A 2-Categorical Analysis of Complementary Families, Quantum Key Distribution and the Mean King Problem

Krzysztof Bar

Department of Computer Science, University of Oxford

krzysztof.bar@cs.ox.ac.uk

Jamie Vicary

Centre for Quantum Technologies, University of Singapore
and Department of Computer Science, University of Oxford

jamie.vicary@cs.ox.ac.uk

This paper explores the use of 2-categorical technology for describing and reasoning about complex quantum procedures. We give syntactic definitions of a family of complementary measurements, and of quantum key distribution, and show that they are equivalent. We then show abstractly that either structure gives a solution to the Mean King problem, which we also formulate 2-categorically.

1   Introduction

The 2-categorical approach to quantum information is now well-developed in its basic aspects [4, 12, 14]. The central aim is to use the structure of a symmetric monoidal 2-category to describe quantum procedures in an abstract way, such that the ordinary versions of these procedures are recovered when we apply the formalism in **2Hilb**, the symmetric monoidal 2-category of 2-Hilbert spaces [3]. This builds on the highly successful categorical quantum mechanics research programme of Abramsky, Coecke and collaborators [1, 2], in which quantum procedures are axiomatized in terms of monoidal 1-categories.

The key advantage of the 2-categorical setup is that many important structures, such as teleportation, dense coding and complementary observables, can be defined by single 2-categorical equations. These typically have direct physical interpretations, with the defining equation for a structure following immediately from a careful physical description of its required properties. A computer algebra system *TwoVect* [10, 11] allows these equations to be directly evaluated computationally.

In this paper, we show that the formalism can be applied successfully to more sophisticated quantum procedures: measurements in a complementary family of bases, quantum key distribution (QKD), and the Mean King problem. For each scenario, we write down a 2-categorical equation that defines the entire procedure in a precise way. For example, here is the defining diagram for BB84 QKD:
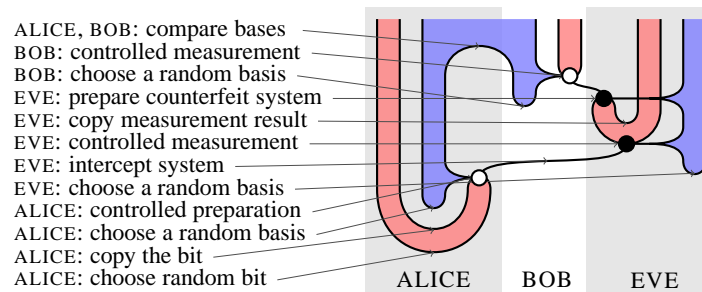
We have annotated this diagram with text to show how the different parts are to be interpreted, but we emphasize that this annotation is superfluous: everything about the flow of quantum and classical information is captured by the diagram itself. To complete the abstract definition of BB84 quantum key

distribution, we require that this diagram is equal to a second diagram which encodes the intended result of the procedure.

The main contributions of this paper are as follows:

- Definitions 15, 20, 21 and 29 give 2-categorical equations whose solutions in **2Hilb** correspond exactly to implementations of a family of complementary observables, BB84 QKD, E91 QKD, and solutions of the Mean King problem respectively.

- In Theorem 27 we show that the 2-categorical definition for a family of complementary measurements is equivalent to that for QKD. While an equivalence between these notions seems generally expected in the community, we are not able to find an existing crisp proof in the literature.

- In Theorem 37 we give a graphical proof of correctness of Klappenecker and Rottleer's solution [9] to the Mean King problem. This is roughly the same complexity as the original proof, but quite different in nature. The graphical proof makes clear the role played by complementarity.

A significant result on the categorical basis of quantum key distribution was given by Coecke and Perdrix in [7, Proposition 7.4], which demonstrates the correctness of QKD based on a pair of complementary observables. Our work goes beyond this result, as we work with arbitrary families of complementary observables rather than a single pair, and we further show that every implementation of QKD gives rise to a family of complementary observables.

A primary avenue of future work arising from our results will be investigating the existence of nonstandard models. It has been shown that a category of groupoids, profunctors and spans admits combinatorial 'toy models' of teleportation, as solutions to a 2-categorical equation, from which ordinary quantum teleportation can be recovered by applying a 2-functor into **2Hilb** [4]. It will be interesting to use the results of this paper to investigate whether combinatorial toy models of quantum key distribution can also be built in that setting.

Remark on colour and transparency. The diagrams in this paper make essential use of colour and transparency. We therefore recommend reading this paper on a screen, or as a colour printout. For printing we recommend Adobe Reader, as some other PDF viewers do not correctly handle transparency.

1.1 The 2-category 2Hilb of 2-Hilbert spaces

It has been argued in [14] that the 2-category of 2-Hilbert spaces [3] is the correct 2-categorical setting in which to analyze quantum informatic procedures. We recall the following construction of **2Hilb**, which is most useful for calculation. For more details, see the papers cited above.

Definition 1. The symmetric monoidal 2-category **2Hilb** has *objects* given by natural numbers, *1-morphisms* given by matrices of finite-dimensional Hilbert spaces, and *2-morphisms* given by matrices of linear maps. Details of the compositional structure of **2Hilb** are available in the references given.

This gives the formal categorical semantics that forms the primary model of our abstract syntax, introduced in Section 1.2.

