Sameness and Oppositeness in Quantum Information

O J E Maroney
Theoretical Physics Research Unit
Birkbeck College, University of London
o.maroney@physics.bbk.ac.uk

ANPA 22, 10-13 August 2000

Abstract

Surprising things happen when information processing is generalised to quantum, rather than classical systems. This paper reviews some recent results about the nature of information stored in quantum bits (qbits). An 'informational equivalence' between 'sameness' and 'oppositeness' in classical information fails to hold when those notions are generalised to quantum information. This has consequences for the sharing and flow of information within quantum networks.

1 Informational Equivalence of Duplicate Classical Bits

Alice and Bob are typical quantum information theorists: they have well stocked laboratories, with state of the art measuring devices, computers and so forth, and have access to an inexhuastible supply of quantum and classical objects. They have three noise free communication channels - one of which allows then to send classical information, in bits, the second for quantum objects and the third is a telephone to talk to each other about what they're doing. When a message from either of the first two channels gets received, it is not 'read' immediately, but is stored in a box (or a memory circuit, or something like that). The receiver then has a number of options as to what kind of operation s/he can perform upon the received 'message', one of which is "open the box and have a look" (of course, if it's a quantum message, the receiver must also decide *how* to open the box). For the moment, we will assume Alice and Bob are dealing with purely classical bits - which have two states - 0 or 1. If the two bits are both in state 0 or both in state 1, we say they are in the *same* state. If one is 0 and the other is 1, they are in *opposite* states.

1.1 Same Bit Test

Alice sends Bob a single bit in a box, but does not let Bob know what state it is in. Bob has to return two bits, each in the same state as Alice's original bit. Bob can pass Alice's bit through whatever logic gates he requires, but he is not allowed to open the box and look at what the bit is (we don't want to make it too easy!).

This test is still quite easy, because Bob just needs one logic gate to solve this perfectly: the Controlled NOT (CNOT) gate.

A	B	C	D
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

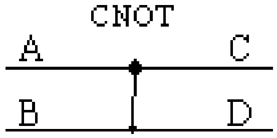

Figure 1: Controlled NOT Gate

With the input $B = 0$ this is often referred to as a FANOUT gate, and with $A = 1$ it is a NOT gate.

Bob takes Alices bit, and a second bit prepared in the state 0. Alice's bit is fed into the A-input, and Bob's second bit is fed into the B-input of the CNOT gate. The two output bits will now be in the same state as Alice's initial bit.

1.2 Opposite Bit Test

The second test requires Bob to return a second bit in the opposite state to Alice's original bit. Again, however, the solution is very simple. Bob requires only a third bit, now prepared in the state 1. After performing the same operation as for the Same Bit test, Bob simply sends the D-output into the B input of a second CNOT gate, with the third bit entering the A-input.

1.3 Informational equivalence

Although these tests seem trivial, they illustrate an important feature of information. Suppose Alice sends Bob a single bit, without specifying the state of the bit. Bob may have a physical system, but has acquired, as yet, no information (Bob has complete uncertainty about the state of the bit). If Alice sends Bob a second, unspecified bit, Bob has two physical systems, but still no information. However, now suppose Alice phones up Bob and tells Bob that, whatever state the first was in, the second was in the ***same*** state (we will assume Alice is not lying!). How much information has Bob acquired? What if Alice said the second was in the ***opposite*** state?

The answer is that Bob acquires 1 bit of information. By passing the two bits through the CNOT gate, A is in the initial state, but D is always in state 0. Although Bob has no information about the state Alice sent, he has an absolute certainty about the state of D. For the second case, Bob performs a NOT upon B, before passing it through the CNOT. By informing Bob of the correlation between A and B, Alice has reduced the number of the

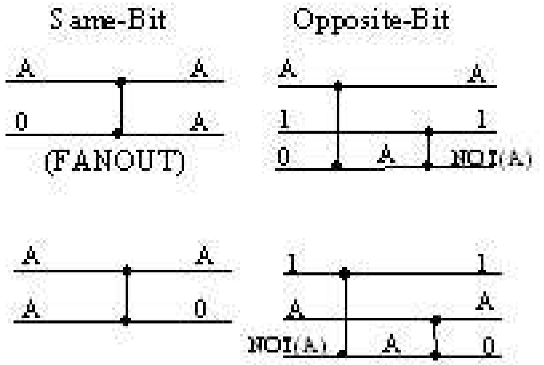

Figure 2: Informational Equivalence

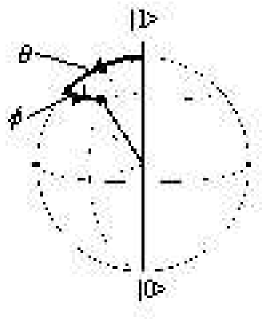

Figure 3: The Bloch Sphere

possible states (or Bob's uncertainty) by 1 bit. Bob converts this correlation information into a certainty about the state of one of the bits ('using up' the correlation). Bob can switch between these states but always has exactly 1 bit of information about the joint system. The three states are "informationally equivalent". Creating duplicate bits, or flipping those duplicate bits, cannot be used to increase or decrease the information available. This is why Bob found the tests so easy: Alice was not requiring Bob to supply any more information back to her, than she had sent to him in the first place.

