

Hybrid Hypercomputing: Towards a Unification of Quantum and Classical Computation

CLARE HORSMAN AND WILLIAM J. MUNRO

Hewlett-Packard Laboratories, Filton Road, Bristol BS34 8HZ

Received: June 08, 2009. Accepted: May 12, 2010

We investigate the computational power and unified resource use of hybrid quantum-classical computations, such as teleportation and measurement-based computing. We introduce a physically causal and local graphical calculus for quantum information theory, which enables high-level intuitive reasoning about quantum information processes. The graphical calculus defines a local information flow in a computation which satisfies conditions for physical causality. We show how quantum and classical processing units can now be formally integrated, and give an analysis of the joint resources used in a typical measurement-based computation. Finally, we discuss how this picture may be used to give a high-level unified model for hybrid quantum computing.

Keywords: Quantum computing, foundations of quantum mechanics, locality, graphical calculus

1 INTRODUCTION

The standard approach to quantum computing treats quantum and classical information processing and communication as essentially two separate systems. Quantum and classical computations are described using different formalisms, and consume separate resources. While they are frequently combined, for example in protocols such as teleportation [4] and dense coding [5] the interface between them is at best not formalised and at worst entirely obscured by standard presentations. Some ‘translation rules’ exist between quantum and classical [19, ch1], and we can formally define the complexity

of specific quantum algorithms compared to their classical counterparts [6], but we still lack an underlying model of computation and resources for both that would enable direct comparisons to be made. It is even the case (although often overlooked) that the lack of a proof for the extended Church-Turing thesis means that it is still an open question whether quantum computers are in fact significantly more powerful than classical computers [3]. Given the potentially important applications of quantum computing methods in areas such as cryptography and quantum simulation [14, 1], it is actually a significant question whether we should deploy our resources to implement them by physically building quantum computers, or by investigating new classical algorithms to run on current hardware. Without a unified framework for quantum and classical computations, it is hard to see how we could begin to answer questions such as this with any degree of certainty.

The problem becomes particularly acute when we consider hybrid computing schemes such as measurement-based quantum computing, where the feed-forward of classical measurement results is an integral part of the quantum design [22, 9]. Consideration of the resources used during such a computation tends to concentrate solely on the quantum resources required (generally in the form of a cluster state [21]), with classical measurement and communication being taken as essentially resource-free. This leaves open problems both of the resources required to physically implement these computations, and also fundamental questions on the computability power of such algorithms. Further problems arise if we consider hybrid cryptographic schemes where formally provable security is desired. The lack of formal links between the quantum and classical elements gives a potential area of uncertainty in the security proofs for such systems.

In this paper we present a candidate for a framework in which to analyse hybrid computation by fully integrating the quantum and classical resources and processes used. This takes the form of a graphical calculus based on the logical Heisenberg picture [15, 12, 17], closely related to the stabilizer formalism that is typically used to describe measurement-based quantum computation [8]. The framework integrates quantum and classical elements directly, and gives an intuitively simple set of formally exact reasoning tools for hybrid information theory. There is a local flow of information, enabling data to be tracked causally through a computation, including through what are typically considered to be simply ‘classical’ communication channels. Furthermore, this flow satisfies all reasonable assumptions of causality in physical systems, such as one-way action in time. We will find that this framework enables us to describe the resource use of a measurement-based computation in terms of a single set of resources, and gives us a much clearer idea both of the physical processes taking place during the computation and the logical dependency structure of various algorithms. We will finish by discussing how the framework may be abstracted to give us a formal computability model for hybrid computation.

2 QUANTUM INFORMATION PROCESSING

The basic component of a quantum information processing system is a two-level quantum state called a quantum bit or qubit. As with classical two-level systems (bits) the levels are usually denoted as the computational ‘0’ and ‘1’, and a measurement of a qubit in the computational basis will return one of these values with a probability depending on the quantum state. Unlike classical bits, however, outside a measurement context a qubit can be in a ‘mixture’ of the 0 and 1 states (which are written $|0\rangle$ and $|1\rangle$), called a *superposition*. Qubits can also maintain correlations that are stronger than those accessible to classical systems, known as *entanglement*. Entanglement can be thought of as ‘spatially extended’ superposition: the joint state of, for example, a system of two qubits is in a superposition, which then gives rise to entanglement between the qubits individually.

Quantum computations are significantly more sensitive to the resources required to complete them than their classical counterparts. Classical information can be freely read, duplicated and deleted; for example, if two copies of a bit are required for an algorithm, a single one can be created and then cloned. By contrast, quantum information is subject to strict theorems on *no cloning* and *no deleting* [24, 20]. No cloning states that we cannot start with a qubit in a given quantum state, interact it with another, and then come out with two copies of the original state (this does not, of course, preclude two qubits being *prepared* in the same, known, state). No deleting is the reverse process: we cannot take a given qubit and change its state using only unitary evolution (that is, quantum evolution without classical measurement) to a ‘blank’ state without transferring the state information elsewhere. These results are for general quantum states; there are specific states which can be cloned and deleted, which however turn out to be indistinguishable from classical ‘bit’ states. Both no cloning and no deleting are closely related to the readability problem for quantum information: in general, measuring the state of a qubit changes it (it will, in general, change from a superposition to a definite value). This again contrasts with classical bits which can be easily read without destruction of their state.