1.2 The topological formalism

The basic 2-categorical structures on which the theory is built have simple graphical representations [14], thanks to the graphical notation for monoidal 2-categories. This graphical formalism involves surfaces, lines and vertices. Their basic interpretation is as follows:

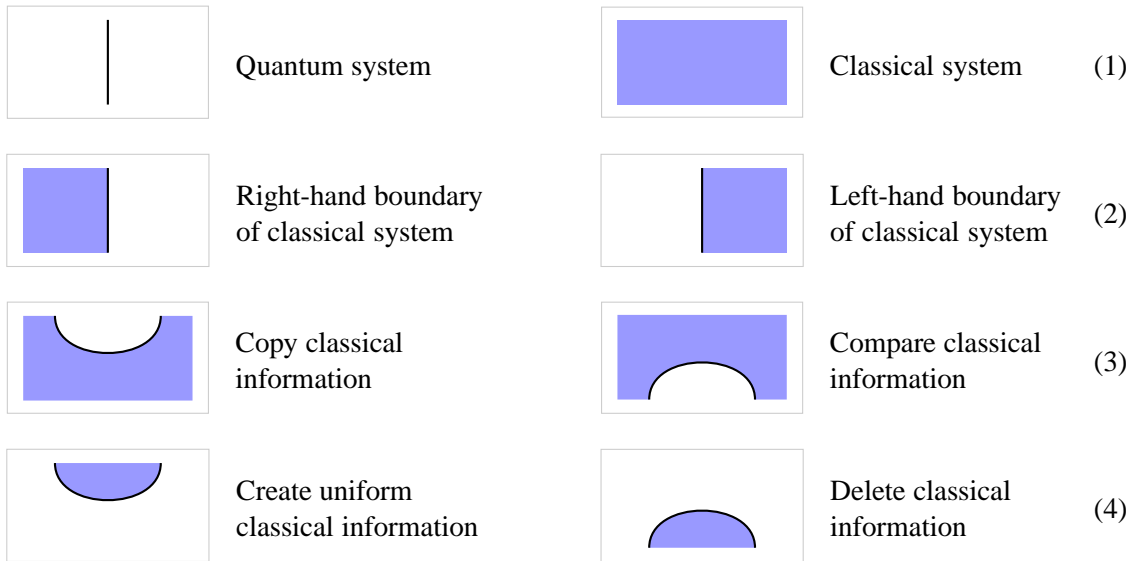| Category theory	Geometry	Interpretation	
Objects	Surfaces	Classical information	
1-Morphisms	Lines	Quantum systems	
2-Morphisms	Vertices	Physical operations	

Composite diagrams involving many vertices are interpreted as a series of actions that place over time, with time flowing from bottom to top. In the graphical calculus, composition of 1-morphisms is given by horizontal juxtaposition, and composition of 2-morphisms by vertical juxtaposition. The tensor product is given by 'overlaying' regions one above the other, perpendicular to the plane of the page and the tensor unit is expressed by an unlabelled, empty region.

We desire the ability to take the formal adjoint of 2-cells, represented graphically by flipping a diagram about a horizontal axis.

Definition 2. A *dagger 2-category* is a 2-category equipped with an involutive operation $\dagger$ on 2-cells, such that for all $\mu : F \Rightarrow G$ we have $\mu^\dagger : G \Rightarrow F$, which is functorial and compatible with the rest of the monoidal 2-category structure.

Definition 3. A 2-cell μ is *unitary* when $\mu \circ \mu^\dagger = \mathrm{id}$ and $\mu^\dagger \circ \mu = \mathrm{id}$.

The core graphical theory makes use of only a small number of graphical components. They give the formal syntax for our theory. We summarize them here, along with their interpretations, which are motivated in detail in [14].

Quantum system	Classical system	(1)
Right-hand boundary of classical system	Left-hand boundary of classical system	(2)
Copy classical information	Compare classical information	(3)
Create uniform classical information	Delete classical information	(4)

These components are required to satisfy a set of axioms, which amount to saying that the boundary of a region is topological, and that holes can be eliminated:

$$(5)$$

$$(6)$$
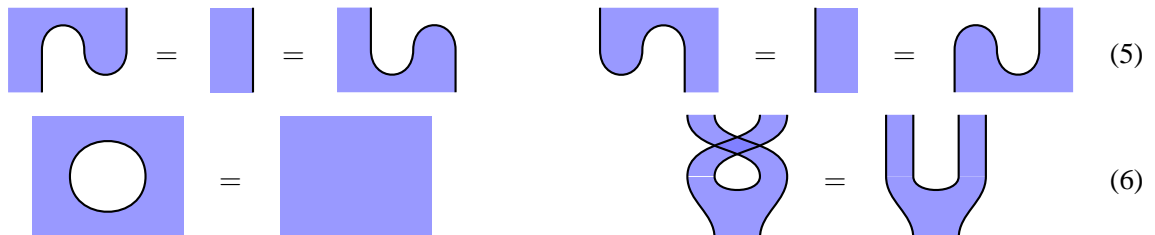
All rotations and mirrored versions of the last of these axioms are also imposed. The net effect of these axioms is that any two connected networks of copying, comparison, creation and deletion operations, with the same number of inputs and the same number of outputs, will be equal. It follows that every such region carries the structure of a commutative dagger-Frobenius algebra in a canonical way. Note that the symmetric monoidal 2-category structure is used crucially in the last equation here, allowing one region to pass above another.

Definition 4. In a symmetric monoidal 2-category, an object has a *topological boundary* if it is equipped with the data (2)–(4) satisfying equations (5)–(6).

We will assume throughout that we are working with dagger 2-categories whose objects are equipped with topological boundaries.

1.3   Controlled operations

In this paper, a key role will be played by the concept of a *controlled family of measurements* which we define here in a new way. This has the following definition in the 2-categorical formalism.

Definition 5. A *controlled family of measurements* is a unitary 2-cell of the following type:


$$(7)$$

The left-hand pool of classical information represents classical data that will determine the measurement basis, which we will always draw in blue. The line at the bottom-right of the diagram represents the quantum system to be measured. The upper-right pool of classical information represents the classical result of the measurement, which we will always draw in red.

We interpret these measurements as perfectly fine-grained (that is, non-degenerate), and projective. The motivation for the definition above is made clear by analyzing its models in **2Hilb**.