2 Quantum Bits

Now Alice and Bob try to do the same thing, but with quantum bits. A quantum bit (or qbit) is a two dimensional Hilbert space, with basis states $|0>$ and $|1>$, The general state of qbit is:

$$\Psi = e^{i\frac{\phi}{2}} \cos \overset{\tilde{A}}{} \frac{\mu}{2} \overset{!}{} |1> + e^{-i\frac{\phi}{2}} \sin \overset{\tilde{A}}{} \frac{\mu}{2} \overset{!}{} |0>$$

often shortened to

$$\Psi = \text{®}|1> + \text{¯}|0>$$

The qbit may be represented by a point on a sphere of unit magnitude (Bloch sphere). The inner product of two qbits is

$$< \Psi|\Psi' >= \text{®}^*\text{®}' + \text{¯}^*\text{¯}'$$

For any given qbit state, there is exactly one other qbit state with which it has a zero inner product. This other state corresponds to the point in exactly the opposite direction on the Bloch sphere. $|1>$ and $|0>$ are 'opposite' to each other, and as the choice of a basis for $|1>$ and $|0>$ is arbitrary, this may be taken as the quantum generalisation of 'oppositeness' of bits. A qbit 'opposite' to $|n>$ will be represented by $|-n>$. For the inner product to be 1, the two qbits must at the same point on the Bloch sphere, and will be in the 'same' quantum state. If there is an ensemble of qbits, prepared in different states, the density matrix corresponds to a point lying inside the sphere.

Now we need the logical operations Alice and Bob can perform upon qbits, and it turns out that a single gate is sufficient to represent all of them - the quantum controlled-not[1].

$$\begin{aligned} C(a;b;c) &= |0><0|_A \otimes I_B + |1><1|_A \otimes U(a;b;c)_B \\ U(a;b;c) &= \text{Ã} \begin{matrix} e^{ia}\cos b & -e^{ic}\sin b \\ e^{-ic}\sin b & e^{-ia}\cos b \end{matrix} \,! \end{aligned}$$

If we take the basis states of $|0>$ and $|1>$ as the 'classical' states 0 and 1, we can reconstruct classical logic gates from this[1]. In particular, the classical CNOT gate is equivalent to $C(0;¼=2;¼):$

How much information is there in a single qbit? There is a lot more possibilities for the qbit, than for the bit. Surely, this gives Alice a much wider range of signals she can send Bob.

However Bob has a problem. Alice sends Bob a single, unknown qbit in a box. It could be pointing anywhere on the Bloch sphere. When receiving a classical bit, Bob can simply open the box, find out what it is, and gain one bit of information. However, for a qbit, Bob must make a measurement, along a particular axis. If he chooses the conventional axis, he gets the probabilities

$$\begin{aligned} \Pr(|0>) &= \sin^2(\frac{\mu}{2}) \\ \Pr(|1>) &= \cos^2(\frac{\mu}{2}) \end{aligned}$$

and afterwards the qbit is in state $|0>$ or $|1>$ respectively.

[1] In classical logic, there are three input gates which cannot be built from reversible two input gates. These three input gates can be constructed from two-input quantum gates that are not equivalent to two input classical gates!

Although a large number of identically prepared qbits will eventually yield up the value of µ, Bob doesn't get any information about Á and Alice could be sending qbits pointing in different directions. As the measurement described has only two outcomes, it turns out Bob can get, at most, one classical bit of information from the transmitted qbit. With an infinite amount of qbits, Bob can find µ exactly, but this is the same as the infinite amount of bits necessary to specify a continuous parameter. The average information conveyed by each qbit is still one bit.[2][3][4]

2.1 Same Qbit Test

This suggests that there is no difference, in information content, between the classical and quantum bits. However, if we look again at the trivial tests Alice set, we find Bob has a much harder task. We will judge Bob's success at playing the game by a FIDELITY test. If Bob is supposed to produce a qbit in the state |*u* >= ®|1 > +¯|0 >, Alice will measure the state he actually produces in the |*u* >; |−*u* > basis, and the fidelity is the probability of Bob's qbit passing the test. In order to test a given strategy, we average this over all the possible states Alice could have chosen.