Using these building blocks, information processing in quantum systems can be categorised broadly into reversible and irreversible computations, dependent crucially on the ordering of quantum and classical elements in the process. Reversible computations use unitary gates acting on coherent quantum systems throughout the computation, with only the final readout of the process result yielding classical data. This has traditionally been the framework used for quantum computing, and includes the circuit and quantum walks models [11, 23]. By contrast, the more recently-devised method of measurement-based quantum computing (MBQC) includes irreversible measurements and classical data during the computation itself as well as for the readout. A coherent and highly-entangled quantum state called a *cluster state*

is prepared at the beginning of the computation, and then the algorithm is implemented through a time-ordered pattern of measurements on individual qubits or qubit blocks. The exact type of future measurements in the algorithm will depend on the outcome of previous measurements on the cluster. At the end of the process the entanglement in the cluster state has been used up (it is therefore considered to be the resource of the computation), and the result is read out from previously-designated ‘output’ elements of the original cluster.

One fundamental measurement-based protocol that we will use frequently (although historically pre-dating the development of MBQC) is teleportation. In teleportation, a qubit in an unknown state is transmitted using two bits of classical information and previously shared entanglement. Essentially the quantum state is converted to classical data, transmitted, and then converted back to quantum, within the framework of two shared entangled qubits. Various teleportation-type schemes are often found in measurement-based computations, as a way of transferring a quantum state (including its entanglement properties) from one part of the cluster to another.

3 QUANTUM MECHANICS IN PICTURES

There has recently been a significant amount of research into graphical calculi for information flow in quantum processes. This has largely centred on the category-theoretic work of Coecke and Abramsky [2, 10]. The calculi abstract out the structure of quantum information processes, and present a high-level framework for reasoning about information flow in systems, generally containing both bits and qubits. There is now a considerable menagerie of diagrammatic representations for the mathematical structure of quantum mechanics (eg. [16, 13]), and it is with some trepidation that we intend to advance yet another. The difference lies in the perspective from which the present calculus has been developed. Previous diagrammatic representations have concentrated on the mathematical, logical and information-theoretic structures of information flow. The present work is concerned rather with the *physical* and *causal* flows of information during quantum computation. These two broad areas are by no means mutually exclusive, but are sufficiently dissimilar to cause difficulties if one attempts to answer questions of interest to one using the representations of the other. A particular example of this comes in the Coecke and Abramsky calculus where there are logical information flows that travel backwards in time. If we want to ask about how information *physically* gets between points in a computation, then such a flow picture will present serious problems. This present calculus has been developed specifically from such a “physics” rather than “computer science” perspective, with the hope of adding to our integrated understanding of the logical and physical nature of quantum information processing.

3.1 The logical Heisenberg formalism

We will first describe the formalism of quantum theory on which the graphical calculus will be based. This is a Heisenberg-picture formulation of quantum mechanics, where operators rather than states give the evolution of a system. The formalism is mathematically entirely equivalent to more standard pictures of quantum mechanics, the only difference being that there is no non-unitary evolution within the system. It was developed by Deutsch and Hayden following Gottesman [15, 12, 17], and can be viewed as a generalised form of Gottesman's stabilizer theory. The basics of this formalism are the Hilbert-Schmidt space *descriptors* for each qubit, from which we can generate the set of all operators on that qubit. These are the Heisenberg operators which track the evolution of the qubit systems through the computation. The initial state for descriptors is defined as the $|0\rangle$ (unentangled) state, which for qubit a in an n -qubit system is written

$$\mathbf{q}_a = \begin{pmatrix} q_{ax} \\ q_{az} \end{pmatrix} = \mathbb{1}^{\otimes n-a} \otimes \begin{pmatrix} \sigma_x \\ \sigma_z \end{pmatrix} \otimes \mathbb{1}^{\otimes a-1}$$

(In its fullest form we should also have a y -component to \mathbf{q}_a , but it is not independent of the other components: $q_{ay} = q_{ax}q_{az}$. We therefore do not need to track it separately).

