense to say that "$A \in \Delta$" is either true or false. We want to quantify this partial truth, and we will do so, of course, using a topos. This is where the many truth values come in, but not in a way one would perhaps expect.

We can canonically associate a projection with a proposition "$A \in \Delta$":

Definition 5.6. Let $\mathcal{H}$ be finite dimensional, let $A \in B(\mathcal{H})$ be an observable and $\Delta \subseteq \mathbb{R}$. Write $A = \sum_i \lambda_i P_i$, with each P_i a projection. The *spectral projection* corresponding to the proposition "$A \in \Delta$" is defined as

$$E[A \in \Delta] = \sum \{ \, P_i \mid \lambda_i \in \sigma(A) \cap \Delta \, \} \, ,$$

where $\sigma(A)$ is the spectrum of eigenvalues of A.

So $E[A \in \Delta]$ projects into the subspace associated with the eigenvalues of A that are also in Δ. Upon measurement of A on a state ϕ, the probability for "$A \in \Delta$" to come out true is $\langle \phi | E[A \in \Delta] | \phi \rangle$. We see that $E[A \in \Delta]$ perfectly represents the proposition "$A \in \Delta$". If $E[A \in \Delta]$ gets value 1, then "$A \in \Delta$" is true, and if it gets value 0, "$A \in \Delta$" is false.

Conversely, any projection P corresponds to a proposition "$A \in \Delta$". Admittedly, there are infinitely many pairs $\langle B, \Gamma \rangle$ such that $P = E[B \in \Gamma]$, but semantically, they are equivalent. Compare for example the propositions (referring to some classical situation) "the system has frequency f" and "the system has period $\frac{1}{f}$". They seem different but in the end mean the same thing. The simplest proposition, then, corresponding to the projection P is "$P \in \{ \, 1 \, \}$".

5.4.2 Daseinisation

Suppose that we have measured (the observables in) a context V and are interested in a proposition $P = E[A \in \Delta] \notin V$. We cannot assign P a value without disrupting the valuation of V. We could however try to find a projection, related in some way to P, that *is* in V. One such projection is the following.

Definition 5.7. Given a context $V \in \mathcal{V}(\mathcal{H})$ and a projection $P \in B(\mathcal{H})$, the *outer daseinisation*[1] of P in V is the least projection in $\mathcal{P}(V)$ greater than P:

$$\delta^0_P(V) = \bigwedge \{ \, Q \in \mathcal{P}(V) \mid P \leq Q \, \} \, .$$

Here, $\leq$ is the order from the lattice of projections $\mathcal{P}B(\mathcal{H})$. Although we have not shown it, the meet operation of any lattice is associative and commutative, so this is well-defined.

The 'proposition' $\delta^0_P(V)$ is more general than P, in the sense that "$P \in \{ \, 1 \, \}$" implies "$\delta^0_P(V) \in \{ \, 1 \, \}$". $\delta^0_P(V)$ is often called a *coarse graining* of P. Note that in many cases $\delta^0_P(V)$ is the identity projection, which is not really useful because it is always 'true'. We get a better approximation of P if we consider δ^0_P for a poset of contexts. While we are at it, we represent a projection in a context by the valuations that assigns it the value 1 (or: the valuations that make it true!).

Definition 5.8. Given a poset of contexts $\mathcal{W}(\mathcal{H})$ and a projection $P \in B(\mathcal{H})$, we define the presheaf δ_P on objects by

$$\delta_P(V) = \{ \, \lambda \in \Sigma(V) \mid \lambda(\delta^0_P(V)) = 1 \, \} \, .$$

[1] This term, derived from "dasein", German for "to be there" and a buzzword of the philosopher Heidegger, was coined by the authors of [7] and refers to the concept of existence in philosophy. *Outer* daseinisation contrasts with *inner* daseinisation, which approximates the projection from below.

Its definition on morphisms is inherited from Σ. Suppose that $U, V \in \mathcal{W}(\mathcal{H})$ with $U \subseteq V$. We must have that $\delta^0_P(V) \leq \delta^0_P(U) \in V$, so if λ_V assigns $\delta^0_P(V)$ the value 1, then it assigns $\delta^0_P(U)$ the value 1, so its restriction $\Sigma(U \subseteq V)(\lambda_V)$ also assigns $\delta^0_P(U)$ the value 1. In other words, $\Sigma(U \subseteq V)$ takes $\delta_P(V)$ into $\delta_P(U)$. Evidently, δ_P is a subpresheaf of Σ. Sometimes we shall call δ_P the *daseinisation* of P as well.

Realising that to a state ϕ corresponds a projection $|\phi\rangle\langle\phi|$, we try the following:

Definition 5.9. Given a poset of contexts $\mathcal{W}(\mathcal{H})$, the *pseudo-state* corresponding to a state $\phi \in \mathcal{H}$ is the presheaf

$$\mathfrak{w}^\phi = \delta_{|\phi\rangle\langle\phi|}.$$[2]

If $\lambda \in \mathfrak{w}^\phi(V)$ then the projection $\tau_V(\lambda)$ (see Theorem 2.10) is not orthogonal to ϕ. This means that if we measure the context V for ϕ, the probability of getting the valuation λ as an outcome is nonzero. $\mathfrak{w}^\phi(V)$ contains precisely those valuations of V accessible by measuring V for ϕ!

In a similar way, if $P = E[A \in \Delta]$ is some proposition and $\lambda \in \delta_P(V)$, then λ does not refute the proposition. In some sense, δ_P expresses that "$A \in \Delta$" holds, while giving 'the benefit of the doubt'[3] if "$A \in \Delta$" has no definite truth value for a particular context.

Example 5.10. For the OR-gate ℓ2-MBQC, the resource state $\psi = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ is a linear combination of the states $|{+}{+}{+}\rangle$, $|{+}{-}{-}\rangle$, $|{-}{+}{-}\rangle$ and $|{-}{-}{+}\rangle$, so $\mathfrak{w}^\psi(V_1) = \{\lambda_{+++}, \lambda_{+--}, \lambda_{-+-}, \lambda_{--+}\}$. By applying $\mathfrak{w}^\psi(V_{X_1} \subseteq V_1)$ to $\mathfrak{w}^\psi(V_1)$, we see that $\mathfrak{w}^\psi(V_{X_1})$ must be $\{\lambda_{+\cdot\cdot}, \lambda_{-\cdot\cdot}\}$.

