Categorical quantum computation

Mark Richard Przepiora

December 20, 2009

1 Introduction and motivation

Dirac published *The Principles of Quantum Mechanics* in 1930, in which he presented the notational framework for studying quantum mechanics that is still ubiquitous today. Indeed, in this work exist all the tools needed to develop our entire current body of knowledge of quantum computation and information processing. However, it wasn't until 1993 that six IBM Fellows discovered the quantum teleportation protocol, more than 60 years after Dirac provided them with the mathematical canvas, brushes and paint.

Like the fact that the concept of mathematical induction wasn't fully developed until the 19^{th} century, this *ought* to shock future historians. The teleportation protocol is strikingly simple, and its steps can be described in one or two sentences. Yet, the difficulty of its analysis using the notation Dirac invented and we inherited is incredibly disproportionate to its description.

As a result, there has been much effort in the past decade to develop new formalisms for studying quantum mechanics and quantum computation especially, ones in which there are more natural analyses of the well-known protocols. In [4], Selinger proposed a design of a quantum programming language with loops, recursion, and data types. Abramsky and Coecke made perhaps the most ambitiously-titled attempt, *Kindergarten Quantum Mechanics*[3], an entirely pictorial calculus from which teleportation supposedly emerges trivially from a "string yanking" rule.

Algebraically, they made their formalism rigorous using the language of category theory in [1] and [2], and this is the side of their formalism on which we focus. Their work attempts to capture the concepts of state spaces, scalars, adjoints, inner products, probability amplitudes and so in very a very general category theoretic setting. Although this approach is rather different than Selinger's, he later attempted to reconcile his work with theirs in [5].

Since moving away from the tangible comfort of Hilbert spaces to the abstractions of a category can be a traumatic experience, our goal is to make the transition as smooth as possible by relating abstract categorical definitions to their concrete incarnations in Hilbert spaces whenever possible.

2 Definitions and properties

From now on, we will no longer live inside the class of Hilbert spaces in particular, but in *compact closed categories*, which (as we shall see) capture a great number of the fundamentals of the Hilbert space model of quantum mechanics, from a starting point of only a handful of properties imposed on a category.

Definition 1. A *compact closed category* is a category $\mathbf{C}$ together with the following:

1. A *tensor product* functor $- \otimes - : \mathbf{C} \times \mathbf{C} \to \mathbf{C}$.

2. A *unit* object I with natural isomorphisms

$$\lambda_A : A \simeq I \otimes A \qquad \rho_A : A \simeq A \otimes I$$

3. Natural isomorphisms

$$\alpha_{A,B,C} : A \otimes (B \otimes C) \simeq (A \otimes B) \otimes C$$

$$\sigma_{A,B} : A \otimes B \simeq B \otimes A$$

   that satisfy some coherence properties.

4. A full and faithful functor $* : \mathbf{C}^{op} \to \mathbf{C}$ for which there are natural isomorphisms

$$\mathbf{C}(A \otimes B, C^*) \simeq \mathbf{C}(A, (B \otimes C)^*)$$

$$u_{A,B} : (A \otimes B)^* \simeq A^* \otimes B^* \qquad u_I : I^* \simeq I$$

Note that such a category is indeed closed, with an internal hom given by

$$A \multimap B = (A \otimes B^*)^* \simeq A^* \otimes B (\simeq B \otimes A^*)$$

Readers versed in the Dirac notation should immediately recognize the above isomorphism, as the taken-for-granted fact that any transformation between vector spaces may be written as a sum of projectors $|\psi\rangle\langle\phi|$.

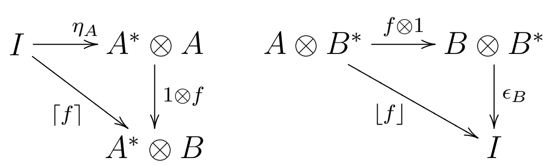
Indeed, all of the above properties are generalizations of facts about Hilbert spaces. For example, the reader should recognize the second property as a generalization of the fact that $\mathcal{H} \simeq \mathcal{H} \otimes \mathbb{C}$, i.e. that constant factors are "absorbed" by a Hilbert space.