Lemma 6. *In **2Hilb**, a controlled family of measurements corresponds precisely to a Hilbert space equipped with a list of orthonormal bases.*

Proof. Given a 2-cell ζ of the type (7) in **2Hilb**, write n for the dimension of the blue object, and m for the dimension of the red object. Then it is immediate that ζ constitutes a list of length n, whose entries are m-by-m matrices [14]. For ζ to be unitary means exactly that each m-by-m matrix is unitary. So we have a list of n unitary operators. However, the red region comes equipped with a canonical commutative dagger-Frobenius algebra structure, and hence a canonical orthonormal basis. Writing the unitaries in terms of this basis, it is clear that the data of ζ is canonically equivalent to a list of n orthonormal bases for the incoming m-dimensional Hilbert space.   □

The unitarity property of (7) takes the following graphical form:

$$(8)$$
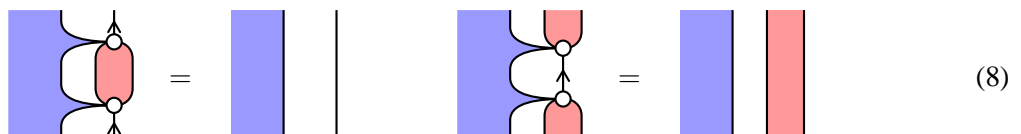
Definition 7 (Conjugate measurement bases)**.** Following the standard conventions, a controlled measurement with respect to the *conjugate* set of bases is represented by mirroring the diagram about a vertical axis:

$$
\vcenter{\hbox{\includegraphics{fig1}}} := \left(\vcenter{\hbox{\includegraphics{fig2}}}\right)_* \equiv \vcenter{\hbox{\includegraphics{fig3}}} \tag{9}
$$

Here we decompose the conjugation operation into a composition of adjoint and transpose operations. The blue classical data controlling the choice of basis is now naturally on the right-hand side.

However, we may want to change the side of the classical data controlling the choice of basis *without* passing to the conjugate set of bases. To do this, we use the symmetric monoidal 2-category structure to directly move the blue classical region to the other side. In order to distinguish this from the conjugate controlled measurement (9), we represent it as a black vertex.

Definition 8 (Control from the other side)**.** We use a black vertex to indicate control of the measurement and encoding vertices from the other side:

$$
\vcenter{\hbox{\includegraphics{fig4}}} := \vcenter{\hbox{\includegraphics{fig5}}} \qquad \vcenter{\hbox{\includegraphics{fig6}}} := \vcenter{\hbox{\includegraphics{fig7}}} \tag{10}
$$

Arrows indicating dual objects will generally be omitted for simplicity.

1.4   Projectors

We will often need to constrain the value held by a pool of classical data, which we do with projectors of different kinds.

Definition 9. Given an object $\mathbf{C} \equiv \mathbf{Hilb}^n$ in **2Hilb**, a *classical data projector* is an element of the canonical n-element basis for the vector space $\mathrm{Hom}_{\mathbf{2Hilb}}(\mathrm{id}_{\mathbf{C}}, \mathrm{id}_{\mathbf{C}})$.

These projectors act to constrain the classical data stored in a region to a particular value. We write them as floating labels that decorate our regions. The following lemma establishes some of their key properties.

Lemma 10 (Properties of classical data projectors)**.** *For diagrams in **2Hilb**, we can use classical data projectors to decompose the identity, and two adjacent projectors annihilate unless they are identical:*

$$
\vcenter{\hbox{\includegraphics{fig8}}} = \sum_{a=1}^{n} \vcenter{\hbox{\includegraphics{fig9}}} \qquad\qquad \vcenter{\hbox{\includegraphics{fig10}}} = \delta_{a,b} \vcenter{\hbox{\includegraphics{fig11}}} \tag{11}
$$

The projectors can move freely around within regions, much like scalars in the theory of monoidal categories. Furthermore, labelled regions can be connected and disconnected arbitrarily:

$$
\vcenter{\hbox{\includegraphics{fig12}}} = \vcenter{\hbox{\includegraphics{fig13}}} \qquad\qquad \vcenter{\hbox{\includegraphics{fig14}}} = \vcenter{\hbox{\includegraphics{fig15}}} \tag{12}
$$

Proof. Straightforward, but omitted for reasons of space.   □

We can also define a different type of projector, which constrains the values of two separate regions of classical data to be the same, or to be different. We will always apply these projectors to regions that are coloured blue in our notation. There will always be exactly 2 blue regions in every diagram where we use the projectors, so it will be unambiguous to which regions they 'attach'.

Definition 11 (Same-value and different-value projectors)**.** In a symmetric monoidal 2-category whose hom-categories are **Ab**-enriched, for an object with topological boundary, the *same-value projector* P_s and *different-value projector* P_d are defined as follows:

$$P_s \quad := \qquad \qquad \qquad \qquad \qquad \qquad \qquad \qquad (13)$$

$$P_d \quad := \qquad \qquad \qquad \qquad - \qquad \qquad \qquad \qquad \qquad (14)$$

The main 2-category we are concerned with is **2Hilb**, in which hom-categories are indeed **Ab**-enriched.

Lemma 12. *The projectors P_s and P_d satisfy $P_s^2 = P_s$, $P_d^2 = P_d$, $P_s \circ P_d = P_d \circ P_s = 0$ and $P_s + P_d = \mathrm{id}$.*

Proof. Straightforward graphical proof, omitted for reasons of space. □

We will assume throughout that we are working in an **Ab**-enriched 2-category, and so these projectors are well-defined. The tensor product, vertical and horizontal composition in the 2-category all distribute over the additive structure introduced by these projectors. Distributivity of 2-cell composition with respect to addition is illustrated by the following. Note, that we can apply the projectors P_s , P_d whenever the appropriate regions have any open boundary:

$$P_d \quad = \quad \left(\qquad \qquad - \qquad \qquad \right) \circ \qquad = \qquad - \qquad \qquad (15)$$

1.5 Attaching controlled phases

Definition 13. A *controlled phase* ϕ is an unitary endomorphism of a family of boundaries:

$$\phi \qquad \qquad \qquad \qquad (16)$$

The white nodes decorating the 2-cell ϕ indicate the boundaries to which it attaches.