$\mathfrak{w}^\psi$ has no global element. Suppose that $\Lambda\colon 1 \to \mathfrak{w}^\psi$ is one. We write λ for the union of the valuations it selects. These valuations are functions that have the same value where their domains coincide, so we can indeed put them together. Now, λ must satisfy the system of equations

$$\begin{aligned}
\lambda(X_1X_2X_3) &= 1\\
\lambda(X_1Y_2\,Y_3\,) &= -1\\
\lambda(Y_1\,X_2Y_3\,) &= -1\\
\lambda(Y_1\,Y_2\,X_3) &= -1,
\end{aligned}$$

since ψ is an eigenvalue of $X_1X_2X_3$ with eigenvalue 1, etc. We can multiply all the left-hand sides. We then take the multiplications out of the valuation (by using $\lambda(X_1X_2X_2) = \lambda(X_1)\lambda(X_2)\lambda(X_3)$, etc.) and shift around the factors to group pairs $\lambda(X_j)\lambda(X_j)$ and pairs $\lambda(Y_j)\lambda(Y_j)$. But $\lambda(X_j)\lambda(X_j) = \lambda(X_jX_j) = \lambda(I) = 1$, and similar for the Y_j's, so the whole multiplication simplifies to 1. If we multiply all the right-hand sides of these equations, we get -1. We see that the equations cannot be satisfied simultaneously, so $\mathfrak{w}^\phi$ has no global element. Although this does not prove the contextuality of all of $\mathcal{V}(\mathcal{H})$, we do know that there is not a global valuation that makes sense for ψ. We call this *state-dependent* contextuality.

[2] The authors of [7] do not seem to motivate their choice for the mysterious symbol "$\mathfrak{w}$", a "w" in fraktur font.

[3] There is perhaps an analogy with classical logic here. We consider the statement "p implies q" to be true if p is false and q is true. But if you think about it, this is tricky business: if p *would* have been true, how can we know for sure that q would be true as well? It makes just as much sense to assign "p implies q" the value false in this case. By saying it is true, we are giving it the benefit of the doubt.

5.4.3 Topos logic

Suppose that we have a poset of contexts $\mathcal{W}(\mathcal{H})$, a state ϕ and a proposition "$A \in \Delta$" with projection $P = E[A \in \Delta]$. For any context $V \in \mathcal{W}(\mathcal{H})$, the daseinisation $\delta_P(V)$ contains the valuations that do not refute "$A \in \Delta$". If $\mathfrak{w}^{\phi}(V) \subseteq \delta_P(V)$, then a measurement of V for ϕ will never refute $\delta^0_P(V)$. We could ask whether this holds for every context in $\mathcal{W}(\mathcal{H})$, or, equivalently, whether $\mathfrak{w}^{\phi}$ is a subpresheaf of δ_P. We will show that the concerned presheaves have surjective functions, so that this proposition gets a truth value in Ω.

Proposition 5.11. *Given a poset of contexts $\mathcal{W}(\mathcal{H})$ and any projection $P \in B(\mathcal{H})$, the function $\delta_P(U \subseteq V)\colon \delta_P(V) \to \delta_P(U)$ is surjective for every $U, V \in \mathcal{W}(\mathcal{H})$ with $U \subseteq V$.*

Proof. Let $\lambda_U \in \delta_P(U)$. The common eigenprojection $\tau_U(\lambda_U)$ of U corresponding to λ_U is in U and therefore in V. As a projection in V, it is also in $\mathcal{P}(V)$. Following the procedure in Theorem 2.10, we can write it as $\tau_U(\lambda_U) = \tau_V(\lambda_1) \vee \cdots \vee \tau_V(\lambda_k)$ where each λ_j is a valuation of V. Since $\lambda_U \in \delta_P(U)$, P is not orthogonal to $\tau_U(\lambda_U)$. This is only possible if it is not orthogonal to $\tau_V(\lambda_j)$ for some $j \leq k$ and therefore $\lambda_j \in \delta_P(V)$. Moreover, it must be that $\delta_P(U \subseteq V)(\lambda_j) = \lambda_U$. Since λ_U was arbitrary, $\delta_P(U \subseteq V)$ is surjective. □

We return to the proposition "$\mathfrak{w}^{\phi}$ is a subpresheaf of δ_P". Since both daseinisations are subpresheaves of Σ and have surjective functions, we know from section 4.3 that this proposition gets as truth value a global element of Ω in $\widehat{\mathcal{W}(\mathcal{H})}$, or, equivalently, a lower set $\mathcal{U}$ of $\mathcal{W}(\mathcal{H})$. This fact has a satisfactory physical interpretation. If $V \in \mathcal{U}$, then $\mathfrak{w}^{\phi}(V) \subseteq \delta_P(V)$ so no measurement of V for ϕ can refute "$A \in \Delta$", the proposition corresponding to P. Moreover, if $U \in \mathcal{W}(\mathcal{H})$ and $U \subseteq V$, then, since $\mathcal{U}$ is a lower set of $\mathcal{W}(\mathcal{H})$, also $U \in \mathcal{U}$ and therefore no measurement of U for ϕ can refute "$A \in \Delta$" either. This makes sense: U is a smaller context than V, so its valuations contain less information about the state of the system. If a valuation in V cannot refute "$A \in \Delta$", then certainly its restriction to U cannot refute it. $\mathcal{U}$ tells us precisely for which contexts the proposition holds 'with the benefit of the doubt'.

Using what we have learnt in section 4.3, we can express "$\mathfrak{w}^{\phi}$ is a subpresheaf of δ_P" as a formula in the language $\mathcal{L}(\widehat{\mathcal{W}(\mathcal{H})})$. If we let χ_{ϕ} and χ_P be the characteristic arrows of $\mathfrak{w}^{\phi}$ and δ_P (seen as subobjects of Σ), then the formula

$$\chi_{\phi}(x) \Rightarrow \chi_P(x)$$

is true for the topos $\widehat{\mathcal{W}(\mathcal{H})}$ if and only if $\mathfrak{w}^{\phi}$ is a subobject of δ_P.

5.5 Formula of determinism

We are now ready to express the determinism of an ℓ2-MBQC in the language of its topos. Our approach will be, for each input of the ℓ2-MBQC, to construct a presheaf containing all accessible valuations, to construct another presheaf that contains all valuations that give the desired output, and to compare them.

Definition 5.12. Let an ℓ2-MBQC be given, together with an input $\mathbf{i} \in \{0, 1\}^n$. We construct a subpresheaf $\mathfrak{w}^{\psi}_{\mathbf{i}}$ of the pseudo-state $\mathfrak{w}^{\psi}$ (remember that ψ is the resource state) that contains precisely those valuations that are accessible to the ℓ2-MBQC for the input $\mathbf{i}$.