The descriptor formalism is unique in quantum mechanics in that the individual qubit descriptors contain locally all the information available to any joint system

$$q_{abij} = q_{ai} q_{bj}$$

The descriptors evolve only when the specific qubit is subjected to a (single- or multiple-qubit) gate, so remote operations do not change the qubit. Some useful single-qubit gates are the NOT gate,

$$\mathbf{q}(t_1) = \begin{pmatrix} q_x(t) \\ -q_z(t) \end{pmatrix}$$

and the Hadamard, which in the Schrödinger picture acts as

$$\begin{aligned} |0\rangle &\rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |1\rangle &\rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned}$$

and in descriptor terms is written

$$\mathbf{q}(t_1) = \begin{pmatrix} q_z(t) \\ q_x(t) \end{pmatrix}$$

Another example of a frequently used gate is the controlled-NOT (CNOT) operation between two qubits. A CNOT operation between a control and target qubit performs a NOT on the target if the control is 1, and does nothing if the control is 0. In the descriptor formalism this is written

$$\begin{aligned} \mathbf{q}_1(t_1) &= \begin{pmatrix} q_{1x}(t) & q_{2x}(t) \\ & q_{1z}(t) \end{pmatrix} \\ \mathbf{q}_2(t_1) &= \begin{pmatrix} q_{2x}(t) \\ q_{1z}(t) & q_{2z}(t) \end{pmatrix} \end{aligned} \quad (1)$$

Entanglement in this formalism is given by a non-trivial dependency of a descriptor outside the space that it occupied at time t_0 [18].

The relationship with the standard, Schrödinger, formalism of quantum mechanics is given most easily through the density matrix, which can be written for two qubits as

$$\rho_{12} = \sum_{i,j=0}^3 \langle q_{1i} q_{2j} \rangle \sigma_i \otimes \sigma_j \quad (2)$$

where $q_{ay} = q_{ax} q_{az}$.

We can use this relation with the density matrix to simplify the formalism from this rather unwieldy state. We can see from (2) that in terms of measurement outcomes, it is the expected values of the descriptors which are important. These expectation values in (2) are defined with respect to the fixed Heisenberg state $|0\rangle$, which for the Pauli operators gives

$$\langle \sigma_x \rangle = \langle 0 | \sigma_x | 0 \rangle = \langle \sigma_y \rangle = 0, \quad \langle \sigma_z \rangle = \langle \mathbb{1} \rangle = 1$$

Recalling the property of the Pauli operators that $\sigma_i \sigma_j = \epsilon_{ijk} \sigma_k$ for $i, j, k \in \{0, 1, 2, 3\}$ (where ϵ_{ijk} is the Levi-Civita symbol), we therefore have the relations

$$\left\langle \sum_{ijkl} (a_i \sigma_x) (b_j \sigma_y) (c_k \sigma_z) (d_l \mathbb{1}) \right\rangle = \left\langle \sum_{ijkl} (a_i \sigma_x) (b_j \sigma_x) (c_k \mathbb{1}) (d_l \mathbb{1}) \right\rangle$$

This means that we do not need separate σ_y or σ_z operators in the description – wherever they occur, they can be replaced by σ_x and $\mathbb{1}$ respectively, without changing any of the current or future predictions of the formalism.

These are now all the elements that are needed to transfer to a graphical calculus. There is an isomorphism between the formalism described and the calculus we will give in the next section, so that anything proven using the calculus can also be proven in the Deutsch-Hayden picture. As this is

also isomorphic to the standard quantum formalism, the calculus will form a complete proof net for quantum propositions.

3.2 Yet another graphical calculus

From the previous section we can pick out the elements that we need to translate graphically. The representation has as its basic elements qubits, which have two ‘slots’ representing the x - and z - components of the descriptor. In these slots we need to put representations of our two basic operators, σ_x and $\mathbb{1}$. The representations must satisfy the properties $\sigma_x. \mathbb{1} = \sigma_x$ and $\sigma_x^2 = \mathbb{1}$. As this is a Heisenberg formalism, we start from our initial ‘zero state’ (we can take this by convention to be $|0\rangle$) and evolve from there using gates. A ‘0’ qubit is given by



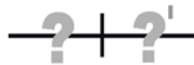
The left side represents q_x and the right q_z . σ_x is given by a triangle, and $\mathbb{1}$ by a space. We can now perform a NOT gate to gain the ‘1’ state of the computational qubit basis. In the descriptor formalism this acts as $q_x \rightarrow q_x$, $q_z \rightarrow -q_z$, so we represent it (time flows from left to right):



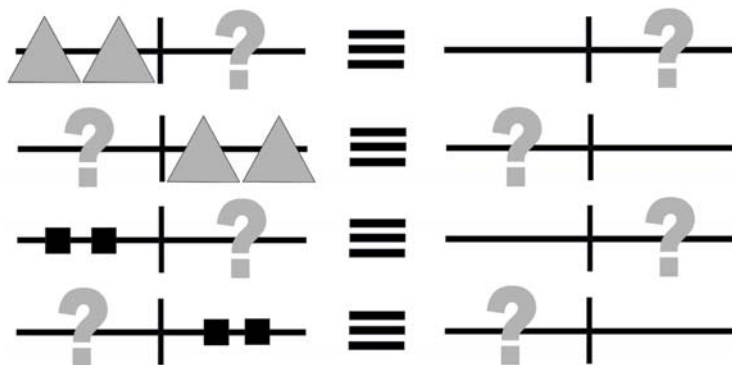
The final single-qubit operation we are interested in is a Hadamard transform, which swaps q_x and q_z components, hence left and right on a qubit:



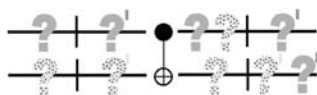
A qubit in an unknown state is represented as



Finally we have composition rules for combining known elements within a qubit. We will represent operators on different subspaces of the full Hilbert space by different colours, so that only triangles of the same colour compose, and different colours commute:



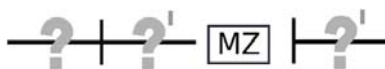
Using two qubits in unknown states we can define the general actions of the two-qubit CNOT gate:



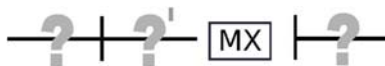
We can look in detail at what's going on here by comparing it with the descriptor formalism (1). A CNOT operation consists of *copying* descriptor dependencies between qubits, with the q_z component of qubit 1 being copied into the q_z component of qubit 2, and the q_x component of qubit 2 copying back into qubit 1. Another copying operation is the controlled-Z (CZ) gate:



We now introduce our representation of classical bits using measurement gates. A measurement in the computational basis is represented



Measurements in other bases are implemented by rotations to the computational basis and then a measurement. One specific useful measurement is that in the X-basis, given by a Hadamard and then a measurement. This is represented as a shorthand by



In operational terms, the bits given by

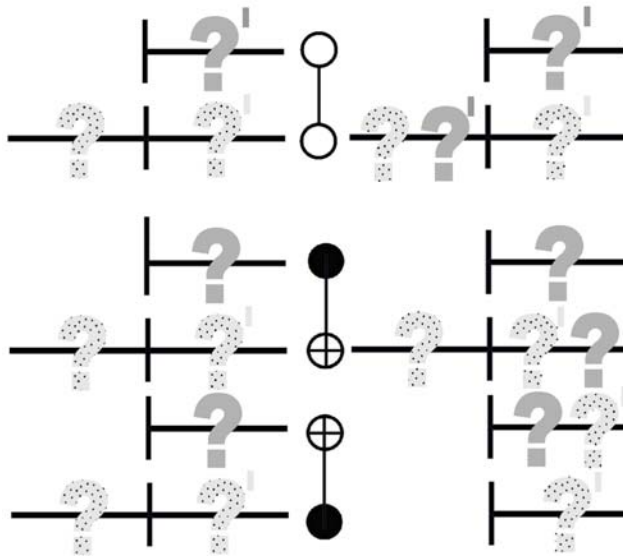


are in a definite state in the measurement basis (0 and 1 respectively). Any bit containing a triangle is in a completely random state.

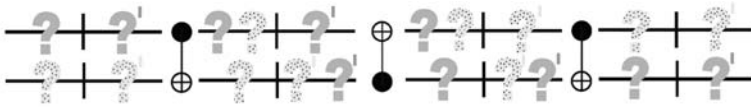
Bits can now participate in the same single-input NOT gate as is used for qubits:



and two-qubit gates can take a mixture of bits and qubits as their inputs:



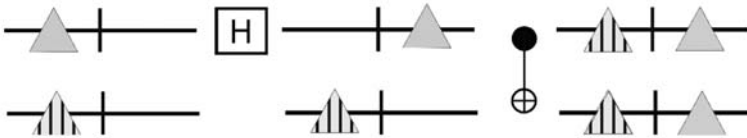
That is now the calculus defined. What we have given is not fully universal for quantum computing as we have do not have a definition for arbitrary single qubit rotation [19, p191]. We do, however, have a full set of Clifford gates which are widely used in measurement-based computing, and give us an interesting subset of quantum computational behaviour. We can now identify the key components of the symmetric monoidal category structure with strong compact closure used by Abramsky and Coecke [2]. The *objects* of the system are the contents of the qubits and bits, that is the positions and quantities of the triangles and the boxes. The gates comprise the *morphisms* between different configurations of the qubit/bit contents, and we can easily see how an *identity* could be defined that corresponds to a $1\mathbb{I}$ gate. We have a *symmetry operation* that swaps the state of the qubits (given by the circuit-model SWAP gate):



It is interesting to consider the structure of compound systems in this representation. In contrast to our usual intuitions about the creation of composite systems in quantum mechanics, in this representation a composite system is given by the simple combination of the constituent systems; there's nothing in the joint system that is not present in the individual ones. It is therefore not immediately obvious that we have a tensor rather than cartesian product structure for compound systems. However, when combining systems we not only need to take into account the individual qubit representations, but also the “triangle” composition rules, which will be important when gates (including measurement) are performed on the joint system. The asymmetry in the composition rules means that unique subsystem states cannot be recovered from a joint system; the correct *associative connective* for the symmetric monoidal category is indeed the tensor product. Finally, the requirement of strong compact closure is satisfied in systems exhibiting teleportation, as will we demonstrate below. We therefore now have all the elements needed for a graphical representation of quantum mechanics.