Bob has a number of strategies.

2.1.1 Random Guesswork

Bob is feeling bored with this silly game. He throws Alice's bit away and sends her two bits, each of which he prepares in some random, but identical state, |*n*′ >= ®′|1 > +¯$_3$′|0 >. When Alice measures Bob's qbits, the probability of passing is cos^2 $\frac{\theta}{2}$ where µ is the angle between the Alice's and Bob's directions. The mean fidelity of each bit is F = 1=2 and the joint fidelity (the probability of getting both right) F_J = 1=3. While random guesswork is not a good solution it gives us a baseline to measure the success of other methods.

2.1.2 Measure and Copy

Bob measures the bit in some basis (for convenience, we use |1 >; |0 >), and sends back two bits in the direction the measurement gives. This gives a density matrix ½ = |®|^2 |11 >< 11| + |¯|^2 |00 >< 00| and average fidelities F = 2=3; F_J = 1=2

2.1.3 FANOUT

Bob thinks the problem might be because he is opening the box to measure the qbit, and this disturbs the quantum system. So he uses in logic gates (FANOUT) to copy the qbit, without opening the box. This produced a perfect solution with classical bits. However, with qbits, the result is $F = 2{=}3$, $F_J = 1{=}2$ and is no better than "measure and copy"! What went wrong?

The answer is that FANOUT fails to copy the qbit - instead it creates an entangled state between the output bits:

$$FANOUT(®|1> + ¯|0>)|0> = ®|1>|1> + ¯|0>|0>$$

As a density matrix this is

$$½ = |®|^2 |11><11| + |¯|^2 |00><00| + ®^*¯|00><11| + ®¯^*|11><00|$$

with diagonal elements equivalent to the 'Measure and Copy' approach. In fact the FANOUT gate bears a lot in common with the process of measurement, and is sometimes referred to as a 'measurement' gate.

2.1.4 Quantum FANOUT and "no-cloning"

Can we build a quantum FANOUT? If we take an initial, unknown qbit, and a auxiliary system, prepared in a known state, does there exist any unitary operation of the form:

$$CLONE(|n>|Aux0>) = |n>|n>|Aux(n)>$$

where $|Aux0>$ is the initial auxiliary system, and $|Aux(n)>$ is an n dependant 'junk' output, which works for all values of n? The answer to this was answered in the negative by Wootters and Zurek[5]. The proof of the non-existence of $CLONE$ can be found from the unitary operation preserving the inner product between states

$$<n|n'><Aux0|Aux0> = (<n|n'>)^2 <Aux(n)|Aux(n')>$$

However, the inner product of two states obeys the relation

$$|<i|j>| \leq 1$$

with equality holding only when $i = j$. The required relationship can only hold when either $n = n'$ or when $<n|n'> = 0$, but cannot hold for general values of *n* . An obvious case for $< n|n' >= 0$, is where $n = 1$, $n' = 0$. So classical information can be cloned (which is fortunate, as we already have a FANOUT gate that does this!)

However, it is possible to build imperfect cloning machines, that produce a fidelity better than simply 'measure and copy'.[6][7][8][9] An example of an optimal quantum cloning, in which the fidelity of the output is independant of the input state, is given by the following unitary operation:

$$\begin{aligned} |0>|00> &\rightarrow \sqrt{\frac{2}{3}}|000> + \sqrt{\frac{1}{6}}|011> + \sqrt{\frac{1}{6}}|101> \\ |1>|00> &\rightarrow \sqrt{\frac{2}{3}}|111> + \sqrt{\frac{1}{6}}|010> + \sqrt{\frac{1}{6}}|100> \end{aligned}$$

For a general input qbit of $|n>$ in the first position, this produces output qbits in the first and second positions of ½ = 5=6$|n >< n|$ + 1=6$|-n >< -n|$. The third qbit is the 'junk' auxiliary output. The fidelty is *F* = 5=6 , with a joint fidelity of F_J = 2=3

2.2 Opposite Qbit Test

What of Alice's second test? What if Bob has to produce two qbits, but in opposite directions?

Bob has the same strategies available to him. If he measures Alice's bit, and sends back opposite qbits $|10>$ or $|01>$, he gets the same fidelity of as 'measure and copy' for producing the same qbits. If he runs the qbit through a FANOUT and a NOT gate, he get the fidelity of 'FANOUT' for same qbits.

What if he uses an optimal cloner and NOT? Surprisingly, our joint fidelity is worse and our opposite bit is terrible!

