Computing with a Quantum Flavor

Andreas Klappenecker

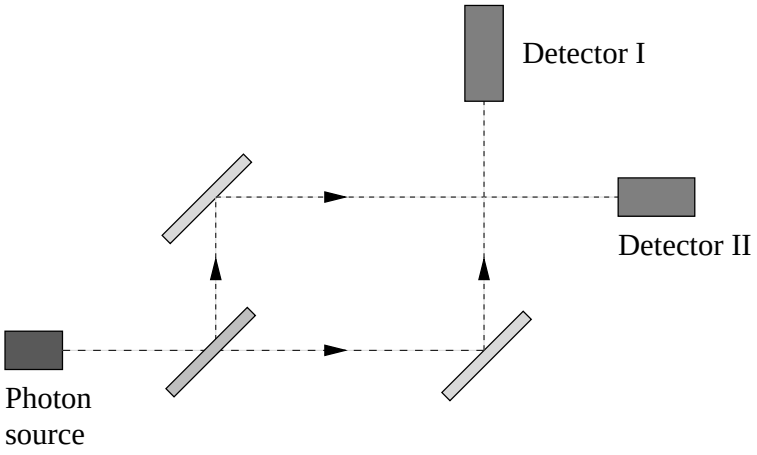
Department of Mathematics, Texas A&M University,
College Station, TX, 77843-3368, USA
Institute for Algorithms and Cognitive Systems, Dept. of Computer Science,
University of Karlsruhe, D-76128 Karlsruhe, Germany

April 24, 2000

Introduction. The last century witnessed the birth and the rapid development of the computer. Although the implementations differ in their design and architecture, the vast variety of computers is implemented with logic gates. As a result, all known implementations can be simulated with a polynomial slowdown by a probabilistic Turing machine. A strong form of the Church-Turing thesis conjecturally asserts that this will be true for *any* computer, that is, even for those computers that are yet to be built.

In some sense this would be bad news, since the truth of the strong Church-Turing thesis would imply that there does not exist a rapid solution to many interesting computational problems. However, at the end of the last century there was a first serious attempt to challenge the validity of the strong Church-Turing thesis. Surprisingly, the main ingredient did not come from computer science but from physics. I want to discuss some computational aspects that have emerged from intertwining computer science and physics. Although I had to prepare these notes at short notice, it is my hope that the reader can get at least an impression of the flavor of this new area.

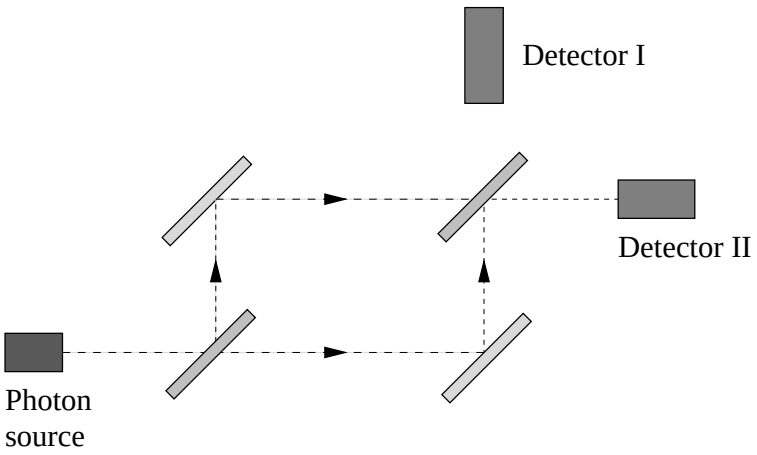
Quantum Effects. Let us consider the following experiment. Take a transparency and a laser pointer, and hold the transparency slightly tilted into the laser beam. You will notice that some photons will be transmitted and some will be reflected by the transparency. A slightly more elaborate form of this experiment can be set up in an optical lab as follows.



We replace the transparency by a semi-silvered mirror, adjusting the setup such that the reflected and the transmitted beam have the same intensity. Moreover, we introduce two mirrors that reflect our two light beams such that they reach two photon detectors, as depicted above. Suppose that these detectors are sensitive enough to register a single photon. Reducing the intensity of our photon source, we will notice that some photons are registered by Detector I and some are registered by Detector II. If the source emits only one single photon, then our setup guarantees that this photon will be registered with probability one-half by Detector I.

