Department of Computer Science

A note on interlaced quantum teleportation

Brendan Fong

CS-RR-14-09

Department of Computer Science, University of Oxford
Wolfson Building, Parks Road, Oxford, OX1 3QD

A note on interlaced quantum teleportation

Brendan Fong

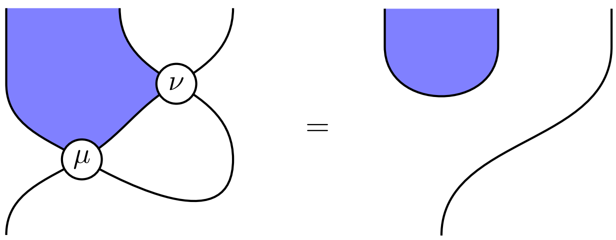
December 17, 2014

Abstract

In Higher Quantum Theory [2], Vicary outlines a generalisation of the usual quantum teleportation protocol, based on the idea of interlacing two separate teleportation procedures. We show here that the protocol he specifies is impossible to implement with qubits.

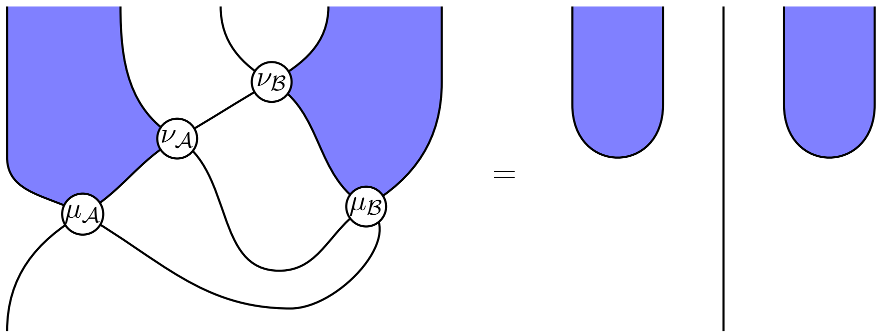
1 Background

An appealing strength of categorical quantum mechanics, initiated by Abramsky and Coecke [1], is that the categorical framework gives a graphical language for expressing quantum operations. Vicary has extended this framework to 2-categories, allowing regions of space that represent classical information [2]. This, to give an example, allows the quantum teleportation protocol to be expressed by the following equality of diagrams, where μ represents measurement with respect to some basis, and ν is a correction corresponding to the measurement outcome:



A feature of this language is that we may then sketch other pictures, led perhaps by our topological intuition, to dream up new quantum protocols. One example of this is interlaced teleportation, in which we interlace two separate teleportation procedures.

The interlaced teleportation protocol is specified by the equality of diagrams:



Our convention here is that diagrams are read from bottom to top. Vicary gives the following interpretation [2, p.38]:

> Step by step, the left-hand side of this equation describes the following procedures.
>
> 1. We begin with a single quantum system S, which we refer to as system 1.
> 2. Four new instances of S are then prepared, referred to as copies 2, 3, 4 and 5, such the pairs (2, 5) and (3, 4) are in a Bell state.
> 3. Copies 1 and 2 of the system are then measured in some multipartite basis $\mathcal{A}$.
> 4. Near simultaneously, copies 4 and 5 are also measured in some multi-partite basis $\mathcal{B}$.
> 5. Copy 3 then has a correction performed on it, depending on the result of the $\mathcal{A}$-basis measurement.
> 6. Finally, another correction is applied to the same qubit, this time depending on the result of the $\mathcal{B}$-basis measurement.
>
> The protocol is successful if this procedure has the same result as that described on the right-hand side of the equation: the initial system S being unaffected, and its state uncorrelated to the results of the two measurements that were performed.

Such a procedure might find application, for example, in storing quantum information such that the presence of two parties is require to retrieve it. The content of this note, however, is that *it is impossible to implement such a procedure with qubits*. I hope such an argument might prove useful in the search for a general characterisation of diagrams of implementable quantum protocols.

2 Proof

Suppose our quantum system S is a qubit. Then we may represent its state space by some two-dimensional complex Hilbert space $\mathcal{H}$. We shall show that it is not possible to find two bases $\mathcal{A}$ and $\mathcal{B}$ for $\mathcal{H} \otimes \mathcal{H}$ that implement the above protocol.

By the Choi-Jamiołkowski isomorphism, we may equivalently show that it is not possible to not possible to find bases $\{A, B, C, D\}$ and $\{S, T, U, V\}$ for the space $\mathcal{U}(\mathcal{H})$ of unitary operators on $\mathcal{H}$ with the property that there exist sets $\{A', B', C', D'\}$ and $\{S', T', U', V'\}$ of unitary operators on $\mathcal{H}$ such that for all $a \in \{A, B, C, D\}$ and all $s \in \{S, T, U, V\}$ we have

$$asa's' = I.$$

The primed operators play the role of the corrections to measurements returning the corresponding unprimed basis operator.

Suppose for the sake of contradiction that such sets of operators exist. As the sets $\{A, B, C, D\}$ and $\{S, T, U, V\}$ form bases for $\mathcal{U}(\mathcal{H})$, there exist $\lambda_a, \lambda_s \in \mathbb{C}$ such that $\sum_a \lambda_a a = I$ and $\sum_s \lambda_s s = I$. Noting that for all a, s we have $asa' = s'^{\dagger}$, we see that we may write

$$aa' = a\left(\sum_s \lambda_s s\right)a' = \sum_s \lambda_s asa' = \sum_s \lambda_s s'^{\dagger}.$$

Write also $U = aa'$, and note that for all a we have $a' = a^{\dagger}U$.

Conjugating $asa's' = I$ by s', we have $s'asa' = I$. As previously, this gives

$$s's = s'\left(\sum_a \lambda_a a\right)s = \sum_a \lambda_a s'as = \sum_a \lambda_a a'^{\dagger},$$

and continuing with our newly-defined operator U we arrive at

$$s's = \sum_a \lambda_a (a^{\dagger}U)^{\dagger} = \sum_a \lambda_a U^{\dagger}a = U^{\dagger}\sum_a \lambda_a a = U^{\dagger}.$$

In particular, we have now shown that $s' = U^{\dagger}s^{\dagger}$.

From this we can conclude that

$$asa^{\dagger}s^{\dagger} = asa^{\dagger}UU^{\dagger}s^{\dagger} = asa's' = I,$$

and hence that for all a and s, a and s commute. But as the s form a basis for $\mathcal{U}(\mathcal{H})$, this shows that each operator a lies in the centre of $\mathcal{U}(\mathcal{H})$, and hence is a scalar multiple of I. Thus the operators $a \in \{A, B, C, D\}$ cannot form a basis for $\mathcal{U}(\mathcal{H})$—a contradiction.

Acknowledgements

I thank Jamie Vicary for suggesting this problem, and for providing the TikZ code for the diagrams used in this paper.

References

[1] S. Abramsky and B. Coecke, A categorical semantics of quantum protocols, in *Proceedings of the 19th IEEE Conference on Logic in Computer Science (LiCS-04)*, IEEE Computer Science Press, 2004. Also available as arXiv:quant-ph/0402130.

[2] J. Vicary, Higher quantum theory, 2012. Available as arXiv:1207.4563.

[3] J. Vicary, Higher semantics for quantum protocols, in *Proceedings of the 27th Annual ACM/IEEE Symposium on Logic in Computer Science (LiCS-12)*, IEEE Computer Science Press, 2012.