Fs = 5=6; *Fo* = 7=12; *Fj* = 2=3

The reason for this failure is that our NOT gate is failing to work in the way we desired:

NOT (®$|1>$ + ¯$|0>$) = ¯$|1>$ +®$|0>$

It is easy to show that *NOT*($|n>$) is opposite to $|n>$ only if $n = 0$ or $n = 1$ (if the input qbit is part of classical logic). Bob needs an operation that performs:

OPP ($|n>$) = $|-n>$
OPP (®$|1>$ + ¯$|0>$) = ¯*$|1>$ −®*$|0>$

Such an operation is not forbidden by the conservation of the inner product, as $< n|m >=< -n|-m >$. However if $OPP(|1>) = |0>$ and $OPP(|0>) = |1>;$ then NOT is the only linear operation that satisfies these conditions (the 'no-spin-flip theorem').

Still, perhaps there is an imperfect OPP, in the same manner that there is an imperfect $CLONE$? It turns out the best that can be done is to build an anti-cloning machine, that takes an input qbit $|n>$ and attempts to make output qbits $|n>|-n>$, succeeding with fidelity $F = 2{=}3$, joint fidelity $F_J = 5{=}8:$ [10][11][12]

Now this is particularly interesting - not only is Bob failing Alice's test, but trying to produce an *opposite* second bit is failing worse than a *same* second bit. Somehow it seems *opposite* is not informationally equivalent to *same*? Rather than examine proofs of the no-cloning and no-spinflipping theorems, let us look at the states we are trying to produce - the duplicate qbits.

3 Duplicate Quantum Bits and Informational Equivalence

Suppose Alice sends Bob a qbit prepared in a state unknown to Bob. Bob's uncertainty is at a maximum, as he has no information on the state of the bit. Now Alice sends Bob a second qbit, also unknown, but prepared in the same state as the first qbit. How much more information does Bob possess?

In the classical case, we saw that the answer was one bit. However, that was clearly related to the fact that we could run both bits through the FANOUT gate, and put one of them into a definite state. This is clearly not possible for qbits: if it were, we could simply reverse the process, and clone a qbit[15].

If we take an ensemble of qbits, in different states eg.

$$|a|^2|00><00| + |b|^2|11><11|$$

the information known about the ensemble is given (in bits), by

$$H = 1 + Tr(½ log_2 ½)$$

For an N-qbit system, the information known is

$$H_N = N + Tr(½ log_2 ½)$$

For a 1 qbit system, a general qbit is described by:

$$\rho = \begin{pmatrix} |\alpha|^2 & \alpha^*\beta \\ \alpha\beta^* & |\beta|^2 \end{pmatrix}$$

The 'general' qbit could have been a point anywhere on the Bloch sphere, with uniform probability. We average α and β uniformly over the Bloch sphere, and get a density matrix

$$\rho = \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}$$

In this case the information is zero, which represents the fact that we know nothing about where on the Bloch sphere a general qbit points. If we knew the state $|n>$ the qbit was prepared in, we can express the density matrix in the basis $|n>, |-n>$, where it becomes

$$\rho = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

and the information is 1 bit, representing a complete knowledge of the state of the qbit.

For two qbits prepared in the same state $|n,n>$, the density matrix, when $|n>$ is integrated over the Bloch sphere, is:

$$\overline{\rho(|n,n>)} = \begin{pmatrix} 1/3 & 0 & 0 & 0 \\ 0 & 1/6 & 1/6 & 0 \\ 0 & 1/6 & 1/6 & 0 \\ 0 & 0 & 0 & 1/3 \end{pmatrix}$$

which can be expressed as

$$\overline{\rho(|n,n>)} = \frac{1}{3}(|u,u><u,u| + |u+><u+| + |-u,-u><-u,-u|)$$

where $|u>$ is an arbitrary point on the Bloch sphere and

$|u+>= \frac{1}{\sqrt{2}}(|u,-u>+|-u,u>)$.

This is not complete uncertainty. A total lack of knowledge is represented by

$$\rho_{\min} = \begin{pmatrix} 1/4 & 0 & 0 & 0 \\ 0 & 1/4 & 0 & 0 \\ 0 & 0 & 1/4 & 0 \\ 0 & 0 & 0 & 1/4 \end{pmatrix}$$

which has information of zero. Instead, the knowledge that we have two bits that are in the same state gives us $H = (2 - \log 3) = 0{:}415$ bits. This is less than the 1 bit that correlated classical bits gives us, but more than complete ignorance. A classical correlation would have given us $H = (2 - \log(2))$ bits.