Each compact closed category has a unit and counit

$$\eta_A : I \to A^* \otimes A \qquad \epsilon_A : A \otimes A^* \to I$$

which, roughly speaking, allow identity transformations to take the scenic route in the ways we'd expect. In Hilbert spaces, the unit is the linear map which sends 1 to either the "identity operator" (actually an element of $A^* \otimes A$) or a "cat state" depending on the interpretation one takes, while the counit takes inner products.

Definition 2. Every morphism $f : A \to B$ has a *name* $\lceil f \rceil : I \to A^* \otimes B$ and a *coname* $\lfloor f \rfloor : A \otimes B^* \to I$ given in the obvious ways,



In the setting of Hilbert spaces, the name of an operator ξ maps 1 to the what is normally interpreted as the operator's representation as a sum of projectors, and the coname evaluates its matrix entries, i.e. it performs the mapping $|j\rangle, \langle k| \mapsto \langle k| \xi |j\rangle$.

As hinted a few paragraphs earlier, in terms of names and conames, we have $\eta = \lceil 1 \rceil$ and $\epsilon = \lfloor 1 \rfloor$. In fact, just as in the case of Hilbert spaces, *every* morphism $I \to A^* \otimes B$ is the name of a morphism from $A \to B$, and similarly every morphism of type $A \otimes B^* \to I$ is the coname of a morphism from $A \to B$. We of course take this for granted in a Hilbert space, where we know that every matrix defines an operator, as does every sum of projections.

As we'd expect, every compact closed category also possesses a natural isomorphism $d_A : A^{**} \simeq A$.

Composition also behaves with names and conames the way we'd expect it to. Namely, $\lceil fg \rceil$ is given by $\lceil f \rceil(1 \otimes g)$. In terms of Hilbert spaces, this expresses the elementary fact that if we write an operator $\xi = \sum_k |\phi_k\rangle\langle k|$ as a sum of projections, then the composition $\zeta\xi = \sum_k (\zeta\,|\phi_k\rangle)\,\langle k|$.

Similarly, we can write fg as

$$\begin{array}{ccccc} A & \xrightarrow{\rho} & A \otimes I & \xrightarrow{1\otimes\lceil g\rceil} & A \otimes B^* \otimes C \\ & & & & \Big\downarrow {\scriptstyle \lfloor f \rfloor \otimes 1} \\ & \searrow^{fg} & & & I \otimes C \\ & & & & \Big\downarrow {\scriptstyle \lambda^{-1}} \\ & & & & C \end{array}$$

and the name $\lceil fgh \rceil$ is equal to

$$\begin{array}{ccccc} I & \xrightarrow{\rho} & I \otimes I & \xrightarrow{\lceil f\rceil\otimes\lceil h\rceil} & A^* \otimes B \otimes C^* \otimes D \\ & & & & \Big\downarrow {\scriptstyle 1 \otimes \lfloor g \rfloor \otimes 1} \\ & \searrow^{\lceil fgh \rceil} & & & A^* \otimes I \otimes D \\ & & & & \Big\downarrow {\scriptstyle \rho^{-1} \otimes 1} \\ & & & & A^* \otimes D \end{array}$$

We note that the last two diagrams suggest a kind of reversal of time, in which applying f followed by g is equivalent to first applying the name of g followed by the coname of f. Indeed, drawing these rules using the equivalent pictorial calculus reveals a clear "quantum information flow" in which the flow of information follows a path which may bend backward through the time dimension.

3 A short digression on teleportation

We can now (very!) informally present the teleportation protocol. Names and conames have a certain physical interpretation in this formalism: a name $\lceil f \rceil$ represents the preparation of an entangled state. (In particular, $\lceil 1 \rceil = \eta$

represents preparation of a Bell state.) On the other hand, a coname $\lfloor f \rfloor$ represents the outcome of a measurement in a particular world.

