High-Level Methods for Quantum Computation and Information

Samson Abramsky
Oxford University Computing Laboratory

1. Background

Quantum information and computation is concerned with the use of quantum-mechanical systems to carry out computational and information-processing tasks [18]. In the few short years that this approach has been studied, a number of remarkable concepts and results have emerged, most notably:

- A couple of spectacular algorithms — Shor's polynomial-time algorithm for prime factorization [23] and Grover's sub-linear search algorithm [14].

- A number of information protocols, exemplified by *quantum teleportation*, which exploit quantum entanglement in an essential fashion. We give a thumbnail sketch of teleportation here, since it may be less familiar, and it will serve as a useful motivating example. Teleportation uses just two classical bits to transport an unknown qubit q from one site to another. Since a qubit is specified by an arbitrary pair of complex numbers (α, β) satisfying $|\alpha|^2 + |\beta|^2 = 1$, achieving this information transfer with just two classical bits is no mean feat! It is accomplished by using an entangled pair q_A, q_B of qubits, one held at the source site A and one at the target B, as a 'quantum information channel', and using a measurement performed on q and q_A at A to cause a 'collapse' in q_B at B. The two classical bits are used to tell the target site B what the outcome of the measurement performed at A was; a 'correction' operation can then be performed at B, after which the state of q_B will be equal to the original state of q. (Because of the measurement, the input qubit no longer has this state — the information in the source has been 'destroyed' in transferring it to the target).

Teleportation is simply the most basic of a family of quantum protocols, including *logic-gate teleportation* [13], *entanglement swapping* [27], and *quantum key exchange* [12], which form the basis for novel and potentially very important applications to secure and fault-tolerant communication and computation [8, 13, 18, 19, 24].

The need for high-level methods

The current tools available for developing quantum algorithms and protocols are deficient on two main levels.

- Firstly, they are too *low-level*. Quantum algorithms are currently mainly described using the 'network model' corresponding to circuits in classical computation. One finds a plethora of ad hoc calculations with 'bras' and 'kets', normalizing constants, matrices etc. The arguments for the benefits of a high-level, conceptual approach to designing, programming and reasoning about quantum computational systems are just as compelling as for classical computation. Moreover, there is the whole issue of integrating quantum and classical features, which would surely be mandatory in any practicable system.

- At a more fundamental level, the standard mathematical framework for quantum mechanics (which is essentially due to von Neumann [17]) is actually *insufficiently comprehensive* for informatic purposes. In describing a protocol such as teleportation, or any quantum process in which *the outcome of a measurement is used to determine subsequent actions*, the von Neumann formalism does not capture the flow of information from the classical or macroscopic level, where the results of measurements of the quantum-mechanical system are recorded, back to the quantum level. This flow, and the accompanying use of 'classical information', which plays a key role in protocols such as teleportation, must therefore be handled informally. As quantum protocols and computations grow more elaborate and complex, this point is likely to prove of increasing importance.

2. Recent Progress

In joint work with Bob Coecke, reported in this Conference Proceedings [3], we have recently made some striking progress in addressing both these points. We have recast the von Neumann formalism at a more abstract and conceptual level, using category theory. This enables a high-level but effective approach to modelling and reasoning about the key features of quantum information processing, including preparation and measurement of entangled states, unitary operations and classical communication. The effectiveness of these methods is shown by the detailed treatment given in [3] of three of the main quantum protocols: teleportation, logic-gate teleportation (which is universal for quantum computation), and entanglement swapping. Because of the explicit treatment of 'classical communication' — *i.e.* the use of measurement outcomes to determine subsequent actions, possibly elsewhere in a compound system than the site at which the measurement was performed — it can reasonably be claimed that these are the *first* completely formal descriptions and proofs of correctness of these protocols. Moreover, the correctness proofs are themselves at a high level, using (and re-using) key structural lemmas which are valid in wide generality.

One of the main results in [3] is a complete formal description—including the classical communication— of the teleportation protocol within a purely categorical semantics. This semantics is sufficiently strong to prove correctness of the protocol.