Recall from Definition 5.1 that $\mathcal{Q} \subseteq \{0, 1\}^d$ is the set of labellings of possible choices of observables, and that $S_{\mathbf{a}}$ is the set of observables corresponding to $\mathbf{a} \in \mathcal{Q}$. Furthermore, if λ is a valuation of $S''_{\mathbf{a}}$, we define $\mathbf{s}_\lambda = (\lambda(A_1^{a_1}), \dots, \lambda(A_k^{a_k}))$. This is simply the vector of measurement outcomes that corresponds to λ. For every $\mathbf{a} \in \mathcal{Q}$, we let

$$\mathfrak{w}_{\mathbf{i}}^{\psi}(S''_{\mathbf{a}}) = \{\, \lambda \in \mathfrak{w}^{\psi}(S''_{\mathbf{a}}) \mid \mathbf{a} = T\mathbf{s}_\lambda + Q\mathbf{i} \pmod 2 \,\}\,.$$

The contexts of the form $S''_{\mathbf{a}}$ are precisely the maximal elements of the poset $\mathcal{W}(\mathcal{H})$. From their valuations we generate the remainder of $\mathfrak{w}_{\mathbf{i}}^{\psi}$ by applying the functions of Σ. For any $V \in \mathcal{W}(\mathcal{H})$,

$$\mathfrak{w}_{\mathbf{i}}^{\psi}(V) = \{\, \Sigma(V \subseteq S''_{\mathbf{a}})(\lambda) \mid \mathbf{a} \in \mathcal{Q}, \quad S''_{\mathbf{a}} \supseteq V \text{ and } \lambda \in \mathfrak{w}_{\mathbf{i}}^{\psi}(S''_{\mathbf{a}}) \,\}\,.$$

Now $\mathfrak{w}_{\mathbf{i}}^{\psi}$ is fully defined on objects. Its definition on morphisms is of course inherited from Σ. This makes it a subpresheaf of $\mathfrak{w}^{\psi}$.

Because the 'top level' component sets of $\mathfrak{w}_{\mathbf{i}}^{\psi}$ simultaneously take into account which measurement outcomes are possible and which choices of observables can come from them, they contain precisely those valuations that have a nonzero probability to be the measurement outcome, after one execution of the ℓ2-MBQC, using input $\mathbf{i}$. The whole of $\mathfrak{w}_{\mathbf{i}}^{\psi}$ is simply the smallest subpresheaf of $\mathfrak{w}^{\psi}$ that contains those valuations.

Now we construct the presheaf containing the valuations that effect a certain output.

Definition 5.13. Let an ℓ2-MBQC be given, together with the labelling $\mathbf{a} \in \mathcal{Q}$ of a choice of observables and an intended output $\mathbf{o} \in \{\,0,1\,\}^m$. The j'th row of R determines an observable $C_{\mathbf{a},j}$ in $S''_{\mathbf{a}}$: $C_{\mathbf{a},j} = \prod \{\, A_k^{a_k} \mid k \le d \text{ and } R_{jk} = 1 \,\} = (O_1(a_1))^{R_{j1}} \otimes \cdots \otimes (O_d(a_d))^{R_{jd}}$, where by $O_k(a_k)^0$ we mean I.

We can consider the daseinisation $\delta_{E(\mathbf{o},\mathbf{a},j)}$ of the proposition $E(\mathbf{o},\mathbf{a},j) = E[C_{\mathbf{a},j} \in \{\,1^{o_j}\,\}]$. Roughly speaking, this presheaf expresses that the j'th output bit is o_j if we measure the context $S''_{\mathbf{a}}$, and gives 'the benefit of the doubt' for other contexts. The conjunction (as in Definition 4.24) of these daseinisations for each $j \le m$ expresses the same for the entire output $\mathbf{o}$. Finally, we conjoin them for each maximal context in $\mathcal{W}(\mathcal{H})$:

$$\pi_{\mathbf{o}} = \bigcap_{\mathbf{a}\in\mathcal{Q}} \bigcap_{j \le m} \delta_{E(\mathbf{o},\mathbf{a},j)}.$$

Lemma 5.14. *For any ℓ2-MBQC, any intended output $\mathbf{o} \in \{\,0,1\,\}^m$ and the labelling $\mathbf{a} \in \mathcal{Q}$ of any choice of observables, we have that $\lambda \in \pi_{\mathbf{o}}(S''_{\mathbf{a}})$ if and only if $R\mathbf{s}_\lambda = \mathbf{o}$.*

Proof. We write $V = S''_{\mathbf{a}}$.

For the forward implication, suppose that $\lambda \in \pi_{\mathbf{o}}(V)$. Let $j \le m$ be arbitrary. The conjunctions in $\pi_{\mathbf{o}}$ are componentwise intersections, so $\lambda \in \delta_{E(\mathbf{o},\mathbf{a},j)}$. Since $E(\mathbf{o},\mathbf{a},j) \in V$, $\lambda(E(\mathbf{o},\mathbf{a},j)) = o_j$ and hence $\lambda(C_{\mathbf{a},j}) = 1^{o_j}$. If Z_j denotes the j'th row of R, then $Z_j\mathbf{s}_\lambda = \iota(\lambda(C_{\mathbf{a}}, j)) = o_j$. Since j was arbitrary, $R\mathbf{s}_\lambda = \mathbf{o}$.

For the other direction, we need to show that we did not lose too many valuations because of the intersections. Suppose that $\lambda \in \Sigma(V)$ satisfies $R\mathbf{s}_\lambda = \mathbf{o}$. We need to show that $\lambda \in \delta_{E(\mathbf{o},\mathbf{b},j)}(V)$ for every $\mathbf{b} \in \mathcal{Q}$ and $j \le m$. That is, $\tau_V(\lambda)$, the projection corresponding to λ, cannot be orthogonal to $E(\mathbf{o},\mathbf{b},j)$. We proceed by contradiction.

Suppose that $E(\mathbf{o},\mathbf{b},j)\tau_V(\lambda) = 0$. By definition, $E(\mathbf{o},\mathbf{b},j) = E[C_{\mathbf{b},j} \in \{\,1^{o_j}\,\}]$. We see from Definition 5.6 that $C_{\mathbf{b},j} = E[C_{\mathbf{b},j} \in \{\,1^{o_j}\,\}] + E[C_{\mathbf{b},j} \in \mathbb{R} \setminus \{\,1^{o_j}\,\}]$. But the only other eigenvalue of $C_{\mathbf{b},j}$ is -1^{o_j}. So $E[C_{\mathbf{b},j} \in \mathbb{R} \setminus \{\,1^{o_j}\,\}] = E[C_{\mathbf{b},j} \in \{\,-1^{o_j}\,\}]$. We have identified the two eigenspaces of $C_{\mathbf{b},j}$, which span $\mathcal{H}$, and $\tau_V(\lambda)$ is orthogonal to the first, so it must project into the second one: $\tau_V(\lambda) \le E[C_{\mathbf{b},j} \in \{\,-1^{o_j}\,\}]$. This implies that $\tau_V(\lambda)$ is an eigenprojection of $C_{\mathbf{b},j}$ with value -1^{o_j}.