Applying the previous compositional properties, we can write,

$$fgU = \rho(1 \otimes \lceil g \rceil)(\lfloor f \rfloor \otimes 1)\lambda^{-1}U$$

This interaction involves three systems: an entangled state is prepared in the rightmost two systems, a measurement is performed on the leftmost systems, and finally an operation U is applied "on the right". In teleportation, we of course want $fgU = 1$.

In Hilbert spaces, when each system is a single qubit, this can be achieved by setting $g = 1$ and picking $U = f^{-1}$. However, there are problems with this naive approach: if we interpret the coname $\lfloor f \rfloor$ as an observational branch, then there will be many possibilities $\lfloor f_i \rfloor$in the protocol. Furthermore, many states $\lfloor f_i \rfloor$ correspond to, far from unitary, but singular operators f_i. Thus, we must choose to measure in a basis $\lfloor f_i \rfloor$ where each f_i is unitary.

In particular, the computational basis does *not* satisfy this requirement, because to

$$\lfloor f_{00} \rfloor = |00\rangle \quad \lfloor f_{01} \rfloor = |01\rangle \quad \lfloor f_{10} \rfloor = |10\rangle \quad \lfloor f_{11} \rfloor = |11\rangle$$

correspond the operators

$$f_{00} = |0\rangle\langle 0| \quad f_{01} = |0\rangle\langle 1| \quad f_{10} = |1\rangle\langle 0| \quad f_{11} = |1\rangle\langle 1|$$

On the other hand, choosing each $f_i = \sigma_i$ to be the i^{th} Pauli operator gives $\lfloor f_i \rfloor$ as the Bell basis, which results in the commonly-known protocol: preparing an EPR pair, measuring in the Bell basis, and applying an appropriate Pauli gate.

4 More definitions and properties

4.1 Biproducts

Suppose a category has a zero object $\mathbf{0}$ and hence a zero morphism $0_{A,B} : A \to B$ between any two objects. Let A_1, A_2 be objects with a product $A_1 \times A_2$ and coproduct $A_1 \sqcup A_2$, and consider a morphism $\xi : A_1 \sqcup A_2 \to A_1 \times A_2$. Since a map from a coproduct is defined by its inclusions and a map to a product is defined by its projections, ξ may be written as a matrix of morphisms

$$\xi_{j,k} = A_j \xrightarrow{i_j} A_1 \sqcup A_2 \xrightarrow{r} A_1 \times A_2 \xrightarrow{\pi_k} A_k$$

Definition 3. Consider the "identity matrix" $\delta_{j,k}$ which extends the definition of the Kronecker delta in the obvious way. If $\delta_{j,k}$ is an isomorphism, then we call $A_1 \sqcup A_2 \simeq A_1 \times A_2$ a *biproduct*, and denote it $A_1 \oplus A_2$.

Given any two morphisms $f, g : A \to B$ in a category with biproducts, we may define the sum $f + g$ by

$$A \xrightarrow{\Delta} A \oplus A \xrightarrow{f \oplus g} B \oplus B \xrightarrow{\nabla} B$$

which is associative, commutative and has an identity $0_{A,B}$.

We can prove a number of facts about categories with biproducts.

Proposition 4. *Consider a biproduct $\bigoplus A_k$. By extending the idea in definition 3, we can choose projections π_j and inclusions i_j such that $i_j \pi_k = \delta_{j,k}$ and $\sum \pi_k i_k = 1_{\bigoplus A_k}$.*

Proposition 5. *In any monoidal closed category with biproducts, there are natural isomorphisms*

$$A \otimes (B \oplus C) \simeq (A \otimes B) \oplus (A \otimes C)$$

$$(A \oplus B) \otimes C \simeq (A \otimes C) \oplus (B \otimes C)$$

Proposition 6. *In any compact closed category with biproducts, there are natural isomorphisms*

$$(A \oplus B)^* \simeq A^* \oplus B^* \qquad \mathbf{0}^* \simeq \mathbf{0}$$

Corollary 7. *Write nX for an n-fold biproduct of X. Then there is a natural isomorphism*

$$nI \simeq (nI)^*$$

4.2 Scalars and vectors

We can define abstract scalars and vectors in this setting.

Definition 8. In a compact closed category, a *scalar* is a morphism $s : I \to I$, and a *vector* is a morphism $\psi : I \to A$.