In **2Hilb**, such a structure gives a controlled phase in the ordinary sense: a family of unit complex numbers, indexed by the values of the classical information of the regions to which the phase is connected. The result of such a controlled phase is to render the overall wavefunction of the system entangled, without introducing any classical statistical correlation between local measurement results [14].

2   Complementary families of measurements

In Definition 5 we introduced a 2-categorical axiomatization of a controlled family of measurements. In this Section, we add the extra requirement that any two distinct measurements in the family are *complementary*. In this case, we say that we have a *complementary family* of measurements. These play an essential role in quantum key distribution and the Mean King problem, which we study in Sections 3 and 4.

For a single pair of nondegenerate measurements to be complementary is a standard condition in quantum information, sometimes also known as *unbiasedness*.

Definition 14. Two bases $\{|a_i\rangle\}$, $\{|b_j\rangle\}$ of a finite-dimensional Hilbert space H are *complementary*, or *unbiased*, when for all i, j we have $|\langle a_i|b_j\rangle|^2 = \dim(H)^{-1}$.

A first characterization of this property in terms of monoidal categories was given by Coecke and Duncan [6], and a 2-categorical definition was given in [14].

2.1   Basic definition

Definition 15 (Complementary family)**.** A *complementary family of measurements*, or simply a *complementary family*, is an ordinary family of measurements as given in Definition 5, such that there exists some unitary 2-cell ϕ satisfying the following equation:

$$(17)$$

The black measurement vertex is as defined in 8. Attenuation of the region controlling the measurement choice is a notation allowing to avoid obstructing the rest of the diagram. This definition has an immediate physical motivation. On the left-hand side, we measure a quantum system in some particular basis, copy the result, and then re-encode the result back into a quantum state using the same basis. Then, according to a second basis guaranteed to be different to the first thanks to the projector P_d, we make a new measurement, represented by the black vertex, on the re-encoded state. The right-hand side of the equation says that this entire procedure must be equivalent to doing the original measurement with respect to the original basis, but then choosing the second measurement result uniformly at random, up to the application of some overall phase that allows the wavefunctions to be entangled without introducing any classical correlation.

That this definition is correct for ordinary quantum theory is immediate from previous results on the 2-categorical characterization of complementary measurements.

Lemma 16. *In **2Hilb**, the complementary families are exactly Hilbert spaces equipped with a collection of pairwise-complementary orthonormal bases.*

Proof. Labelling the left- and right-hand blue regions on each side of equation (17) with distinct projectors a and b respectively, we obtain the ordinary 2-categorical condition for a complementary pair of orthonormal bases [14]. Conversely, suppose we have a family of orthonormal bases; then by writing the identity as a sum of projectors using Lemma 10, equation (17) follows.   □

2.2 Alternative characterizations

Here we examine alternative characterizations of the complementary family definition.

Lemma 17 (Complementarity through unitarity)**.** *A controlled family of measurements is complementary if and only if the following 2-cell is unitary on the support of the projector P_d:*

$$\alpha \quad := \qquad \tag{18}$$

Proof. See Appendix. □

The following alternative formulations of complementarity will prove useful in a later section.

Lemma 18 (Complementarity condition under horizontal reflection)**.** *A family of controlled measurement operations is complementary if and only if the following equation is satisfied:*

$$\tag{19}$$

Proof. By Lemma 17, both α and $\alpha^\dagger$ are unitary on the support of the projector P_d. The condition 19 can be obtained by elementary 2-cell operations from the unitarity of $\alpha^\dagger$. □

Lemma 19 (Alternative formulation of complementarity)**.** *A controlled family of measurement operations is complementary if and only if the following condition is satisfied:*

$$\tag{20}$$

*Proof.* The result is proved using Lemma 17 and by performing topological manipulations. □

3 Quantum key distribution

In this Section we give 2-categorical equations defining quantum key distribution (QKD), in both its BB84 [5] and E91 [8] forms. In Theorem 22 we show that these forms are equivalent. Our main result is Theorem 27, in which we demonstrate that these quantum key distribution equations are equivalent to Definition 15 of a complementary family of measurements.

3.1   Abstract definitions

Definition 20 (BB84 QKD). A controlled family of measurements satisfies *BB84 quantum key distribution* if there exists a unitary 2-cell ψ satisfying the following equation:
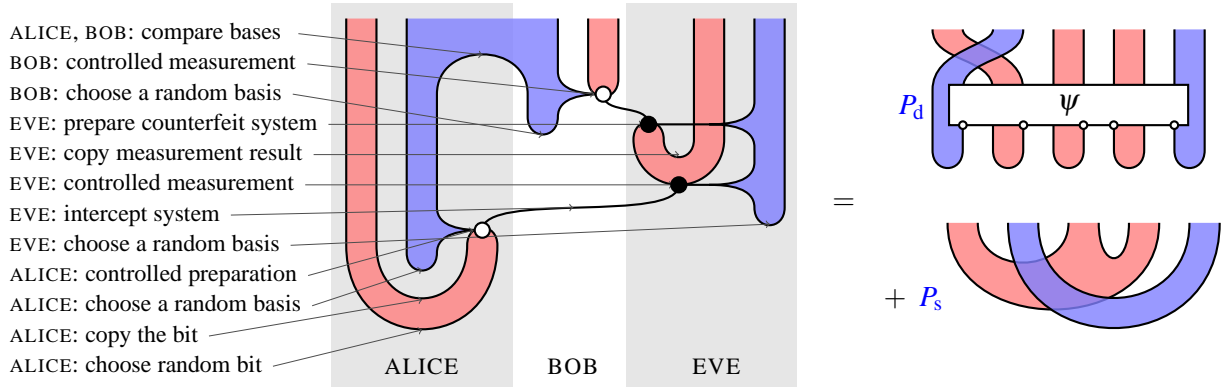
Each of the diagrams on the right-hand side corresponds to the desired behaviour depending on whether Eve guessed the basis correctly. If Eve guesses incorrectly, then the P_{d} term says that both basis choices and all 3 measurement results are classically uncorrelated. If Eve guesses correctly, the then P_{s} term says that Eve shares Alice and Bob's basis, and that all 3 agents share the same classical data.