Each $O_k(a_k)$ is non-degenerate, so when they are all measured, the state of every qubit is fixed and 'disentangled'. Only this ensemble state corresponds to the valuation obtained by the measurement. Therefore, $\tau_V(\lambda)$ is rank-1 and corresponds to a non-entangled state $\Phi = \phi_1 \otimes \cdots \otimes \phi_d$, and Φ is an eigenstate of $C_{\mathbf{b},j}$ with value -1^{o_j}.

Next, we can write $C_{\mathbf{b},j} = (O_1(b_1))^{R_{j1}} \otimes \cdots \otimes (O_d(b_d))^{R_{jd}}$. Since Φ is non-entangled, it can only be an eigenstate of $C_{\mathbf{b},j}$ if each ϕ_k is an eigenstate of $(O_k(b_k))^{R_{jk}}$. Of course, each ϕ_k is also an eigenstate of $O_k(a_k)$. But $O_k(0)$ and $O_k(1)$ aren't allowed to share eigenstates. We conclude that $a_k = b_k$ for every $k \leq d$ with $Z_jk = 1$.

But then $C_{\mathbf{a},j} = C_{\mathbf{b},j}$! From the assumption $R\mathbf{s}_\lambda = \mathbf{o}$ follows that $\lambda(C_{\mathbf{a},j}) = o_j$, which implies that Φ is an eigenstate of $C_{\mathbf{a},j}$ with value 1^{o_j}. But we have also seen that Φ is an eigenstate of $C_{\mathbf{b},j}$ with value -1^{o_j}. This is a contradiction, and therefore, $\lambda \in \delta_{E(\mathbf{o},\mathbf{a},j)}(V)$ for each $\mathbf{b} \in \mathcal{Q}$ and $j \leq m$. Since

$$\pi_{\mathbf{o}} = \bigcap_{\mathbf{b}\in\mathcal{Q}} \bigcap_{j\leq m} \delta_{E(\mathbf{o},\mathbf{b},j)}$$

and the conjunctions are componentwise intersections, also $\lambda \in \pi_o(V)$, completing the proof. □

The next proposition immediately follows.

Proposition 5.15. *An ℓ2-MBQC is deterministic for input $\mathbf{i}$ with output $\mathbf{o}$ if and only if $\mathfrak{w}_{\mathbf{i}}^{\psi}$ is a subpresheaf of $\pi_{\mathbf{o}}$.*

Proof. The probability for a valuation to be measured when the input is $\mathbf{i}$ is nonzero if and only if it occurs in $\mathfrak{w}_{\mathbf{i}}^{\psi}$. A valuation gives the right output if and only if it occurs in $\pi_{\mathbf{o}}$. $\mathfrak{w}_{\mathbf{i}}^{\psi}$ is a subpresheaf of $\pi_{\mathbf{o}}$ if and only if all the component sets of $\mathfrak{w}_{\mathbf{i}}^{\psi}$ are subsets of the component sets of $\pi_{\mathbf{o}}$. Therefore, the valuations that could be measured when the input is $\mathbf{i}$ all give the right output if and only if $\mathfrak{w}_{\mathbf{i}}^{\psi}$ is a subpresheaf of $\pi_{\mathbf{o}}$. □

Note that, unlike the daseinisations, $\mathfrak{w}_{\mathbf{i}}^{\phi}$ and $\pi_{\mathbf{o}}$ do not necessarily have only surjective functions, and hence the proposition "$\mathfrak{w}_{\mathbf{i}}^{\phi} \subseteq \pi_{\mathbf{o}}$" might not get a global element of Ω as a truth function like before. We can nonetheless express this proposition as a formula in the topos language, just as in the previous section. If we then take the conjunction over all inputs of this formula, we finally get the formula we were looking for.

Definition 5.16. Let notation be as in Definitions 5.12 and 5.13. $\chi_{\mathbf{o},\mathbf{a},\mathbf{j}}$ is the characteristic arrow of $\delta_{\mathbf{o},\mathbf{a},j}$ (seen as a subobject of Σ). $\chi_{\mathbf{i}}$ is the characteristic arrow of $\mathfrak{w}_{\mathbf{i}}^{\psi}$ (seen as a subobject of Σ).

Theorem 5.17. *An ℓ2-MBQC is deterministic with output function $\mathbf{o}(\mathbf{i})$ if and only if the formula*

$$\bigwedge_{\mathbf{i}\in\{0,1\}^n} \left(\chi_{\mathbf{i}}(x) \Rightarrow \bigwedge_{\mathbf{a}\in\mathcal{Q}} \bigwedge_{j\leq m} \chi_{\mathbf{o}(\mathbf{i}),\mathbf{a},j}(x) \right)$$

in the language $\mathcal{L}(\widehat{\mathcal{W}(\mathcal{H})})$ (in which x is a variable of type Σ) is true for the topos $\widehat{\mathcal{W}(\mathcal{H})}$.

Proof. By intuitionistic rules, conjunction is associative so the formula is well-defined. The formula is true (for $\widehat{\mathcal{W}(\mathcal{H})}$) if and only if all the operands of the outer conjunction are true, if and only if for each input, the condition in Proposition 5.15 is satisfied, if and only if the ℓ2-MBQC is deterministic with output function $\mathbf{o}(\mathbf{i})$. □

Using intuitionistic deduction, the conjunction symbols can be put before the brackets so that the formula takes a sort of conjunctive normal form. We could very loosely interpret the formula as saying: "For every x that is like a state, and for every input $\mathbf{i}$, if x could be encountered for $\mathbf{i}$, then x gives the right output, for each context and output bit", but this interpretation should not be taken too seriously.

This theorem is the climax of our report. But there are still things to be said. In the next section, we explore the foremost message of [14], relating the Booleanness of topoi and computational power. After that, in the final section, we comment on what we have seen.

5.6 Non-Booleanness

In the field of quantum computation, there is still some uncertainty as to what feature of quantum mechanics it is precisely that gives quantum computers an advantage over classical computers. One could make a few guesses based on what we have seen from MBQC. In an MBQC, the entanglement of the qubits decreases for each measurement, along with the computational possibilities. One could claim that entanglement is a *computational resource*. Somewhat similarly, in [18] it is shown that if an $\ell 2$-MBQC computes a nonlinear Boolean function, it must exhibit contextuality (remember that the classical side processing is linear, i.e. based on addition modulo 2), so contextuality could also be put forward.