What if they are in opposite states - how much information have we gained? Two qbits in unknown, opposite states have a averaged density matix of

$$\overline{\text{½}(|n;-n>)} = \begin{pmatrix} 1{=}6 & 0 & 0 & 0 \\ 0 & 1{=}3 & -1{=}6 & 0 \\ 0 & -1{=}6 & 1{=}3 & 0 \\ 0 & 0 & 0 & 1{=}6 \end{pmatrix}$$

or

$$\begin{aligned} \overline{\text{½}(|n;-n>)} &= \frac{1}{6}(|u;u>< u;u| + |u+ >< u+| + |-u;-u>< -u;-u|) \\ &\quad + \frac{1}{2}(|u- >< u-|) \\ &= \frac{1}{2}\overline{\text{½}(|n;n>)} + \frac{1}{2}(|u- >< u-|) \end{aligned}$$

with $|u- >= \frac{1}{\sqrt{2}}(|u;-u> - |-u;u>)$ This has $H = (2 - \frac{1}{2}\log 12) = 0{:}208$ bits, exactly half the information of the same states.

3.1 Why don't we have 1 bit of correlation information?

If we expand the pure states, in the conventional basis, we obtain:

$$\begin{aligned} \Psi(|n;n>) &= \text{®}^2|11> + \sqrt{2}\,\text{®}\text{¯}\left(\frac{|01> + |10>}{\sqrt{2}}\right) + \text{¯}^2|00> \\ \Psi(|n;-n>) &= \text{®}\text{¯}^*|11> + \left(\frac{|\text{®}|^2 - |\text{¯}|^2}{\sqrt{2}}\right)\left(\frac{|01> + |10>}{\sqrt{2}}\right) \\ &\quad + \left(\frac{|\text{®}|^2 + |\text{¯}|^2}{\sqrt{2}}\right)\left(\frac{|01> - |10>}{\sqrt{2}}\right) - \text{®}^*\text{¯}|00> \end{aligned}$$

When measured in a different basis to the preparation basis, the same-state qbits may yield opposite results, while the opposite-state qbits can give the same results!

This clearly is a property of non-orthogonality in the quantum measurement process - even if we are sure the states were prepared in same (or opposite states), we cannot be sure they will both pass/fail (or the opposite) if the measurement is in a different basis. The essential feature of this is the non-orthogonality of the states the qbits *may have been* prepared in. If we are told that the qbits are prepared in a *particular* basis, then we can simply switch our logic gates to operate on that basis, and all our results of classical logic apply.

3.2 Why does oppositeness convey less information than sameness?

Although the separation between the two cases is guaranteed by the no-spin flip theorem, this does not explain why oppositeness conveys so much less information than sameness.

The wavefunctions and density matrices above, were expressed in the basis

$$\begin{array}{lllllll} \Phi_1 & = & |11> & & \Phi_2 & = & \frac{1}{\sqrt{2}}(|10> +|01>) \\ \Phi_3 & = & \frac{1}{\sqrt{2}}(|10> -|01>) & & \Phi_4 & = & |00> \end{array}$$

In $\overline{½(|n;n>)}$, the probability of finding the state Φ_3 is zero, while for $\overline{½(|n;-n>)};$ it is one half.

Using the notation

$$\begin{array}{lllllll} |1>_X & = & \frac{|1>_Z+|0>_Z}{\sqrt{2}} & & |0>_X & = & \frac{|1>_Z-|0>_Z}{\sqrt{2}} \\ |1>_Y & = & \frac{|1>_Z+i|0>_Z}{\sqrt{2}} & & |0>_Y & = & \frac{i|1>_Z+|0>_Z}{\sqrt{2}} \end{array}$$

we can construct the Φ basis from a superposition of opposite states:

$$\begin{aligned} \Phi_1 &= \frac{(1-i)}{2}(|01>_Z -|10>_Z) + |10>_X -i|10>_Y \\ \Phi_2 &= \frac{1}{\sqrt{2}}(|10>_Z +|01>_Z) \\ \Phi_3 &= \frac{1}{\sqrt{2}}(|10>_Z -|01>_Z) \\ \Phi_4 &= \frac{(1+i)}{2}(|10>_Z -|01>_Z) - |10>_X -i|10>_Y \end{aligned}$$

however, we can only construct 3 out of the 4 basis from same states:

$$\Phi_1 = |11>_Z$$

$$\begin{aligned}\Phi_2 &= \sqrt{2}|11>_X - \frac{1}{\sqrt{2}}(|11>_Z + |00>_Z) \\ \Phi_4 &= |00>_Z\end{aligned}$$

The space of the two qbits $SU(2) \times SU(2)$ has two invariant subspaces, under global rotations: a symmetric subspace, of dimension 3, and an antisymmetric subspace, of dimension 1. 'Sameness' means that the qbits can only be found within the symmetric subspace, and are evenly distributed throughout it. While in the classical case, the correlation information restricts the bits to a two dimensional subspace (and therefore represents an ignorance of log(2) bits) in the quantum case the restricted subspace is 3 dimensional, and the ignorance is log(3) bits. The opposite qbits are distributed throughout the entire state space - but they are likely to be found in the antisymmetric subspace, so 'oppositeness' does give some correlation information.