A different equation can be obtained from consideration of the E91 QKD protocol.

Definition 21 (E91 QKD). A controlled family of measurements satisfies *E91 quantum key distribution* if there exists a unitary 2-cell ψ satisfying the following equation:
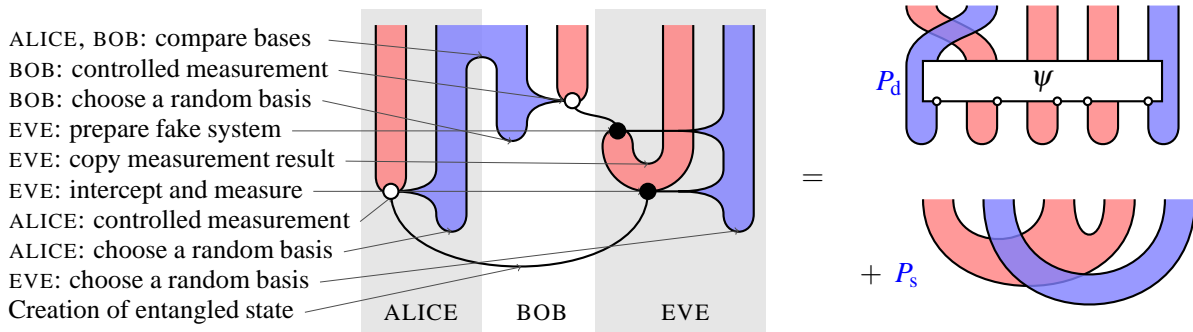
Theorem 22. *The equations for BB84 and E91 QKD are equivalent.*

Proof. Elementary topological manipulation.   □

Lemma 23 (Eve's successful interference). *On the support of projector P_{s}, the quantum key distribution specification is satisfied for any controlled family of measurements.*

Proof. See Appendix.   □

3.2 Quantum key distribution from a complementary family

Lemma 24. *If a controlled family of measurements is complementary, then it satisfies the quantum key distribution specification with:*

$$(21)$$

Proof. See Appendix. ☐

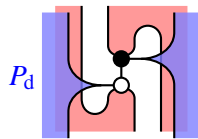## 3.3 A complementary family from quantum key distribution

Lemma 25. *If a controlled family of measurements allows quantum key distribution with a phase ψ, then:*

$$(22)$$

Proof. See Appendix. ☐

Lemma 26. *If a controlled family of measurements allows quantum key distribution, then the family is complementary.*

Proof. By Lemma 25 the following map is unitary:

By Lemma 17, we can conclude that the controlled family of measurements is complementary. ☐

Theorem 27. *A controlled family of measurements satisfies quantum key distribution if and only if it is complementary.*

Proof. Immediate by Lemmas 24 and 26. ☐

Lemma 28. *If a controlled family of measurements allows quantum key distribution with phase ψ, then we can decompose ψ in the following way:*

$$(23)$$

Proof. Immediate by Lemmas 24 and 26.   □

4   The Mean King problem

The Mean King problem is defined as follows [13, 9]. There are two agents, Alice and the King, who take part in the following procedure.

1. Alice hands a quantum state to the King.

2. The King measures the state in one of n mutually unbiased bases, keeping both the basis and the outcome secret, and returns the state to Alice.

3. Alice performs any quantum measurement she wishes.

4. The King reveals his measurement basis to Alice.

5. Using only classical processes, Alice must calculate the King's earlier measurement outcome.

With some thought, it becomes clear that for Alice to have the best chance of succeeding, she should retain an entangled partner to the system initially passed to the King. Alice should then apply a predetermined measurement procedure to the entangled state that will reveal the King's measurement result every time, regardless of his basis choice. In other words, she should perform some nondegenerate PVM μ on both systems in step 3, and prepare a lookup table f that tells her, depending on the King's measurement basis choice and her own measurement result, what King's result was.

The key results of this Section is a graphical definition of a solution of the Mean King problem, and a graphical proof of the correctness of Klappenecker and Rötteler's solution [9] to the Mean King problem.

4.1   Abstract definition

We begin with an abstract definition of the Mean King problem. Recall that in categorical quantum mechanics, a *classical function* is defined as a morphism between classical data which satisfies the comonoid homomorphism property, and that regions with topological boundary carry a canonical comonoid structure.

Definition 29 (Mean King scheme). Given a complementary family of measurements ●, a bipartite measurement μ, and a classical function f, a *Mean King scheme* $\mathrm{MK}_{●,\mu,f}$ is defined as the following composite:

$$(24)$$

Definition 30 (Mean King solution). A Mean King scheme $\mathrm{MK}_{●,\mu,f}$ *solves the Mean King problem* if the following equation holds:

$$(25)$$

This says exactly that, after carrying out the procedure, Alice and the King carry the same measurement result information. It will be satisfied precisely if the Mean King scheme $\mathrm{MK}_{●,\mu,f}$ is correct.