In [14] another suggestion is made for the origin of the quantum advantage: "the *non-classical internal logic* of the given computation". We will first explain this claim and then challenge it.

5.6.1 Non-Booleanness decreases

Definition 5.18. A *Boolean algebra* is a Heyting algebra in which the law of excluded middle holds. That is, $x \wedge \neg x = \top$ for every element x.

In any topos, for two monic arrows f and g with the same domain, we have defined a relation $f \subseteq g$. It can be shown that the set of all subobjects[4] of any given object form a Heyting algebra under this ordering.

Definition 5.19. A topos is called *Boolean* if for every object X, the set of subobjects of X is a Boolean algebra when ordered by $\subseteq$.

Besides this generally known qualitative definition of non-Boolean, in [14] a quantitative one is given. In any Heyting algebra, $\neg\top = \bot$, so $\top \vee \neg\top = \top$ and $\bot \vee \neg\bot = \top$. Even when the law of excluded middle does not hold for all elements, it does for some. The authors of [14] therefore count the relative number of truth values in Ω for which the law of excluded middle does not hold. Specifically, the *non-Booleanness* of a topos is defined as

$$\mathfrak{q}\Gamma\Omega = 1 - \frac{|\mathrm{comp}\Gamma\Omega|}{|\Gamma\Omega|},^{5}$$

where $\Gamma\Omega$ is the set of global elements of Ω and $\mathrm{comp}\Gamma\Omega$ is the set of *complemented* ones: for which the law of excluded middle holds. Recall that for a global element f of Ω, we defined $\neg f$ as $f \Rightarrow \bot$. Note that, as we will see in the final section of this chapter, there is more to Ω than is exhibited by its global elements, and very importantly, $\mathfrak{q}\Gamma\Omega = 0$ for a topos does *not* imply that the topos is Boolean in the sense of Definition 5.19.

[4] Here we mean the formal definition of *subobject*: an isomorphism class of monic arrows.

[5] It seems to be a sport to choose a random letter in fraktur font for a new definition.

Next, the authors of [14] note that we can construct a new poset of contexts and therefore a new topos for every stage of an ℓ2-MBQC. Although they do not explicitly define these posets, we can imagine what they mean: they contain only the contexts that are still relevant to the computation. In the OR-gate example, it may happen that X_1 is measured first. In that case, for example, the contexts containing Y_1 do not need to be considered anymore.

For a specific execution of the OR-gate ℓ2-MBQC, they calculate the non-Booleanness at each stage, by counting the lower sets of the underlying posets. The result is a sequence $\frac{111}{113}$, $\frac{3}{5}$, $\frac{0}{2}$. In a few more sentences, they conclude that non-Booleanness decreases in any ℓ2-MBQC and that it therefore can be seen as a computational resource.

5.6.2 Non-Booleanness is constant

We see that the above non-Booleanesses are all of the form $\frac{k-2}{k}$. This is because in those cases $\top$ and $\bot$ are in fact the only complemented elements of the respective Heyting algebras. We wonder whether there can be other complemented elements for some ℓ2-MBQC.

We have seen that the Heyting algebra of the truth values in a topos of presheaves is equivalent to some $\downarrow P$, the set of lower sets of a poset P ordered by inclusion. Recall that in $\downarrow P$, $\vee$ and $\wedge$ are given by set union and intersection. $A \Rightarrow B$ is the largest lower subset of $(P \setminus A) \cup B$. The pseudo-complement $\neg X$ of $X \in \downarrow P$ is defined as $X \Rightarrow \bot$, where $\bot = \emptyset$. So $\neg X$ is the largest lower set in $P \setminus X$.

The law of excluded middle holds for X when $X \vee \neg X = \top = P$, i.e. when $\neg X = P \setminus X$. In what cases is $P \setminus X$ still a lower set? Suppose that we see P as an *un*directed graph and that there is a path from an element in X to an element in $P \setminus X$. Where the path leaves X between a and b, it must be that either $a \leq b$ or $b \leq a$, contradicting that X and $P \setminus X$ are lower sets. So, if there are to be other complemented elements than $\top$ and $\bot$, P must be disconnected.

According to [14], each stage of an ℓ2-MBQC has an associated subposet of $\mathcal{W}(\mathcal{H})$, although no concise definition has been given. We can however wager that, after measuring $O_1(q_1), \ldots, O_k(q_k)$ (where $k \geq 1$), such a subposet $\mathcal{W}(\mathcal{H})'$ has the following properties:

1. When represented as a subposet of $\mathcal{W}(\mathcal{H})_0$, it is closed under taking intersections (excluding the empty set).
2. If $U \in \mathcal{W}(\mathcal{H})'$, then there is a $V \in \mathcal{W}(\mathcal{H})'$ such that V is maximal in $\mathcal{W}(\mathcal{H})$ and $U \subseteq V$.
3. Every $U \in \mathcal{W}(\mathcal{H})'$ is compatible with $\{ O_1(q_1), \ldots, O_k(q_k) \}$.

At least we have that the single example in [14] satisfies these properties, but they seem reasonable in general. The second property means that there is a 'final' context of the ℓ2-MBQC that corresponds to U. If this were not the case, then either not all final contexts that are still accessible are in $\mathcal{W}(\mathcal{H})'$, or U could never be visited as an intermediate context and is therefore irrelevant.

Proposition 5.20. *For any ℓ2-MBQC, if $\mathcal{W}(\mathcal{H})' \subset \mathcal{W}(\mathcal{H})$ has the above properties, then $\downarrow \mathcal{W}(\mathcal{H})'$ has only two complemented elements.*

Proof. We need to show that $\mathcal{W}(\mathcal{H})'$ is connected as an undirected graph. Let $U, V \in \mathcal{W}(\mathcal{H})'$. Using property 2, find the maximal $\widetilde{U}$ and $\widetilde{V}$ that encompass U and V respectively. By property 3, $\{ O_1(q_1), \ldots, O_k(q_k) \}'' \subseteq \widetilde{U}, \widetilde{V}$ so by property 1, there is a $W \in \mathcal{W}(\mathcal{H})'$ with $W \subseteq \widetilde{U}, \widetilde{V}$. Now $(U, \widetilde{U}, W, \widetilde{V}, V)$ is a path. We conclude that $\mathcal{W}(\mathcal{H})'$ is connected and that therefore $\downarrow \mathcal{W}(\mathcal{H})'$ has only two complemented elements. □

What about $\mathcal{W}(\mathcal{H})$ itself? If $\mathbf{a} \in \mathcal{Q}$, then only $\mathbf{a}^c = (1 - a_1, \ldots, 1 - a_d) \in \mathcal{Q}$ shares no components with $\mathbf{a}$. So if $\mathcal{W}(\mathcal{H})$ has three or more maximal contexts, then it must be connected. If it has only the maximal contexts corresponding to $\mathbf{a}$ and $\mathbf{a}^c$, then the corresponding intersection is empty and it has only two elements altogether. In that case, $\downarrow\mathcal{W}(\mathcal{H})$ does have four complemented elements.