Given a scalar s, we can naturally extend it to $s_A : A \to A$ by $s_A = \lambda(s \otimes 1)\lambda^{-1}$, and hence define a scalar multiplication for morphisms $f : A \to B$, defined by $s \cdot f = s_A f$.

In terms of Hilbert spaces, a linear transformation from $s : \mathbb{C} \to \mathbb{C}$ is determined entirely by $s(1)$, and so there is a one-to-one correspondence between *scalars* and elements of $\mathbb{C}$. Similarly, a linear transformation $\psi : \mathbb{C} \to \mathcal{H}$ is determined by the value $\psi(1)$, and so each element of a space $\mathcal{H}$ can be thought of as such a transformation.

4.3 Adjoints

At this point we adopt the more common right-to-left compositional convention. Although this is much less natural in general, it is consistent with the Dirac notation and the convention used in linear algebra in general, which is after all the prime motivating example for this entire topic and this section in particular.

If a category is compact closed, then it has a natural isomorphism $A \simeq A^{**}$ which we may assume without loss of generality is the identity.

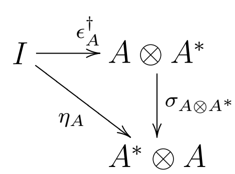
Definition 9. A compact closed category is *strongly* compact closed if the object mapping $A \mapsto A^*$ can be extended to a covariant functor where we denote $f_* : A^* \to B^*$ for $f : A \to B$, satisfying

$$f_{**} = f \qquad (f_*)^* = (f^*)_*$$

Definition 10. In a strongly compact closed category, we define the *adjoint* of a morphism $f : A \to B$ to be $f^\dagger = (f_*)^* : B \to A$.

Proposition 11. *The adjoint* $\dagger$ *defines a dagger in the usual sense as a contravariant involution.*

Proposition 12. *In a strongly compact closed category the following diagram commutes.*



(Indeed, a compact closed category with a dagger satisfying the above is sometimes taken to be the definition of a strongly compact closed category.)

Definition 13. A morphism U is called *unitary* if and only if it is an isomorphism satisfying $U^{-1} = U^{\dagger}$.

Definition 14. The *inner product* of $\psi, \phi : I \to A$ is the scalar defined by $\langle \psi | \phi \rangle = \psi^{\dagger} \phi$.

Proposition 15. *We have* $\left\langle f^{\dagger}\psi | \phi \right\rangle = \langle \psi | f\phi \rangle$ *whenever this expression makes sense. Thus, we can unambiguously define* $\langle \psi | \, f \, | \phi \rangle$ *to be the above.*

Proposition 16. *If* U *is unitary then* $\langle U\psi | U\phi \rangle = \langle \psi | \phi \rangle$.

Proposition 17. *In a category with biproducts, the adjoint* $\dagger$ *is additive, i.e.* $(f+g)^{\dagger} = f^{\dagger} + g^{\dagger}$ *and* $0^{\dagger}_{A,B} = 0_{A,B}$.

We generally want biproducts to behave nicely with the dagger, and so when we talk about a "strongly compact closed category with biproducts" we also require that the coproduct injections $i_j : A_j \to \bigoplus_k A_k$ *satisfy* $i_j^{\dagger} i_k = \delta_{j,k}$.

4.4 Spectral decomposition

The spectral theorem plays an incredibly important role in quantum mechanics, and we can make strides towards generalizing it in this setting.

Definition 18. A *spectral decomposition* of an object A is a unitary isomorphism $U : A \to \bigoplus_k A_k$.

If U is a spectral decomposition as above, then we can define projectors $\mathbf{P}_j = (\pi_j U)^{\dagger} \pi_j U$ which are clearly self-adjoint, and furthermore sum to the identity.

4.5 Bases

We may generalize the concept of a basis as follows.

Definition 19. A *basis* for an object A is a unitary isomorphism $b : nI \to A$.