What is remarkable, however, is that these differences can only appear when one looks in an entangled basis, ***even though the qbits themselves are always prepared in product states!*** The measurement is of a joint property of the qbits - we cannot relabel the parts of the apparatus that apply only to the second particle, because there are no such parts. If we were to 'flip' the second qbit in the 'opposite state' expansion of the of the Φ basis, the result would no longer be an orthonormal basis, and does not correspond to a valid measurement (see also [13]). This strange phenomena - entangled state measurements yielding more information than any combination of local measurements, even when made on ensembles of product states - has been dubbed 'non-locality without entanglement'[14]

4 Information and reversible computing

The theory of reversible computation was developed following the discovery of Landauer's principle[16], that only logically irreversible operations implied an irretrievable loss of energy (prior to that, it was thought that each logical operation involved a dissipation of $kT \ln(2)$ per bit). The amount of lost energy is directly proportional to the Shannon measure of the information that is erased.

It is often defined as a requirement to 'do work' to perform the erasure. This is not strictly accurate. It requires an ***investment*** of $kT \ln(2)$ free energy, per bit of information that is stored. At any time in the computation, any bit that is in a known state can have this free energy recovered. A known state is one that is in a particular value, regardless of the choice of input state, (we may extend this to include always in the same state as an initial input state). When we examine a computational network, given the program, and the input state, we can recover all the free energy from the bits that are known. Other bits may be in determinate states, well defined functions of the input. It may be argued that these are, therefore, 'known' but, as these states are non-trivially dependant upon the input state (eg. (A OR NOT B) AND (C XOR D)), to extract the energy requires one to find the value of the bit from the input state ie. to recapitulate the calculation on a second system, which requires an investment of an equivalent amount of free energy - so no gain is made in terms of recoverable energy. The objective of reversible computing is to reduce the amount of the free energy invested into the calculation that cannot be recovered at the end without losing the results of the computation.

A reversible calculation may be defined as one which operates, upon an input state i and an auxiliary system, prepared in an initial state $Aux0$, to produce an output from the calculation $O(i)$, and some additional 'junk' information $Aux(i)$:

$$F : (i; Aux0) \rightarrow (O(i); Aux(i))$$

in such a manner that there exists a complementary calculation:

$$F' : (O(i); Aux(i)) \rightarrow (i; Aux0)$$

The existence of the 'junk' information corresponds to a history of the intervening steps in the computation, so allowing the original input to be reconstructed. A computation that did not keep such a history, would be irreversible, and would have lost information on the way. The information lost would correspond to an amount of free energy invested into the system that could not be recovered.

However, $Aux(i)$ is not generally known, being non-trivially dependant upon the input, $i;$ and so represents free energy that cannot be recovered. A general procedure for discovering the complementary calculation F' can be given like this: take all the logical operations performed in F, and reverse their operation and order. As long as all the logical operations in F are is always possible to make a computation reversible. However, this is not immediately very useful: although we could recover the energy by reversing the computation, we lose the output $O(i)$ in doing so.

Bennett[17][18] showed that a better solution was to find a different reverse calculation F"

$$F'' : (O(i); Aux(i); AuxO) \rightarrow (i; Aux0; O(i))$$

The only additional unknown information is $O(i)$, which is simply the output we desired (or extra information we needed to know). A general procedure for F", is: copy $O(i)$ into a futher auxiliary system $AuxO$ by means of a FANOUT gate, then run F'on the original system. This has also been shown to be the optimal procedure[19][20] for F". We call such a calculation, G, TIDY. All classical reversible computations are TIDY.

Straight away, we should notice a problem! The universal FANOUT gate does not exist for a quantum computation.