We remark that, in the definition of non-Booleanness, it is not really 'fair' to include $\top$ and $\bot$, because they are always complemented. So we redefine non-Booleanness:

$$\mathfrak{p}\Gamma\Omega = 1 - \frac{|\mathrm{comp}\Gamma\Omega| - 2}{|\Gamma\Omega| - 2}.$$

This is undefined for the case of classical logic, with only $\top$ and $\bot$ as truth values, in which case we define it as 0. Every ℓ2-MBQC ends up with this logic, when all measurements are done, because then only one context is left. As an example, the earlier non-Booleanness sequence $\frac{111}{113}$, $\frac{3}{5}$, $\frac{0}{2}$ changes to 1, 1, 0. Now we can claim that the non-Booleanness of an ℓ2-MBQC stays constant, except during one measurement, where it may drop once. We thus reject the idea that non-Booleanness is a computational resource.

There still remains the question of a topos being Boolean or not (as defined in Definition 5.19) and its relation to computation. This is settled by the following corollary of a theorem in [11] (which thankfully also appears in [14]):

Proposition 5.21. *Let P be a poset. Then $\widehat{P}$ is Boolean if and only if P contains just one element.*

This situation occurs when a computation no longer depends on the input or intermediate measurements after a certain stage. We do not have to look for any further computational significance behind a topos being Boolean or not.

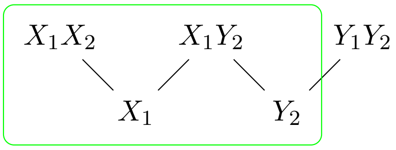
5.7 Comments

In this final section, we will tie up some loose ends and work towards a conclusion.

5.7.1 Physical interpretation of pseudo-complements

We have seen that we can assign a lower set of $\mathcal{W}(\mathcal{H})$ as a truth value to the proposition "$\mathfrak{w}^\phi \subseteq \delta_P$". What does it mean that this truth value is complemented or not? Can we associate a meaningful proposition with the pseudo-complement of the truth value? The following example shows that the answer to this last question is a rather unsatisfactory *no.*

Example 5.22. Consider any ℓ2-MBQC operating on two qubits. Designate the observables on the first qubit by X_1 and Y_1, and on the second one by X_2 and Y_2. Suppose first that $\mathcal{W}(\mathcal{H})$ is such that it can be represented by the following diagram (ignore the green box):



If we consider the proposition $P = E[Y_1 \in \{1\}]$, then P can never be refuted in the first four contexts. If moreover a state ϕ is not an eigenstate of Y_1, then the proposition "$\mathfrak{w}^\phi \subseteq \delta_P$" gets as truth value the lower set indicated by the green box in the figure. The pseudo-complement of this truth value is the largest lower set that shares no elements with it. This can only be the empty set.

Now suppose instead that the matrices Q and T are changed so that the context to X_1Y_2 is no longer accessible. The new $\mathcal{W}(\mathcal{H})$ can now be represented by this diagram:

$$\begin{tikzcd} X_1X_2 & & Y_1Y_2 \end{tikzcd}$$

This time, the proposition "$\mathfrak{w}^{\phi} \subseteq \delta_P$" gets as truth value the lower set containing only the context $\{ X_1, X_2 \}''$. This corresponds sensibly to the previous truth value. However, its pseudo-complement is now the lower set containing only $\{ Y_1, Y_2 \}''$, which is very different from the pseudo-complement from before! Clearly, only propositions explicitly depending on $\mathcal{W}(\mathcal{H})$ can have these pseudo-complements as truth values.

What can we make of this? Although we can come up with many candidate negations of "$\mathfrak{w}^{\phi} \subseteq \delta_P$" – like "$\mathfrak{w}^{\phi} \nsubseteq \delta_P$" or "$\mathfrak{w}^{\phi} \subseteq \delta_{I-P}$" – they will in general not get the pseudo-complement of the original truth value as their truth value, or sometimes not even a lower set at all. This brings us back to a point that has been made a few times before: the global elements of Ω do not play that special a role. Just as in the OR-gate ℓ2-MBQC $\mathfrak{w}^{\psi}$ does not have a global element, Ω is much more complex than the Heyting algebra of global elements we have defined for it. In particular, we cannot expect a link between computation and the structure of this Heyting algebra.

5.7.2 The value of the topos approach

Example 5.22 may also give the feeling that the definition of $\mathcal{W}(\mathcal{H})$ is somewhat arbitrary. Why is X_1 present in the first figure, while X_2 is not? Why is Y_2 in it, even though it can never be measured first? We made a similar point when we defined $\mathcal{W}(\mathcal{H})$. We can bet that in [14] $\mathcal{W}(\mathcal{H})$ is defined as it is, because it features contextuality for the OR-gate ℓ2-MBQC this way. However, our story remains largely unaltered when a different definition for $\mathcal{W}(\mathcal{H})$ is substituted. Specifically, Theorem 5.17 only depends on the final, maximal contexts corresponding to an ℓ2-MBQC. The fact that the Heyting algebra of truth values in Ω changes drastically with the arbitrary choice of a definition for $\mathcal{W}(\mathcal{H})$ is another reason to not overrate its importance.

A more serious flaw in the topos approach is the heavy use of constants in the formula of Theorem 5.17. In the language $\mathcal{L}(\widehat{\mathcal{W}(\mathcal{H})})$, each $\mathfrak{w}_{\mathbf{i}}^{\psi}$ and $\pi_{\mathbf{o},\mathbf{a},j}$ is a symbol with a particular arrow as interpretation — this is what we mean by constants. We may claim that we have a fully internal formulation of determinism, but it is only 'useful' when we, with our external view, assign the right arrows to the right constant symbols of the language. There is no way around this.

This may need some extra explanation. A topos can only 'think' in arrows and their compatibility — not in elements of component sets of presheaves. This is reflected in the internal language, where there are only symbols corresponding to arrows. We have mentioned in the previous chapter that there is no way of differentiating internally between isomorphic objects (other than by using constants). This even applies to objects like 'the' terminal object 1. We could express internally something like "for every object X, there is a unique arrow $X \to Y$". Then 1 satisfies this characterisation of Y, but so do infinitely many other isomorphic objects. In a similar fashion, if we do not want to use constants, we can only isolate Σ up to an isomorphism.