Consider the following diagram:

$$\begin{tikzcd}
Q \arrow[r, equal] \arrow[ddddd, "\langle 1\rangle_{i=1}^{i=4}"'] & Q \arrow[d, "(1\otimes\eta)\circ\rho"', "\textbf{produce EPR-pair}"] \\
& Q\otimes(Q_A^*\otimes Q_B) \arrow[d, "\alpha"', "\textbf{spatial relocation}"] \\
& (Q\otimes Q_A^*)\otimes Q_B \arrow[d, "\langle \llcorner U_i \lrcorner\rangle_{i=1}^{i=4}\otimes 1"', "\textbf{measurement}"] \\
& (4\cdot \mathrm{I})\otimes Q_B \arrow[d, "(4\cdot\lambda^{-1})\circ\upsilon"', "\textbf{classical communication}"] \\
& 4\cdot Q_B \arrow[d, "\bigoplus_{i=1}^{i=4} U_i^{-1}"', "\textbf{unitary correction}"] \\
4\cdot Q_B \arrow[r, equal] & 4\cdot Q_B
\end{tikzcd}$$

Here Q, Q_A and Q_B are all instances of a qubit object, I is the tensor unit, and $n \cdot A$ is the biproduct of n copies of A. The natural isomorphisms are $\rho : Q \simeq Q \otimes \mathrm{I}$, $\lambda : Q \simeq \mathrm{I} \otimes Q$, 'associativity' α and 'distributivity' υ of tensor $\otimes$ over biproduct $\oplus$. The morphism $\eta : \mathrm{I} \to Q^* \otimes Q$ is the unit of compact closure, that is the 'name' of $1_Q : Q \to Q$, and represents preparation of the EPR state [18], while $\llcorner U_i \lrcorner : Q \otimes Q^* \to \mathrm{I}$ is the 'coname' of U_i, and the tupling $\langle \llcorner U_i \lrcorner \rangle_{i=1}^{i=4}$ represents a Bell-base measurement [18].

The right-hand-side of the diagram gives a complete description of the teleportation protocol, while the left-hand-side expresses the intended behaviour (copying the qubit from Q to Q_B). The proof of correctness, that is the commutativity of the diagram, can be found in [3].

The abstract setting is that of *strongly compact closed categories with biproducts*. Any such category allows us define abstract counterparts to the basic ingredients of quantum mechanics such as measurement and unitary data transformation, and to add to that a description of classical communication.

Conceptually:

- the tensor product $\otimes$ of the monoidal structure allows compound systems to be described;
- the compact closed structure (cf. 'names' and 'conames') allows preparations and measurements of entangled states to be represented, *and their key properties to be proved*;
- the biproducts allows measurements, branching on measurement outcomes, superpositions, and classical communication (using distributivity of tensor over biproduct) to be captured.

Although these axioms are all structural, and seem purely 'qualitative', in fact they suffice to yield good notions of 'scalars', 'probability amplitudes', and the *Born rule*—the key quantitative feature of quantum mechanics.

Entanglement as information flow. A key part of our work is the analysis of the information flow inherent in entanglement, which exploits the compact closed structure. In the above commutative diagram for teleportation, note that the measurement is formed by tupling the *conames* $\llcorner U_i \lrcorner$ of (the inverses of) the unitary correction operators U_i^{-1}. This makes visible the structure underlying the apparently ad hoc juggling with Bell bases and unitary matrices in the standard presentations. The flow along each 'branch' as we follow the possible measurement outcomes can then be analyzed using general algebraic properties of compact closed categories. See [3] for details, and also [9, 10] for an extended account at a more concrete level, with many diagrams and examples.

3. Some Further Developments

We survey some promising further developments we are currently pursuing.

Categorical quantum logic. Although the work in [3] is not presented in logical terms, the well-established paradigm of categorical logic and proof theory is directly applicable, and leads to another perspective, and some potentially very useful syntactic methods. In particular, my student Ross Duncan and I are currently studying a notion of *proof nets* for compact closed categories with biproducts. This builds on the seminal study by Kelly and Laplaza of coherence for compact closed categories [16], to yield an amenable graphical proof theory corresponding to the categorical semantics in [3]. This offers the prospect that the correctness proofs in [3] can be performed automatically by *cut-elimination*. Duncan is building an experimental implementation of proof nets, and we intend to use it to perform some of these computations.

Since the quantitative features of quantum mechanics (scalars, the Born rule etc.) are also captured in the categorical semantics in [3], it seems that one can obtain an interesting and applicable diagrammatic tool for automating a class of 'structural calculations' in quantum informatics.

Transformations for parallelism and fault-tolerance. In [9, 10], Coecke uses the Logic of Entanglement setting, which is now subsumed by the more general categorical semantics in [3], to give a 'compilation scheme' for quantum networks into a special, highly parallel form. (A similar compilation is carried out by Duncan in [11], using the proof-net formalism.) This parallel form, which avoids reuse of outputs from quantum gates, is particularly attractive because of its *fault-tolerance properties*; these have been emphasized in the influential work of Shor [24] and Preskill [19]. We aim to pursue these ideas, and more generally to see how our powerful algebraic methods can be applied to yield useful program transformations for quantum circuits and other computational systems. The situation is quite analogous to that in standard program transformation and hardware design and verification, where categorical methods have been applied with considerable success [7, 15].