4 DEPENDENCIES AND ENTANGLEMENT

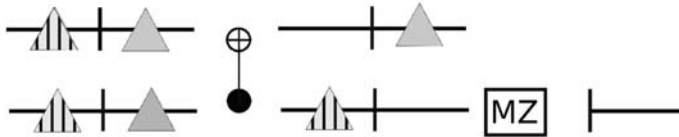
The first important element of quantum computing to consider in this representation is entanglement. As this is the physical outcome of the tensor product structure in quantum mechanics, we can see that it will come from a “triangle” composition. To see this in detail, let us look at an entangling Bell operation:



The first obvious thing to say about this system is that the two qubits finish as identical: each has now incorporated part of the state of the other qubit from the interaction operation. In other words, the state of one qubit now depends on information that it picked up from the other during their mutual interaction. Note that this dependency does not change unless there are local operations performed on that particular qubit; unlike in the standard representation of quantum mechanics, remote operations do not change the state of a qubit.

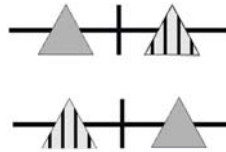
So how precisely are these dependencies encoding the entanglement between qubits? As mentioned above, the key to this is the composition rule

for triangles. Two qubits are entangled if there is a particular joint measurement which gives a different result from the composition of the individual measurements (eg. [19, ch2]). As the presence of any triangle in a bit means a completely random outcome, entanglement is shown by the ability to use the composition rule to annihilate all triangles from at least one joint measurement outcome bit. Taking the above example of the Bell state, we see that all individual measurements on the two qubits will give random bits. However, we can recover a definite bit in the following way by performing the reverse operation:



The true power of the dependencies comes in, however, when they are used to carry information through a computation, and only annihilated at key points. We can see this by turning to arguably the most important measurement-based protocol, teleportation.

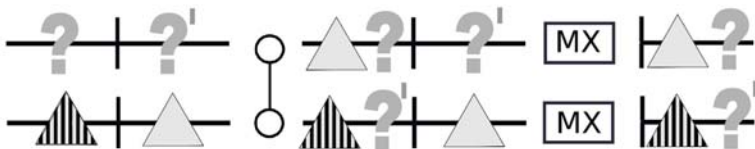
In a teleportation protocol, Alice and Bob begin by sharing a pair of qubits in the state $|01\rangle + |10\rangle$:



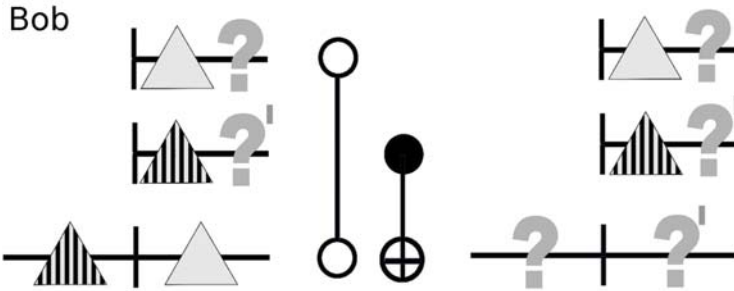
(proof that this is indeed the correct representation of the state is left as an exercise to the interested reader).

Alice and Bob are spatially separate, so we can (in this representation) look only at the qubits and bits local to each. Alice now has a qubit in an unknown state that she wishes to teleport. She entangles this with her half of the shared qubit pair, and then performs two measurements:

Alice



These two bits are then communicated over the intervening distance to Bob, using a classical communication channel. Bob performs two operations between the bits and his half of the original qubit pair, and recovers Alice's teleportation qubit:



One immediate consequence of describing teleportation in this representation is that it ceases to become a non-local operation. The state that Alice is sending to Bob does not disappear at one end and reappear at the other; rather, the data contained in the qubit is split into two bits which are then sent from Alice to Bob. An interesting question then becomes what role the pre-shared entanglement is playing in this picture. In the usual model, the role of the entangled qubits is to create a quantum communication channel. Alice's operation that entangles her half of the pair with the teleportation qubit is considered to change the joint state of the shared qubit pair. Bob can then recover the teleported state if he performs certain operations on his half. The classical communication is only needed to tell Bob which operation to do; it does not, in itself, convey any of the quantum information. By contrast, in this picture Alice's operations do nothing to the state of Bob's qubit: it is only when Bob performs the operations between his qubit and the communicated bits that its state changes. Neither quantum nor classical information or dependencies can travel between two points without something physically carrying them.

Rather than acting as a quantum channel, the role of the shared entanglement instead in this picture is analogous to that of an encryption key. The data to be teleported is composed with the "key" (the red and green triangles), transmitted, and then decoded at the other end. The sharing of an entangled pair of qubits beforehand then becomes a form of *key distribution*: Bob has an exact copy of the key that Alice is using, generated through the entangling operations that produce the original qubit pair. This is shared ahead of time, and enables him to extract the data contained in the bit pair that is communicated between them.