But it gets worse. If we have objects X and Y isomorphic to Σ and $\mathfrak{w}_{\mathbf{i}}^{\psi}$, then there are still multiple ways in which Y can 'lie in' X. Given two such ways (i.e. monic arrows), the topos can tell whether they are equal or distinct, but it can only differentiate in this relative manner. We see Σ as a pair of shoes, but the topos only sees a pair of socks. We cannot, using only general properties, isolate the monic that corresponds to $\mathfrak{w}_{\mathbf{i}}^{\phi}$ as a subpresheaf of Σ.

These flaws make us question how appropriate the topos approach really is. It certainly took some trouble to set it up. Contexts and valuations do give a different perspective on computation. And so does the presheaf of valuations on contextuality[6]. But beyond that, we cannot say that the topoi and presheaves gave new insights into quantum computation — or new questions!

5.7.3 Generalisation

Our results were only derived for a very restricted scheme of MBQC. We have made the following assumptions in ℓ2-MBQC:

1. There are two observables per qubit.
2. The observables are non-degenerate.
3. The classical side processing is linear.
4. The observables have eigenvalues in $\{1, -1\}$.
5. The observables have no shared eigenstates.

Our argument never depended on assumption 1 in a crucial way, so it can be dropped. Thanks to assumptions 3 and 4, we could elegantly represent an output bit by the value of one observable, but they are not essential either. A proposition like "$X_1 \in \Delta$ or $X_2 \in \Gamma$" can be dealt with just as well as "$\lambda(X_1 X_2) = 1$". Assumptions 5, on the other hand, is indispensable. For example, suppose that $O_1(0) = X$ and $O_1(1) = -X$, and that R is such that $o_1 = s_1$. If, for a certain input, the intended output is $o_1 = 0$, then the corresponding propositions are "$X_1 \in \{1\}$" and "$-X_1 \in \{1\}$". But any valuation of a context containing X_1 refutes one of these propositions. As a consequence, some component sets of $\pi_{\mathbf{o}}$ will be empty, so our grand formula can never be true, while the MBQC may still be deterministic. Assumption 2 can only be dropped insofar assumption 5 is not violated — which is never, for single-qubit observables.

5.7.4 Distributivity

As a final digression, we bring up a curiosity of daseinisation. The well-informed reader knows that 'traditional' quantum logic, as introduced by von Neumann himself [5] (but co-author Birkhoff must be credited as well), is non-distributive — this means that $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ does not hold for every triple x, y, z. The even better informed reader knows that any Heyting algebra is a distributive lattice. The daseinisation process has as domain the non-distributive lattice of projections $\mathcal{P}(B(\mathcal{H}))$, which has a greatest element and a least element, namely I and 0, which has a complement $I - P$ to each projection P, and in which projections can be seen as propositions. The daseinisation has as codomain the Heyting algebra of subobjects of Σ, which is necessarily distributive. What does daseinisation deform, so that distributivity is possible?

It turns out that, although $\delta_{P \vee Q} = \delta_P \vee \delta_Q$ always, in general $\delta_{P \wedge Q} \leq \delta_P \wedge \delta_Q$. By applying daseinisation, we lose the law of excluded middle, but we gain distributivity and the relative pseudo-complementation $\Rightarrow$. As the authors of [7] put it: "The inequality (...) is the price that must be paid for liberating the projection operators from the shackles of quantum logic and transporting them to the existential world of Heyting algebras."

[6] This perspective is also very general, in the sense that physical quantities and their values seem indispensable to any physical theory, so that the concepts *context* and *valuation* will always recur, while abstract conceptions like Hilbert spaces may not. This generality might be a remnant of [7] and its "new way of constructing theories of physics".

Chapter 6

Conclusion

Let us summarise what we have seen. Contexts and valuations offer a fresh perspective on computation. When structured in a presheaf, we can see which valuations are accessible by measuring qubits in a particular state, and which valuations make a proposition true. Thanks to the linear side processing and other constraints of $\ell 2$-MBQC, the output of an $\ell 2$-MBQC can be encoded as the value assigned to a particular observable, depending on the context in which it is measured. The proposition that a certain $\ell 2$-MBQC is deterministic can therefore be expressed as a relation between presheaves of valuations. This relation can in turn be represented by a formula in a formal language language of $\widehat{\mathcal{W}(\mathcal{H})}$, an associated topos of presheaves:

$$\bigwedge_{\mathbf{i}\in\{0,1\}^n}\left(\chi_{\mathbf{i}}(x)\Rightarrow\bigwedge_{\mathbf{a}\in\mathcal{Q}}\bigwedge_{j\leq m}\chi_{\mathbf{o}(\mathbf{i}),\mathbf{a},j}(x)\right)$$

The $\ell 2$-MBQC is deterministic if and only if this formula is true for $\widehat{\mathcal{W}(\mathcal{H})}$. Finally, we have seen some negative results on the importance of the topos logic for the computation. One is that non-Booleanness is not as significant as has been suggested in [14]. Another is that the language of $\widehat{\mathcal{W}(\mathcal{H})}$ cannot be used in a natural way to prove determinism completely internally, because we always need an external view to assign the right interpretations to the constants of the language.

We conclude that topos theory is not very suitable for quantum computation theory, even though it *is* very interesting when applied to general quantum mechanics, especially for foundational aspects. It has not given significant insights, applications or research questions.

Bibliography

[1] M. Adelman and J. V. Corbett. A sheaf model for intuitionistic quantum mechanics. *Applied Categorical Structures*, 3(1):79–104, 1995.

[2] J. Anders and D. E. Browne. Computational power of correlations. *Physical Review Letters*, 102(5):050502, 2009.

[3] J. S. Bell. On the Einstein Podolsky Rosen paradox. *Physics Physique Fizika*, 1(3):195, 1964.

[4] J. S. Bell. On the problem of hidden variables in quantum mechanics. *Reviews of Modern Physics*, 38(3):447, 1966.

[5] G. Birkhoff and J. Von Neumann. The logic of quantum mechanics. *Annals of mathematics*, pages 823–843, 1936.

[6] C. M. Constantin. Sheaf-theoretic methods in quantum mechanics and quantum information theory. *arXiv preprint arXiv:1510.02561*, 2015.

[7] A. Döring and C. Isham. "What is a thing?": topos theory in the foundations of physics. In *New structures for physics*, pages 753–937. Springer, 2010.

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

[9] R. Goldblatt. *Topoi: the categorial analysis of logic.* Elsevier, 2014.

[10] C. J. Isham and J. Butterfield. Topos perspective on the Kochen-Specker theorem: I. quantum states as generalized valuations. *International journal of theoretical physics*, 37(11):2669–2733, 1998.