This experiment suggests a particle-like behavior of our photon. We are led to belief that the photon travels with probability one-half on either path.

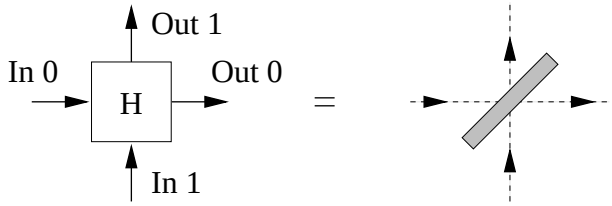
Let us modify the experiment a little bit. We insert another semi-silvered mirror just where the two beams intersect, as shown in the following figure:



The first experiment suggested that a photon emitted from the source will be reflected or transmitted with probability one-half at the first semi-silvered mirror. Traveling either way, there is another 50:50 chance that the photon will transmitted or reflected at the next semi-silvered mirror. Following this line of thought, we would expect that the photon will be registered with probability one-half at Detector I. However, we observe a completely different behavior in the experiment, namely that the photon will *always* be registered by Detector II, and never by Detector I.

This second experiment reveals a wave-like behavior of a photon. In fact, after the photon passes the first semi-silvered mirror, it is best to assume that it is in a superposition of the reflected and the transmitted state, rather than in either one of those two alternatives. After passing through the second semi-silvered mirror, there is a constructive interference at Detector II and a destructive interference at Detector I.

The Rules of the Game. We can view the semi-silvered mirror as a device H with two input ports and two output ports.

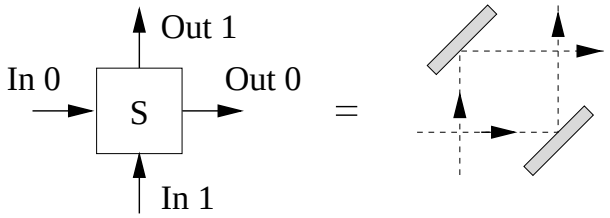


A photon entering this device through input port 0 will be put into superposition of the transmitted state $|0\rangle$ and the reflected state $|1\rangle$, which is expressed as $H|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle$. A photon entering the device through input port 1 will be put into the state $H|1\rangle = \frac{1}{\sqrt{2}}|1\rangle + \frac{i}{\sqrt{2}}|0\rangle$.

The symbols $|0\rangle$ and $|1\rangle$ have a simple mathematical meaning, they denote a fixed orthonormal basis of the two-dimensional complex vector space $\mathbf{C}^2$. A superposition of states $a|0\rangle + b|1\rangle$ as an output of the device means that the photon can be observed at output port 0 with probability $|a|^2$ and with probability $|b|^2$ at output port 1. This explains why Detector I registered only half of the photons in the first experiment. Indeed, the output of the semi-silvered mirror was $H|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle$, and thus the outcome 0 has probability $|1/\sqrt{2}|^2 = 1/2$.

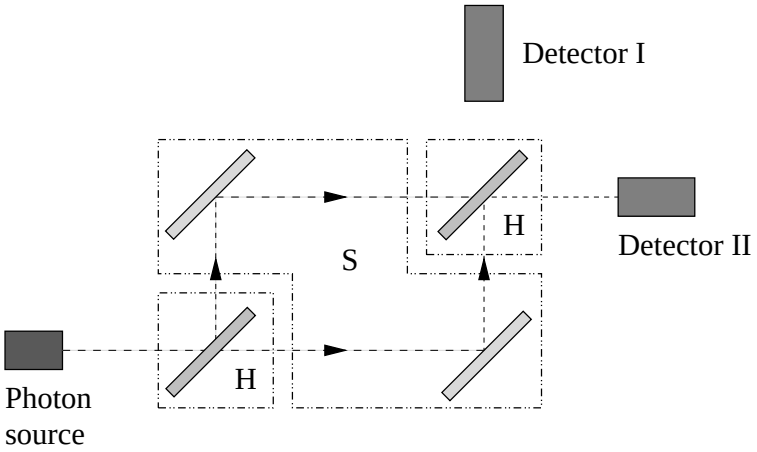
It should be noted that only the measurement of the output introduces some randomness. The behavior of the semi-silvered mirror is fully deterministic, and can be viewed as an action of a unitary operator on the state space $\mathbf{C}^2$. In fact, if one of the coefficients in the linear combination $a|0\rangle + b|1\rangle$ is zero, say $b = 0$, then we will always observe 0. We will see some examples later on.