This representation of teleportation also significantly changes the emphasis placed on the final operations performed on his qubit by Bob. On a standard understanding, by this point in the process Alice's operations have changed the state of Bob's qubit into a different definite state. This is the original teleportation state, with an additional 'Pauli correction' [9] (one of four known states). All the classical communication does is tell Bob which correction operation he needs to do in order to recover the teleportation state – *i.e.*

it tells him which of four states he actually has. The correction operation becomes almost an afterthought: Bob has the state, but does not know it yet. The correction operation can therefore be dealt with almost completely informally; the information transmission protocol is complete by that point. In the graphical representation, however, Bob's "correction operations" are the only way in which the teleported information gets to his qubit. These "decoding operations" are of equivalent importance to Alice's "encoding operations", and are entirely integrated into the formalism. This is, in fact, how all such Pauli corrections are represented in the calculus: a Z-correction translates to a CNOT between bit and qubit, and an X-correction is a CZ operation. The feed-forward of classical information therefore becomes an integral part of the *processing* of information in a hybrid computation, rather than what is necessary to read out the results of an already-completed computation.

5 CLASSICAL INFORMATION

We have seen that classical feed-forward looks very different in the graphical representation compared with the usual view. Even at a formal level we have defined CNOT and CZ gates which can take both bits and qubits as inputs. This is simply not possible on the standard view, but emerges completely naturally within the graphical calculus. Because this is so different from the usual view of classical information, we are left with the problem of defining what exactly it is that is being transmitted through the classical channel in this representation. The usual view of the classical data is a single measurement outcome, either a 0 or a 1; a detector either clicks or it does not. How then does this relate to the relatively complex objects that are bits in processes such as the teleportation example above?

The first thing to note when trying to understand the role of the classical channel here is that, in a measurement-based computation, the measurement outcomes are never single outcomes in isolation. Future computational actions are changed dependent on these outcomes, so within the logical structure of the computation they carry with them contextual information. A classical measurement outcome does not just mean "detector X clicks", for example: it means, in context, "detector X clicks, this was caused by state Y, and so operation Z should be performed". This is precisely the interface between the quantum and classical information processing units that is treated informally in standard presentations. As the aim is to fully formalise the entire process, this "informal" data will need to be found within the representation itself, rather than added by hand. There are, then, three elements to the representation: quantum systems and processes, classical systems and processes, and the formal treatment of their interaction within a given protocol.

What we find with the graphical representation is that the contextual algorithm information is formalised by being incorporated into the description of

the classical channel. This makes intuitive sense as this information concerns the function of a particular bit within the process. In logical terms, then, what is represented by the triangles etc. in a classical bit is not only the 0 or 1 of a straightforward measurement on that bit, but also the information about how that bit will interact with the quantum systems to change the future state of the computation. This in turn will depend on previous states of the computation (for example, in teleportation the states of the bits will depend on the state of the qubit that Alice is trying to teleport). So the description of a bit includes not only the results of measurements on that bit itself, but how those measurements depend on the states of the qubits with which it had previously interacted.

In general, these dependencies will not have a significant effect on the outcome of measurements on a bit. However, for certain situations such as teleportation, it is possible to arrange the systems so that the bits interact with qubits which contain identical dependencies. In this case, different data can be extracted from the bit than is possible from individual bit measurements. This is done by making sure there are copies of the dependencies used in the systems with which it will interact – in other words, by pre-sharing entangled qubits.

We can see, then, that the information in the classical channel in this representation fully defines how the bits interact with the qubits. In logical terms, the calculus can be viewed as giving the dependency structure of an algorithm, showing which previous states the future of the computation is dependent on. The representation of classical information therefore also needs to include these dependencies, and to formalise the bit-qubit interaction.

In physical terms, the dependencies carried by the bits have been generated by entanglement. Shared entanglement gives shared dependencies, and we can also see from the available gates that it is only the entangling operations (CNOT and CZ) that allow us to copy dependencies from one qubit to another. The unusual feature of the classical bits here is that they too can carry the dependencies created by entanglement, and feed this back into the computation by interacting with qubits containing other dependencies.

By carrying these dependencies, the classical channel in this picture has now become part of the computation on a par with the quantum system, rather than merely giving data about the state of the qubits which perform the main computational work. It is the dependencies which enable the computation to happen: the computational resources in this picture are *dependencies* rather than bits or qubits. Bits and qubits become different ways of utilising and transmitting these resources, rather than separate resource entities in their own right. Quantum and classical elements to the computation are unified both by evolving under the same set of actions and interactions (the gates), and also by carrying the same set of fundamental resources.

Similarities between the processing abilities of quantum and classical elements now come down to how they carry the dependencies of the computation.

At the most fundamental level in the calculus, qubits have two separate components whereas bits have one. When these are acted on by identical gates, there are therefore differences in how bits and qubits appear to act, even though the dependencies are interacting in exactly the same way in all cases. One consequence of this fundamental similarity is that measurement-based computation is possible at all: classical elements can be used in the computation because they carry the same resources as quantum elements. If at some point during a quantum computation these only need to be transmitted individually rather than in pairs, then classical bits rather than qubits can be used. Moving between quantum and classical parts of a computation now becomes a question of how we wish to implement the underlying dependency structure of an algorithm. If we choose to use only qubits then we have a coherent computation with classical read-out at the end, but if we choose to send some dependencies through the system individually then we have a measurement-based implementation. Fundamentally, these are the same type of information processing, and the graphical calculus gives us a visual and intuitive method of translating between the two types of computation.