The One-Way Quantum Computation Model. The 'one-way' or 'measurement-based' model [20, 21] has been proposed recently as an alternative to the standard 'network model' of quantum circuits. In the one-way model, the computation starts from an initially prepared entangled state (a 'cluster state'), which consists of entangled qubits laid out on a 2-D grid, or more generally a graph. Computation proceeds by performing measurements on these qubits. In general, these have to be combined with unitary corrections. Thus the arrangement generalizes that of teleportation. This model is seen as promising because of its good properties as regards modularity and fault-tolerance.

The full expressive power of the model has yet to be explored; it may well offer new possibilities going beyond the standard network model (which it has been shown can be represented within it).

The categorical semantics in [3] seems well adapted to study the one-way model. In fact, the key modularity property of the one-way model appears to fall out as a consequence of one of our general algebraic results — which in turn corresponds to the soundness of Cut-elimination in the categorical logic approach described above. Our aim here will be to explore how our methods can be used to give an analytical description of the one-way model, and how this relates to current methods based on the stabiliser formalism [18]. We believe that our algebraic approach will lead to simpler and more tractable descriptions of this model, and more insight into its expressive power.

Multipartite entanglement. The methods and results in [3] give a comprehensive semantic and logical analysis of bipartite entanglement. The situation with multipartite entanglement — several qubits or other quantum systems mutually entangled — is less clear. It seems that some of the relevant structure will be addressed by our categorical logic and semantics, since we can represent compound quantum systems of any degree, arbitrary (linear) functional dependencies, etc. Whether this suffices to address all significant forms of multipartite entanglement remains to be investigated. This is an area which is generally agreed to be both important and very poorly understood currently, so if logical methods do gain some traction this would have considerable impact.

Foundational issues. There are numerous important and promising ideas which arise in seeking to extend and strengthen the categorical foundations established in [3]. Firstly, the discussion in [3] is limited to *Finitary Quantum Mechanics*, in which only finite-dimensional 'spaces' (concrete or abstract), corresponding to observables with finite spectra, are considered. A first step towards the general case has already been taken in the previous work by Abramsky, Blute and Panangaden on Nuclear ideals [1], which shows how to lift the compact closed arguments to the general case. However, a proper treatment of observables with continuous spectra is challenging. We have started collaborative work with Rick Blute and Prakash Panangaden on this topic.

Another important issue is to see how far our general and axiomatic approach can be exploited to yield insights into the degrees of freedom in quantum mechanics, and to what extent the structure is *forced* by various information-theoretic principles. We have already shown in [3] how a kind of 'reverse mathematics' applies, in which one can show what requirements are placed on the ambient category in order for protocols such as teleportation to be expressed. We will also look at possible weakenings of the axioms, and how much quantum information processing can still be carried out in weaker settings.

4. Does Quantum Informatics belong in LiCS?

I conclude by addressing a question which does seem to arise for some members of the LiCS community. In fact, a similar issue seems to arise whenever a new topic first appears in LiCS. Some would like to leave probabilistic computation to the probabilists; real-number computation to the numerical analysts; hybrid systems to the control engineers; quantum informatics to the physicists; computational biology to the biologists. In my view, this attitude is profoundly misguided.

A Personal View

Computer Science, and more particularly the LiCS community, has something important and distinctive to bring to the table, which can lead to fruitful interactions with a wide range of scientific disciplines. This is clear enough for 'Track A theory' — algorithms and complexity. It is important — and for LiCS vital — to insist that it holds no less for 'Track B theory' — semantics and logic. What 'Track B' has to offer, above all, it seems to me, is the paradigm of *compositional syntax and semantics*, with the accompanying idea of working at different levels of abstraction, and explicitly relating these levels. The classical modelling paradigms in the physical and biological sciences (and economic modelling too, for that matter) are generally *monolithic* in nature, for all the formidable ingenuity and mathematical depth which has gone into their development.

The great opportunity for Computer Science is to spread these ideas of compositionality and abstraction outwards into these disciplines. If we do this well, then we may elevate our field into a universal substrate for science alongside mathematics. If we fail to grasp this opportunity, we may be left behind as a rump discipline, a disregarded remnant.

The signs for our field as a whole seem to me encouraging. And these emerging new developments are well represented at the Affiliated Workshops at this meeting. The challenge for LiCs is to respond to, and indeed take the lead in, these activities, while retaining its identity. We live in interesting times!