Clearly, in the case where the output states from a quantum computer are in a known orthogonal set, then the quantum computation can be made tidy. In fact, for other reasons, having orthogonal output states was initially taken as a requirement on a quantum computer, as it was deemed necessary for reading out the output. This was suggestive not of a general quantum computation, but of limited quantum algorithmic boxes: each connected by classical communication. However, developments in quantum information theory have suggested that distributed quantum information may be desirable - in particular, a more general conception of quantum computation may be required which takes inputs from different sources, and/or at different times. In Figure 5 we see an example of this - Alice performs some quantum computation, and stores the result of it in a 'quantum data warehouse'. At some later time, Bob takes part of these results as an input into his own computation. We are going to take our definition of a quantum computation as: [2]

$$U_C(|i > |Aux0 >) \rightarrow |O(i) > |Aux(i) >$$

so that the ouput is always in a separable state (in other words, we regard the 'output' of the computation as the subsection of the Hilbert space that is

[2] There is further complication when entanglement enters the problem. When part of an entangled state is transmitted, the loss of free energy is always greater than the entropy

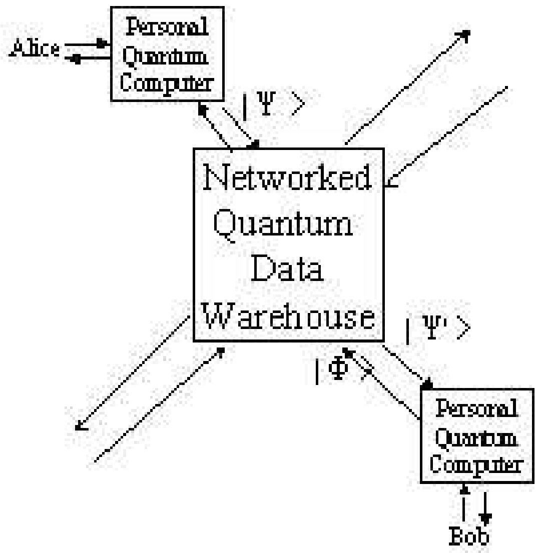
Alice
Personal Quantum Computer
$|\Psi>$
Networked Quantum Data Warehouse
$|\Psi'>$
$|\Phi>$
Personal Quantum Computer
Bob

Figure 4: Distributed Quantum Computing

interesting, and the 'auxiliary' as everything that is uninteresting. If the 'output' were entangled with the 'auxiliary' space, then there would be additional information relevant to the 'output', contained in the super-correlations between 'output' and 'auxiliary' spaces). As any quantum computation must be performed by a unitary operation, all quantum computers must be reversible. But are they TIDY?

If this model of computation is classical, then each time data is sent to the central database, the local user can FANOUT the data before sending it, and tidy up their computer as they go along. The only energy commitment is: total input, plus stored data. The difference between connected classical algorithmic boxes and a single classical computation is a trivial distinction, as the computation may be tidied along the way.

Considering a general quantum operation, unitarity requires that the inner products between different input states and between the corresponding output states is unchanged by the computation. Reversibility must always hold.

$$\begin{aligned} REVERSIBLE &: < i|j >< Aux0|Aux0 >= \\ & < O(i)|O(j) >< Aux(i)|Aux(j) > \\ TIDY &: < i|j >< Aux0|Aux0 >< AuxO|AuxO >= \end{aligned}$$

$$< i|j >< O(i)|O(j) >< Aux0|Aux0 >$$

We can eliminate $< Aux0|Aux0 >= 1$ and $< AuxO|AuxO >= 1$, leaving only three cases.

4.1 Orthogonal Outputs

The output states are orthogonal set:

$$< O(i)|O(j) >= \pm_{ij}$$

Reversibility *requires* the input states to be an orthogonal set $< i|j >= 0$, and the TIDY condition will hold. This is not too surprising, as an orthogonal set of outputs *can* be cloned, and so can be tidied using Bennett's procedure.

4.2 Orthogonal Inputs

The input states are orthogonal set $< i|j >= \pm_{ij}$, but the output states are not. To satisfy unitarity, the *auxiliary* output states must be orthogonal.

$$< Aux(i)|Aux(j) >= \pm_{ij}$$

There is a unitary operator for tidying the computation, without losing the output. However, this tidying computation is not Bennett's procedure. If we cloned the auxiliary output, and run the reverse operation, we would lose the output, and be left with the 'junk'! Whether there is an equivalent general procedure for obtaining F'' is not known.

One obvious method is to examine the resulting auxiliary output states, construct a unitary operator from

$$U_G|Aux\,(i)\,;O\,(i) >= |Aux0;O\,(i) >$$

and decompose U_G into a quantum logic circuit. However, it is not clear whether the operator can be constructed without explicitly computing each of the auxiliary output states - which may entail running the computation itself, for each input, and measuring the auxiliary output basis. Alternatively, examine the form of the auxiliary output (eg. (A OR NOT B) AND (C XOR D))) and devise a logic circuit that reconstructs the input state from this. This simply restates the problem: although some such circuit (or U_G) must exist, is there a general procedure for efficiently constructing it from only a knowledge of U_C?

4.3 Non-orthogonal Inputs

The input states are a non-orthogonal set. This corresponds to Bob's position in the quantum distribution network of Figure 5.