4.2 Solving the Mean King problem

Our solution to the Mean King problem is presented entirely graphically. It is based on a solution due to Klappenecker and Rötteler [9]. Giving this solution graphically is an interesting exercise in the graphical formalism, and demonstrates that it is capable of reasoning about sophisticated schemes. Our presentation is roughly comparable in complexity to Klappenecker and Rötteler's. One advantage of our presentation is that it is perhaps clearer exactly how complementarity is being used.

We begin by giving a scheme to construct a bipartite state from a classical function.

Definition 31. Given a classical function $f_i : n \to m$, and an n-fold controlled family of measurements on $\mathbb{C}^n$, the associated bipartite state $|\mu_f\rangle \in \mathbb{C}^n \otimes \mathbb{C}^n$ is defined as follows:

Definition 32 (Collisions)**.** Given classical functions $f, g : n \to m$, let $f \diamond g := |\{a | f(a) = g(a)\}|$ be the number of *collisions* between them.

Lemma 33. *Let $f, g : [n+1] \to [n]$ be functions. Then $n\langle \mu_f | \mu_g \rangle + 1 = f \diamond g$.*

Proof. A straightforward graphical proof is possible, which we omit. □

Lemma 34. *Given a family of n^2 classical functions $f_i : [n+1] \to [n]$ with $i \neq j \Rightarrow f_i \diamond f_j = 1$, the states $|\mu_{f_i}\rangle$ form an orthonormal basis.*

Proof. Rearranging the result of Lemma 33, we see that $\langle \mu_f | \mu_g \rangle = ((f \diamond g) - 1)/n$, and the conclusion follows. □

Lemma 35. *For any prime power $n = p^k$, the following structures exist:*

1. *a family of n^2 functions $f_i : [n+1] \to [n]$, such that for $i \neq j$ we have $f_i \diamond f_j = 1$;*

2. *a family of $n+1$ mutually complementary bases.*

Proof. See [9, Section 2]. □

Lemma 36. *For a complementary family of controlled measurements and a classical function g, the following holds:*

(26)

Proof. See Appendix. □

Theorem 37 (Solution to the Mean King problem). *For a family of functions $f_i : [n+1] \to [n]$ such that $|\mu_{f_i}\rangle$ form a basis, and a family $\bullet$ of $n+1$ complementary bases of $\mathbb{C}^n$, the following assignments give a Mean King solution:*
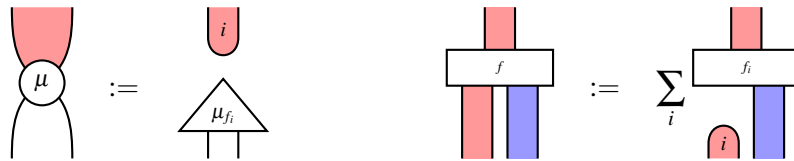
Proof. See Appendix.   □

References

[1] Samson Abramsky & Bob Coecke (2004): *A Categorical Semantics of Quantum Protocols*. Proceedings of the 19th Annual IEEE Symposium on Logic in Computer Science, pp. 415–425, doi:10.1109/LICS.2004.1. arXiv:quant-ph/0402130.

[2] Samson Abramsky & Bob Coecke (2008): *Handbook of Quantum Logic and Quantum Structures*, chapter Categorical Quantum Mechanics, pp. 261–323. 2, Elsevier.

[3] John C Baez (1997): *Higher-Dimensional Algebra II: 2-Hilbert Spaces*. Advances in Mathematics 127, pp. 125–189, doi:10.1006/aima.1997.1617. arXiv:q-alg/9609018.

[4] Krzysztof Bar & Jamie Vicary (2014): *Groupoid Semantics for Thermal Computing*. arXiv:1401.3280.

[5] C.H. Bennett & G. Brassard (1985): *Quantum public key distribution*. IBM Technical Disclosure Bulletin 28, pp. 3153–3163.

[6] Bob Coecke & Ross Duncan (2011): *Interacting Quantum Observables: Categorical Algebra and Diagrammatics*. New Journal of Physics 13(043016), doi:10.1088/1367-2630/13/4/043016. arXiv:0906.4725.

[7] Bob Coecke & Simon Perdrix (2012): *Environment and Classical Channels in Categorical Quantum Mechanics*. Logical Methods in Computer Science 8(4), pp. 1–24, doi:10.2168/LMCS-8(4:14)2012. arXiv:1004.1598.

[8] Artur Ekert (1991): *Quantum cryptography based on Bell's theorem*. Physical Review Letters 67, p. 661, doi:dx.doi.org/10.1103/PhysRevLett.67.661.

[9] Andreas Klappenecker & Martin Rötteler (2005): *New Tales of the Mean King*. arXiv:quant-ph/0502138.

[10] Dan Roberts (2011): *Representing Modular Tensor Categories: A Computer Algebra System for Topological Quantum Computing*. Master's thesis, Department of Computer Science, University of Oxford.

[11] Dan Roberts & Jamie Vicary: *The TwoVect Package*. A computer algebra system for higher linear algebra. http://ncatlab.org/nlab/show/TwoVect.

[12] Mike Stay & Jamie Vicary (2013): *Bicategorical Semantics of Nondeterministic Computation*. In: Proceedings of the 29th Conference on the Mathematical Foundations of Programming Semantics, 298, pp. 367–382, doi:10.1016/j.entcs.2013.09.022. arXiv:1301.3393.

[13] Lev Vaidman, Yakir Aharonov & David Z. Albert (1987): *How to Ascertain the Values of σ_x, σ_y and σ_z of a Spin-$\frac{1}{2}$ Particle*. Physics Review Letters 58, pp. 1385–1387, doi:dx.doi.org/10.1103/PhysRevLett.58.1385.

[14] Jamie Vicary (2012): *Higher Semantics of Quantum Protocols*. Proceedings of the 27th Annual IEEE Symposium on Logic in Computer Science, pp. 606–615, doi:10.1109/LICS.2012.70. Extended version at arXiv:1207.4563.