This basic similarity between quantum and classical information can also show the apparently fundamental differences between how information is stored and processed in bits and qubits. Arguably the most important difference between them is the persistence of information: classical bits can be cloned and deleted, whereas qubits are subject to the tight constraints of the no-cloning and no-deleting theorems. From the structure of the graphical calculus we can note the equivalent rules for the dependency information, which turn out to differ from both: *dependencies can be cloned and annihilated but not deleted.*

The cloning of dependencies is straightforward; this is what an entangling operation does between two (qu)bits. Entanglement simply is the sharing of identical copies of dependency information in this picture. The interesting question then becomes why we can't clone two dependencies from the left and right hand sides of a qubit at the same time, but we can just for one – in other words, why a qubit cannot be cloned but a bit can. The key to this lies in the entangling operations in this representation, in particular the CNOT operation. The CNOT operation here is symmetric between the control and target, up to a left/right symmetry on the inputs. The dependencies from the right-hand side of the control are copied into the target, and the target reacts back by copying its left-hand dependencies back to the control. Only one side of a qubit can be copied to another during an entangling operation – in order for both sides to be copied, two operations would be needed. The CNOT operation can be thought of as a “perfect measurement”, and so this can be described as a measurement not being possible without a back-reaction from the measuring system onto that being measured. However, after one interaction the state of the system is no longer the same as before the measurement, so trying to extract the second set of dependencies will give the original set but composed with

the dependencies picked up during the measurement. So if the information containing system has only one set of dependencies then it can be cloned, but if it contains two then the necessary back-reaction from any entangling operation means that it cannot be duplicated. Bits can be cloned, qubits cannot, but both are a consequence of how dependencies are copied between systems.

6 A LOCAL INFORMATION FLOW

We now turn to the second motivation for developing the graphical calculus, that of giving a logically and physically local notion of information flow through a hybrid computation, with the flow respecting standard notions of causality (such as action only into the future). There are a number of conditions that such a flow would have to satisfy in order to be considered as local, and we will look at these in turn.

Firstly, there is the question of what exactly is representing the ‘information’ that is ‘flowing’ in this picture. What is it that gets tracked through a computation? As we would expect, what are tracked are the resources for the computation – in this representation, information flow is the flow of dependency information through both bits and qubits.

The simplest locality condition on this flow is that the representation of an individual system must give all the information available for the evolution of that system. This is indeed what the individual calculus elements do, by construction. The next condition is much stronger, and is not satisfied by the usual state descriptions in quantum mechanics. This is the condition that there is no global state information that is not present in the local state. In standard quantum mechanics, the product of individual state descriptions of some set of systems (the reduced density matrices) is in general different from the description of the global state (the full density matrix). By contrast, in the graphical representation given here, there is no information contained in a joint state that is not already present in the individual states. There is no separate representation of joint system states in the calculus – the nearest to such an idea would be how two or more systems evolve under the action of a joint gate. Individual systems retain their individual representations even under entangling operations, and giving the set of individual states in a system gives the complete evolution of that system as a whole.

As well as this “mathematical locality”, we also want our information flow to satisfy “physical locality” conditions. The most important of these is that local operations change only local states. This again is something that is usually violated in standard representations of quantum mechanics, but arises naturally in the calculus. This is one of the differences that we saw during teleportation. In the standard picture, Alice’s local operations on her qubits change the state of Bob’s qubit non-locally. By contrast, in the graphical representation, Alice’s operations only act locally, as do Bob’s. Information

flows between them down the classical channel, rather than jumping from one to the other.

The final condition is that not only do local operations only change local states, but that the *only* way to change the state of a system is by locally operating on it. This is true in the graphical calculus by construction: the only morphism on an object is a gate, and the only gates that have been defined are those that act locally.

We therefore have a graphical representation of a flow of information through a computation that is represented using objects local to the systems being described, and which change only when acted on locally. This flow is not only local but also *causal*. Information contained within a system is only changed by actions on that system, and these actions only occur in one temporal direction. Information flows forward in time through a computation and never backwards, either logically or physically.

7 CONCLUSION

We have developed here a graphical calculus for information flow in hybrid information processing systems. This is a framework for information processing that integrates both quantum and classical elements into the same formalism, and explicitly defines the interface between bits and qubits using the same interactions as between qubits alone. This allows a fully formalised description of measurement-based computations, including a full description of the role played by the classical information channel. This leads to new descriptions of hybrid computational situations such as teleportation, with information previously considered to be entirely quantum being transmitted through the classical channel.

Quantum and classical resources in a computation are unified in this representation as instances of the underlying dependency resources. These dependencies are the basis for computation in this model, and their transmission and processing during a protocol demonstrate the flow of information. This flow model is local and causal, and defines both the logical structure of an algorithm and the physical flow of information within it. One interesting question is the connection between the information flow given by this representation and the flow notions defined in [2, 7], and whether this physical flow underpins these logical flow ideas.