If we look at the requirements for a tidy computation, this leads to:

$$< O(i)|O(j) >= 1$$

The output is always the same, regardless of the input! Obviously for a computation to be meaningful, at least some of the output states must depend in some way upon the particular input state. So there does not exist *any* non-trivial ($|O(i) > \neq |O(j) >$) computations of the form

$$G : |i > |Aux0 > |AuxO >\to |i > |Aux0 > |O(i) >$$

for which $< i|j > \neq \pm_{ij}$: [3]

It should be clear: this does NOT mean useful, reversible quantum computations of the form

$$F : |i > |Aux0 > |- > |Aux(i) > |O(i) >$$

do not exist when $< i|j > \neq \pm_{ij}$ - simply that such computations cannot be 'tidy'. For such computations, not only is the free energy used to store the auxiliary output unrecoverable, but also the input state cannot be recovered, except through losing the output. For our distributed network, this means that not only can Bob not 'tidy' his computation, but he cannot restore Alice's data to the database.

5 Summary

We have examined the notion of 'sameness' and 'oppositeness' when applied to quantum information and found that the 'informational equivalence' of these in the classical case no longer hold. Quantum information cannot be copied or duplicated, in the manner of classical information.

This has a surprising consequence for computation. The flow of information in a classical computation can be broken down into separate algorithms, with these algorithms passing classical information between them. Such algorithms can be reversibly, and tidily, implemented. If the overall calculation

[3] It is interesting to note that the 'no-cloning' theorem is a special case of this.

requires input data in separate places and times, it can easily be broken down into separate algorithms at each place and time, with classical communications between them. This is only because such classical information can be duplicated in an 'informationally equivalent' manner.

Existing quantum algorithms have been designed on the basis of replacing similar classical algorithms. They therefore take a set of classical inputs, at one place and time, and produce a set of classical outputs, and so can be implemented in a tidy manner. However, each quantum algorithm itself cannot be broken down into sub-algorithms.

A more generalised conception of the flow of information in a quantum system appears necessary. Information enters and is shared at separate times and places, and cannot necessarily be processed by tidy sub-algorithms, as the information exchanged is not necessarily classical in nature. Even where a tidying procedure can exist, it is not clear that a general and/or efficient program for implementing this procedure is available.

"Oppositeness" and "Sameness" are well defined, conceptually simple, relationships between qbits, yet there are no physical systems that can implement these as operations such as OPP and CLONE. We must therefore be very careful before assuming which logical ideas can still be relied upon when trying to understand the nature of information in quantum processess.

References

[1] DiVincenzo DP, cond-mat/9407022

[2] Schumacher B, Phys Rev A, Vol 51 No 4, 2738-2747 (1995)

[3] Jozsa R, Shumacher B, J Mod Optics, Vol 41 No 12, 2343-2349 (1994)

[4] Holevo AS, Prob Inf Trans, Vol 9, 110, 177 (1973)

[5] Wootters WK, Zurek WH, Nature Vol 299, 802-803 (1982)

[6] Buzek V, Hillery M, Phys Rev A, Vol 54 No 3, 1844-1852 (1996)

[7] Gisin N, Massar S, Phys Rev Lett, Vol 79 No 11, 2153-2156 (1997)

[8] Buzek V, Braunstein SL, Hillery M, Bruss D, Phys Rev A, Vol 56 No 5, 3446-3452 (1997)

[9] Bruss D, DiVincenzo DP, EKert A, Fuchs CA, Macchiavello C, Smolin JA Phys Rev A, Vol 57 No 4, 2368-2378 (1998)

[10] Gisin N, Popescu S, Phys Rev Lett, Vol 83 No2, 432-435 (1999)

[11] Buzek V, Hillery M, Werner RF, Phys Rev A, Vol 60 No 4, R2626-R2629 (1999)

[12] Song DD, Hardy L, quant-ph/0001105

[13] Massar S, quant-ph/0004035

[14] Bennett CH, DiVincenzo DP, Fuchs CA, Mor T, Rains E, Shor PW, Smolin JA, Wootters WK, Phys Rev A, Vol 59, 1070 (1999)

[15] Pati AK, quant-ph/9911090

[16] Landauer R, IBM J Res Develop, Vol 5, 183-191 (1961)

[17] Bennett CH, IBM J Res Develop, Vol 17 525-532 (1973)

[18] Bennett CH, Int J Theor Phys, Vol 21, 905-940 (1982)

[19] Li M, Tromp J, Vitanyi P, Physica D, Vol 120 No 1-2,168-176 (1998)

[20] Li M, Vitanyi P, Proc Roy Soc Lon A, Vol 452, 769-789 (1996)