Appendix

**Proof of Lemma 17.** We consider the following chain of equivalences:

For the first equivalence we compose at the bottom with the inverse of the controlled measurement vertex; for the second we perform a topological manipulation. Since ϕ is an arbitrary unitary 2-cell, it is clear that the last condition is exactly that given in the statement of the lemma. □

Proof of Lemma 23. We investigate this scenario by applying the projector P_s on both sides of the specification. In this case the right-hand side only retains the P_s component, and the left hand side simplifies as follows:

Vertex colour changes are justified by changing the side from which the operations are controlled in accordance with Definition 8. By this, we can conclude that after application of P_s the QKD specification becomes a tautology. □

Proof of Lemma 24. Suppose the controlled complementarity condition 15 is satisfied. Then we make the following argument:
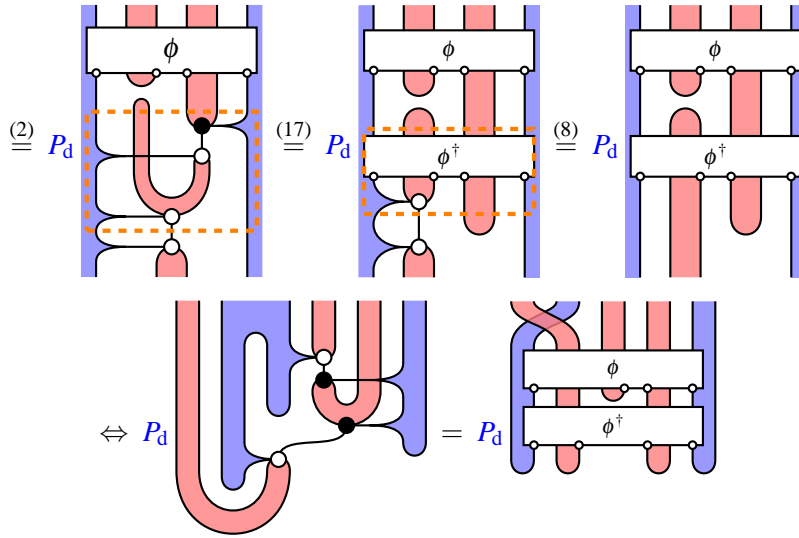
The final equality follows from the first chain of equalities by topological deformation. This final equality is equivalent to the statement of BB84 quantum key distribution as given in Definition 20, since by Lemma 23 the P_s component is trivially satisfied. □

Proof of Lemma 25. If Eve picks the wrong basis but does not influence the communication between Alice and Bob, their key information is still the same. We post-select on this scenario by applying a projector P_d to pools of classical information corresponding to Alice's, Bob's and Eve's basis information and by applying the comparison operation to pools corresponding to Bob's and Alice's key information:


$$(27)$$
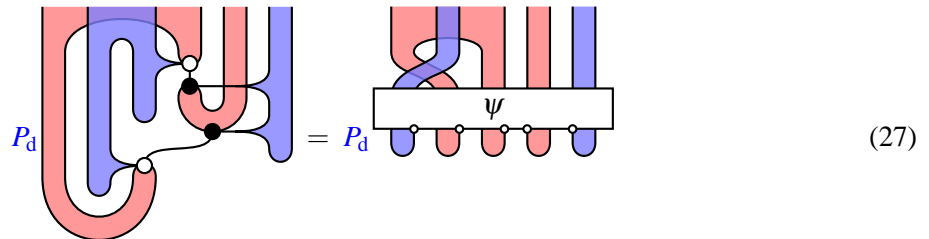
Using topology-preserving elementary 2-cell operations, the first equality in 22 is obtained. For the second equality, up to application of P_d on the outer pools of classical information, the middle 2-cell in equation 22 is a unitary, since ψ is a unitary. Also, $\alpha^\dagger \circ \alpha$ is a positive map. The only positive unitary is the identity, hence the result is established. □

Proof of Lemma 36. We use the fact that these controlled measurements form a family of complementary controlled operations. Hence equation (20) holds, and we combine it with the classical

function g to obtain the left-hand side given below:
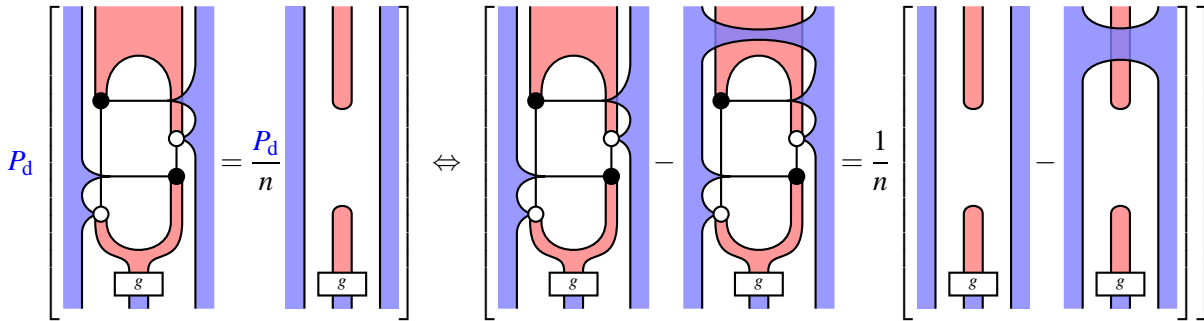
The right-hand side is obtained by expanding out the action of the projectors P_d. We next assign specific values a, b to pools of classical information and perform elementary 2-cell operations. We can replace black vertices with white, as long as we switch the side from which the vertex is controlled. Since pools of classical information exhibit topological behaviour, we can reposition them freely.
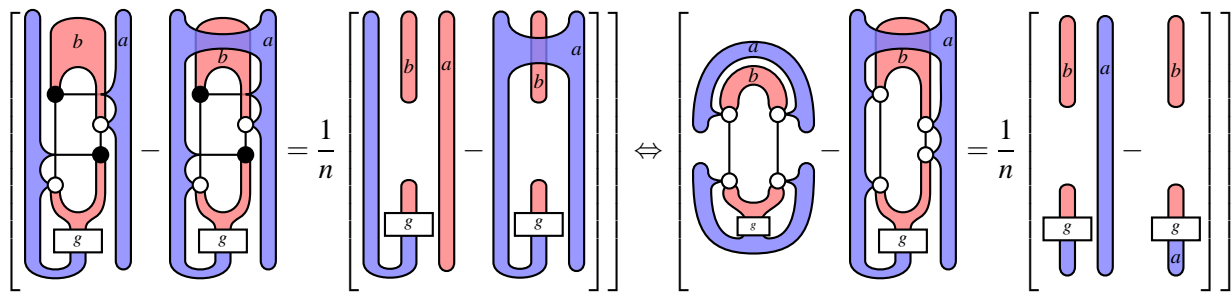