[11] P. T. Johnstone. *Sketches of an Elephant: A Topos Theory Compendium*, volume 1. Oxford University Press, 2002.

[12] S. Kochen and E. P. Specker. The problem of hidden variables in quantum mechanics. In *The logico-algebraic approach to quantum mechanics*, pages 293–328. Springer, 1975.

[13] K. Landsman. *Foundations of quantum theory: from classical concepts to operator algebras.* Springer Nature, 2017.

[14] L. Loveridge, R. Dridi, and R. Raussendorf. Topos logic in measurement-based quantum computation. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 471(2176):20140716, 2015.

[15] S. Mac Lane. *Categories for the working mathematician.* Springer Science & Business Media, 2013.

[16] S. MacLane and I. Moerdijk. *Sheaves in geometry and logic: A first introduction to topos theory*. Springer Science & Business Media, 2012.

[17] N. D. Mermin. Hidden variables and the two theorems of John Bell. *Reviews of Modern Physics*, 65(3):803, 1993.

[18] R. Raussendorf. Contextuality in measurement-based quantum computation. *Physical Review A*, 88(2):022322, 2013.

[19] R. Raussendorf and H. J. Briegel. A one-way quantum computer. *Physical Review Letters*, 86(22):5188, 2001.

Nomenclature

1	Terminal object in a topos of presheaves, page 18
1_a	Identity arrow for an object a, page 15
A_k^0, A_k^k	Observable on the ensemble of qubits corresponding to $O_k(0)$ and $O_k(1)$, page 12
$B(\mathcal{H})$	C*-algebra of all linear operators on a Hilbert space $\mathcal{H}$, page 6
$E[A \in \delta]$	Projection corresponding to a proposition "$A \in \delta$", page 27
$\mathcal{H}$	Hilbert space of an $\ell 2$-MBQC, page 12
I	Identity operator on a Hilbert space, page 6
$\mathcal{L}(\mathcal{T})$	Formal language of a topos $\mathcal{T}$, page 23
M_V	Set of minimal projections of $\mathcal{P}(V) \setminus \{0\}$, page 9
$O_k(0)$, $O_k(1)$	Single-qubit observables of an $\ell 2$-MBQC, page 12
$\mathcal{P}(V)$	Lattice of projections in V, page 8
Q	Matrix for determining a choice of observables from an input, page 12
$\mathcal{Q}$	Set of labellings of possible choices of observables, page 24
R	Matrix for determining an output from measurement outcomes, page 12
$S_{\mathbf{a}}$	Set of observables corresponding to the choice of observables $\mathbf{a}$, page 24
Set	Category of sets, page 15
T	Matrix for determining a choice of observables from measurement outcomes, page 12
$\mathcal{V}(\mathcal{H})$	Partially ordered set of unital Abelian subalgebras of $B(\mathcal{H})$, page 6
$\mathcal{W}(\mathcal{H})$	Partially ordered set of contexts relevant to an $\ell 2$-MBQC, page 24
$\mathcal{W}(\mathcal{H})_0$	Partially ordered set of choices of observables relevant to an $\ell 2$-MBQC, page 24
X	Pauli matrix, page 6
Y	Pauli matrix, page 6
Z	Pauli matrix, page 6
d	Number of qubits of an $\ell 2$-MBQC, page 12

m	Output size in bits of an $\ell 2$-MBQC, page 12
n	Input size in bits of an $\ell 2$-MBQC, page 12
$\mathbf{o}$	Output of an $\ell 2$-MBQC, page 13
$\mathbf{q}$	Choice of observables for an $\ell 2$-MBQC, page 12
$\mathbf{s}$	Vector of measurement outcomes of an $\ell 2$-MBQC, page 12
$\mathbf{s}_\lambda$	Vector of measurement outcomes corresponding to a valuation λ, page 30
$\mathfrak{w}^\phi$	Pseudo-state presheaf corresponding to a state ϕ, page 28
$\mathfrak{w}^\psi_\mathbf{i}$	Presheaf of accessible valuations for an input $\mathbf{i}$, page 29
$\Gamma\Omega$	Heyting algebra of truth values, page 22
Σ	Spectral presheaf, page 25
$\Sigma(V)$	Set of valuations on a context V, page 7
Ω	Truth value object of a topos, page 21
δ_P	Daseinisation presheaf of a projection P, page 27
$\delta^0_P(V)$	Outer daseinisation of a projection P in a context V, page 27
ι	Function that maps 1 to 0 and -1 to 1, page 12
$\pi_\mathbf{o}$	Presheaf of valuations that effect an intended output $\mathbf{o}$, page 30
$\sigma(A)$	Spectrum of eigenvalues of a linear operator A, page 7
τ_V	Bijection that maps a valuation of V to its corresponding eigenspace, page 9
ψ	Resource state of an $\ell 2$-MBQC, page 12
χ	Characteristic arrow of a monic arrow f, page 21
S'	The commutant of a set of observables S, page 10
$\circ$	Composition of arrows of a category, page 15
$\cong$	Isomorphism of objects of a category, page 16
$\downarrow P$	Set of lower sets of the poset P, page 22
$\|+\rangle$	Eigenstate of X with eigenvalue 1, page 6
$\|-\rangle$	Eigenstate of X with eigenvalue -1, page 6
$\|0\rangle$	Eigenstate of Z with eigenvalue 1, page 6
$\|1\rangle$	Eigenstate of Z with eigenvalue -1, page 6
$\|\downarrow\rangle$	Eigenstate of Y with eigenvalue -1, page 6
$\|\uparrow\rangle$	Eigenstate of Y with eigenvalue 1, page 6

$\langle f, g\rangle$	Product arrow, page 19
$\leq$	Partial order of projections, page 8
$\leq$	Partial order of truth values, page 21
$\leq$	Partial order, page 8
$\oplus$	Integer addition modulo 2, page 11
$\subseteq$	Inclusion relation on monic arrows, page 20
$\subseteq$	Subpresheaf relation, page 20
$\times$	Product of objects in a topos of presheaves, page 19
$\widehat{P}$	Topos of presheaves on a poset P, page 18
$\bot$	Falsehood arrow, page 21
$\top$	Truth arrow, page 21
$\cap$	Conjunction of subobjects, page 20
$\cup$	Disjunction of subobjects, page 20
$\Rightarrow$	Implication of characteristic arrows, page 21
$\Rightarrow$	Relative pseudo-complementation in a Heyting algebra, page 21
$\neg$	Pseudo-complementation, page 22
$\vee$	Disjunction of projections, page 8
$\vee$	Join operation of a lattice, page 8
$\wedge$	Conjunction of characteristic arrows, page 21
$\wedge$	Conjunction of projections, page 8
$\wedge$	Meet operation of a lattice, page 8