Finally, we note that we now have the basis for a formal model of computation for both quantum and classical elements that can enable us to make direct comparisons between the two. Such comparisons could include resources use, including how quantum and classical resources can be interchanged for different implementations of a particular algorithm. Such a formal computability model would have its basic elements as the dependencies which are contained in both quantum and classical systems, and would allow the calculation of,

for example, the number of classical bits and gates needed to implement a known quantum algorithm. This in turn is an important step towards giving a formal definition of the relative processing powers of quantum, classical and hybrid computing.

ACKNOWLEDGEMENTS

We would like to thank Keith Harrison for prompting the construction of the calculus, and for critical feedback during its development. We also acknowledge fruitful discussions with Damian Markham, Kae Nemoto and Viv Kendon. This work was supported by European projects QAP and HIP.

REFERENCES

- [1] Daniel S. Abrams and Seth Lloyd. Simulation of many-body fermi systems on a universal quantum computer. *Phys. Rev. Lett.*, 79:2586 – 2589, 1997.
- [2] S. Abramsky and B. Coecke. A categorical semantics of quantum protocols. In *Proceedings of 19th IEEE conference on Logic in Computer Science*, pages 415–425. IEEE Press, 2004.
- [3] Charles H. Bennett, Ethan Bernstein, Gilles Brassard, and Umesh V. Vazirani. Strengths and weaknesses of quantum computing. *SIAM Journal on Computing*, 26:1510–1523, 1994.
- [4] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, , and William K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, 70:1895 – 1899, 1992.
- [5] Charles H. Bennett and Stephen J. Wiesner. Communication via one- and two-particle operators on einstein-podolsky-rosen states. *Phys. Rev. Lett.*, 69:2881 – 2884, 1992.
- [6] Ethan Bernstein and Umesh Vazirani. Quantum complexity theory. *SIAM Journal on Computing*, 26:11–20, 1997.
- [7] Daniel E Browne, Elham Kashefi, Mehdi Mhalla, and Simon Perdrix. Generalized flow and determinism in measurement-based quantum computation. *New J. Phys.*, 9(250), 2007.
- [8] D.E. Browne and H.J. Briegel. One-way quantum computation. In Dagmar Bruss and Gerd Leuchs, editors, *Lectures on Quantum Information*. Wiley, 2006.
- [9] Andrew M. Childs, Debbie W. Leung, and Michael A. Nielsen. Unified derivations of measurement-based schemes for quantum computation. *Phys. Rev. A*, 71(032318), 2005.
- [10] Bob Coecke. Kindergarten quantum mechanics. 2005. arXiv:quant-ph/0510032.
- [11] David Deutsch. Quantum theory, the Church-Turing principle, and the universal quantum computer. *Proceedings of the Royal Society of London*, A400:97–117, 1985.
- [12] David Deutsch and Patrick Hayden. Information flow in entangled quantum systems. *Proc. R. Soc. Lond. A*, 456:1759–1774, 1999.
- [13] Sara Felloni, Alberto Leporati, and Giuliano Strini. Diagrams of states in quantum information: an illustrative tutorial. 2009. arXiv:0904.2656v1.
- [14] Nicolas Gisin, Grgoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Reviews of Modern Physics*, 74:145–195, 2002.
- [15] Daniel Gottesman. The Heisenberg representation of quantum computers’. In S. P. Corney, R. Delbourgo, and P. D. Jarvis, editors, *Group22: Proceedings of the XXII International Colloquium on Group Theoretical Methods in Physics*, pages 32–43, 1999. Longer version at quant-ph/9807006.

- [16] Chris Heunen and Bart Jacobs. Quantum logic in dagger kernel categories. 2009. arXiv:0902.2355.
- [17] Clare Hewitt-Horsman and Vlatko Vedral. Developing the Deutsch-Hayden approach to quantum mechanics. *New Journal of Physics*, 9(5):135, 2007.
- [18] Clare Hewitt-Horsman and Vlatko Vedral. Entanglement without nonlocality. *Physical Review A*, 76:062319, 2007.
- [19] Michael Nielsen and Isaac Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.
- [20] Arun Pati and Samuel Braunstein. Impossibility of deleting an unknown quantum state. *Nature*, 404:164–165, 2000.
- [21] Robert Raussendorf and Hans J. Briegel. A one-way quantum computer. *Phys. Rev. Lett.*, 86:5188 – 5191, 2001.
- [22] Robert Raussendorf, Daniel E. Browne, and Hans J. Briegel. Measurement-based quantum computation on cluster states. *Phys. Rev. A*, 68(022323), 2003.
- [23] Niel Shenvi, Julia Kempe, and K. Birgitta Whaley. A quantum random walk search algorithm. *Phys. Rev. A*, 67(5), 2003. quant-ph/0210064.
- [24] W. K. Wothers and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982.