If A, B have bases b_A, b_B respectively, then for any morphism $f : A \to B$ we have $b_B^{\dagger} f b_A$ a morphism from $n_A I \to n_B I$, and so it admits a matrix representation f_{jk} in these bases. Furthermore, we may prove that the matrix of $f^{\dagger}$ is the conjugate transpose of the matrix of f.

Also, in case A, B have bases, then the definitions of adjoint morphisms and unitary isomorphisms coincide with the usual definitions from linear algebra:

Proposition 20. *If A and B each have a basis, then $g = f^\dagger$ if and only if $\langle f\psi|\phi\rangle = \langle\psi|g\phi\rangle$ for all vectors ψ, ϕ.*

Proposition 21. *If A and B each have a basis, then a morphism U is unitary if and only if $\langle U\psi|U\phi\rangle = \langle\psi|\phi\rangle$ for all vectors ψ, ϕ.*

The above, of course, are usually taken as the *definitions* of these concepts in a Hilbert space.

5 Quantum mechanics

By making the following physical interpretations, we see that the fundamentals of quantum computing can be captured in any strongly compact closed category with biproducts.

1. Each object A is a *state space.*

2. There is an elementary state space Q (a qubit) with a *computational basis* $b_Q : 2I \to Q$.

3. Compound systems are described by tensor products.

4. Data transformations are unitary isomorphisms.

5. A *preparation* of a state space is a morphism $\psi : I \to A$ such that there's a unitary $U : I \oplus B \to A$ with $\psi = Ui_1$.

6. Every spectral decomposition and its projectors

   $$U : A \to \bigoplus_k A_k \qquad \mathbf{P}_j$$

   define a *non-destructive measurement*

   $$\langle \mathbf{P}_j \rangle : A \to nA$$

   where each $\mathbf{P}_j$ is a *measurement branch.*

7. In the special case of a decomposition $U : A \to nI$, we say U itself is a *destructive measurement* or *observation*

   $$\langle \phi_k \rangle : A \to nI$$

where each morphism

$$\phi_k = \pi_k U : A \to I$$

is an *observation branch*.

8. As hinted above, biproducts represent *branching* into many worlds depending on the outcome of a measurement.

9. Distributivity of tensor products over biproducts represents nonlocal, classical *communication*.

Axioms 1–4 should be apparent. The extra condition in axiom 5 (in terms of Hilbert spaces) imposes that we can only prepare nonzero, normalized states (i.e. images of unitary transformations.)

Using this interpretation, Abramsky and Coecke present an abstract (state) teleportation scheme, (gate) teleportation scheme, and entanglement swapping scheme, and prove their correctness. We refer the reader to [1] for the detailed analysis.

6 Conclusions

Abramsky and Coecke's formulation of quantum mechanics certainly captures details completely hidden by the standard, Hilbert space formulation. On the pictorial side, the most striking example of this is the quantum information flow explicitly captured by their approach. Algebraically, their formalism captures the indeterminacy of measurement formally, whereas measurement is treated in a very ad hoc manner in the usual Hilbert space formulation.

However, we also observe shortcomings: despite Abramsy and Coecke's claims that protocols like teleportation are almost trivial in their formalism, only the naive presentations are simple. The complete proofs of correctness of their abstract schemes are no shorter than the standard, Hilbert space proofs, and in many nontrivial ways *more* complicated. Their formalism certainly allows for much easier intuitive understanding of the schemes, but this comes at the cost of working within an incredibly rigorous system.

References

[1] S. Abramsky and B. Coecke, "A categorical semantics of quantum protocols," 2004. [Online]. Available: http://arxiv.org/abs/quant-ph/0402130v5

[2] ——, "Categorical quantum mechanics," 2008. [Online]. Available: http://arxiv.org/abs/0808.1023

[3] B. Coecke, "Kindergarten quantum mechanics," 2005. [Online]. Available: http://arxiv.org/abs/quant-ph/0510032

[4] P. Selinger, "Towards a quantum programming language," *Mathematical Structures in Computer Science*, vol. 14, no. 04, pp. 527–586, 2004.

[5] ——, "Dagger compact closed categories and completely positive maps," *Electron. Notes Theor. Comput. Sci.*, vol. 170, pp. 139–163, 2007.