References

[1] S. Abramsky, R. Blute, and P. Panangaden. Nuclear and trace ideals in tensored ∗-categories. *Journal of Pure and Applied Algebra* **143**, 3–47 (1999).

[2] S. Abramsky and B. Coecke. Physical traces: classical vs. quantum information processing. *Electronic notes on Theoretical Computer Science* **69** (2003) – CTCS'02 issue. `arXiv:cs/0207057`

[3] S. Abramsky and B. Coecke. A categorical semantics of quantum protocols. *Proceedings of 19th Annual IEEE Symposium on Logic in Computer Science* (LiCS'04). `arXiv:quant-ph/0402130`[1]

[4] S. Abramsky, S. J. Gay and R. Nagarajan. Interaction categories and foundations of typed concurrent programming. *Deductive Program Design: Proceedings of the 1994 Marktoberdorf International Summer School*, pp. 35–113. NATO ASI Series F, Springer-Verlag, 1995.

[5] J. Baez. Quantum Quandaries: A Category-Theoretic Perspective. To appear in *Structural Foundations of Quantum Gravity*, ed. S. French, D. Rickles and J. Sahatsi, Oxford University Press. Available at `http://math.ucr.edu/home/baez/quantum/`.

[6] C. H. Bennett, C. Brassard, C. Crépeau, R. Jozsa, A. Peres and W. K. Wooters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters* **70**, 1895–1899 (1993).

[7] R. S. Bird and O. de Moor. *Algebra of Programming*. Prentice-Hall International, 1996.

[8] D. Bouwmeester, A. Ekert and A. Zeilinger. *The Physics of Quantum Information*. Springer-Verlag, 2001.

[9] B. Coecke. The Logic of entanglement. An invitation. PRG-RR-03-12 Oxford University Computing Laboratory. `http://web.comlab.ox.ac.uk/oucl/publications/tr/rr-03-12.html`.

[10] B. Coecke. The logic of entanglement. `arXiv:quant- ph/0402014`

[11] R. Duncan. D.Phil. thesis transfer report. Oxford University Computing Laboratory, 2004.

[12] A. K. Ekert, Quantum cryptography based on Bell's theorem. *Physical Review Letters* **67**, 661–663 (1991).

[13] D. Gottesman and I. L. Chuang. Quantum teleportation is a universal computational primitive. *Nature* **402**, 390–393 (1999). `arXiv:quant-ph/9908010`

[1] Papers posted on the physics `arXiv`'s are downloadable at the address `www.arXiv.org/`*name* e.g. `www.arXiv.org/quant-ph/0402130`.

[14] L. K. Grover. Quantum mechanics helps in searching for a needle in a haystack. *Physical Review Letters* **79**, 325–328 (1997).

[15] G. Jones and M. Sheeran. Circuit design in Ruby. *Formal methods for VLSI design*, ed. J. Staunstrup, 13–70, Elsevier, 1993.

[16] G. M. Kelly. and M. L. Laplaza. Coherence for compact closed categories. *Journal of Pure and Applied Algebra* **19**, 193–213 (1980).

[17] J. von Neumann. *Mathematische Grundlagen der Quantenmechanik*. Springer–Verlag, 1932. English translation: *Mathematical Foundations of Quantum Mechanics*. Princeton University Press, 1955.

[18] M. A. Nielsen and L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[19] J. Preskill. Reliable quantum Computers. `arXiv:quant-ph/9705031`

[20] R. Raussendorf and H. J. Briegel. Computational model for the one-way quantum computer: concepts and summary. `arXiv:quant-ph/0207183`

[21] R. Raussendorf, D. E. Browne and H. J. Briegel. Measurement-based quantum computation on cluster states. `arXiv:quant-ph/0301052`

[22] P. Selinger. Towards a quantum programming language. *Mathematical Structures in Computer Science*. To appear.

[23] P. W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science*, pp. 124–134. IEEE Computer Society Press, 1994.

[24] P. W. Shor. Fault-tolerant quantum computation. *Proceedings of the 37nd Annual Symposium on Foundations of Computer Science*, pp. 56–65. IEEE Computer Society Press, 1996. `arXiv:quant-ph/9605011`

[25] A. van Tonder. Quantum computation, categorical semantics, and linear logic. `arXiv:quant-ph/0312174`

[26] W. Wootters and W. Zurek. A single quantum cannot be cloned. *Nature* **299**, 802–803 (1982).

[27] M. Żukowski, A. Zeilinger, M. A. Horne and A. K. Ekert. 'Event-ready-detectors' Bell experiment via entanglement swapping. *Physical Review Letters* **71**, 4287–4290 (1993).