After we cancel out measurement and encoding operations controlled by the same pools of classical information, the equation is simplified to:

$$(28)$$

Proof of Theorem 37. By Lemma 35 a suitable family of n^2 functions $f_i : [n+1] \to [n]$ and a complementary family of controlled measurements in $n+1$ bases exist. The latter by defining a controlled operation to pick one of the $n+1$ complementary bases to measure in. For each f_i we define a state μ_{f_i} in accordance with Lemma 31. By Lemma 34 states $|\mu_{f_i}\rangle$ form an orthonormal basis μ that we

use to solve the problem. The scheme $MK_{\bullet,\mu,f}$ then simplifies to:
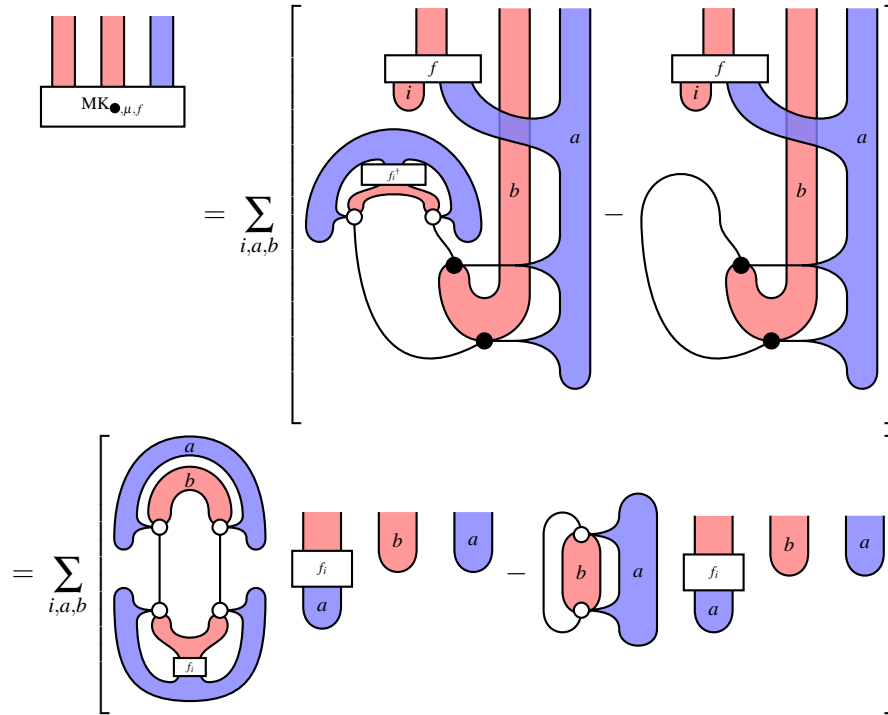
By Lemma 36, this simplifies as follows:
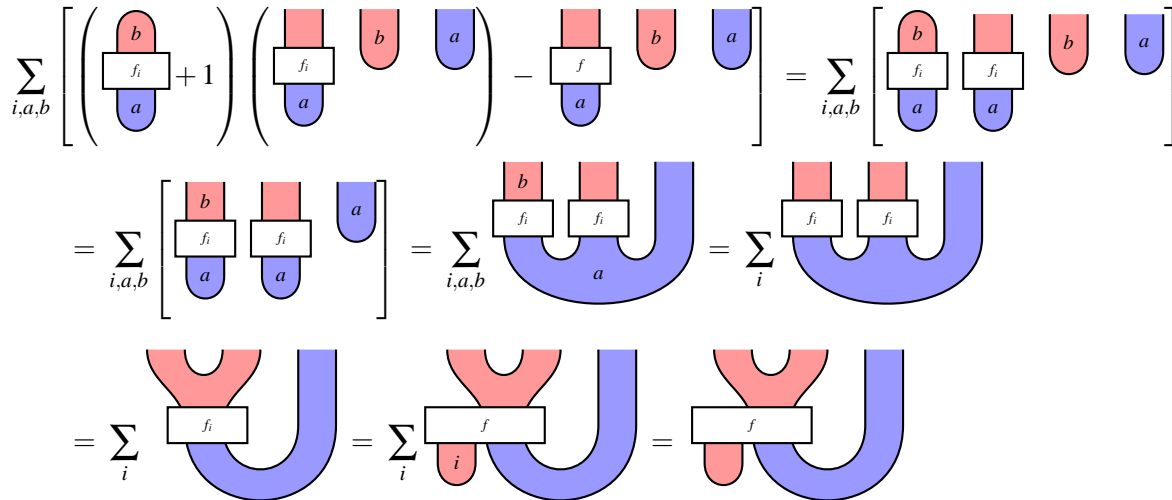
The final diagram clearly remains unchanged under application of the projector as per Definition 30, hence the result is established. □