The two fully silvered mirrors may also be viewed as a device with two input ports and two output ports.



The behavior is $S|0\rangle = i|1\rangle$ and $S|1\rangle = i|0\rangle$. Thus, a photon entering this device through input port 0 will be put into the state $i|1\rangle$, and can be measured with probability $1 = |i|^2$ at output port 1.

The Mach-Zehnder Experiment. Let us revisit our second experiment. The setup is a composition of the devices H, S, and H:



Our mirror devices operate as unitary operators on the state space $\mathbf{C}^2$. The behavior in then determined by $HSH|0\rangle$. By definition, we get

$$HSH|0\rangle = HS\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle\right) = H\left(\frac{i}{\sqrt{2}}|1\rangle - \frac{1}{\sqrt{2}}|0\rangle\right),$$

and the evaluation of the right hand side illustrates the destructive interference of superpositions in the second semi-silvered mirror:

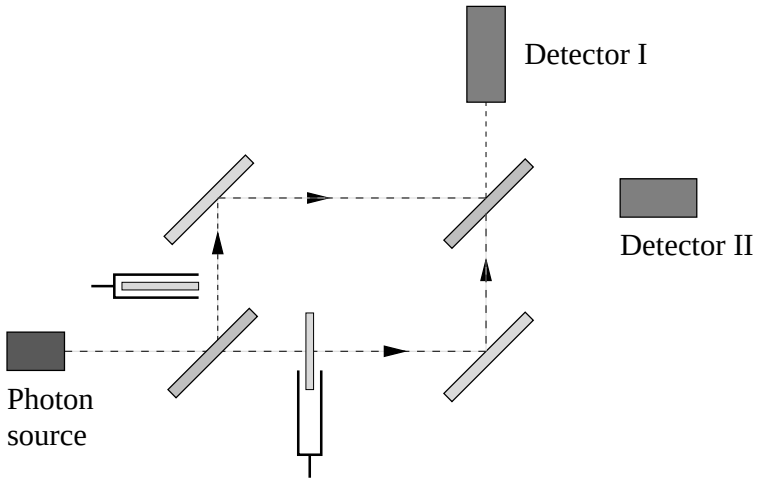
$$H\left(\frac{i}{\sqrt{2}}|1\rangle - \frac{1}{\sqrt{2}}|0\rangle\right) = \frac{i}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}|1\rangle + \frac{i}{\sqrt{2}}|0\rangle\right) - \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle\right) = -|0\rangle.$$

Hence we see that the photon will be observed with probability $|-1|^2 = 1$ at the output port 0.

Deutsch's Problem. We want to exploit the interference properties for computation. David Deutsch suggested a slight modification of our second experiment that nicely illustrates some benefits of the superposition and interference principles.

Let us assume that we are given a black box containing a Boolean function f that maps the set $\{0, 1\}$ into itself. There exist four such functions. Suppose you want to find out if the function in the black box is constant or not. On a classical computer you need more than one evaluation of the function to figure out if both function values are the same or not. Can we do better than that using our optical devices?

We install two phase shifters – some thin transparent material – after the first semi-silvered mirror. We assemble them in such a way that it is possible to slide them individually into the light beams. Each phase shifter has the effect that the probability amplitude of that light beam is multiplied by the phase factor -1. The setup is shown in the following figure:



If we slide the phase shifter following output port 0 into the path, then its effect can be described by $T_0(a|0\rangle + b|1\rangle) = -a|0\rangle + b|1\rangle$. Similarly, if we slide the other phase shifter into the vertical path, then it has the effect $T_1(a|0\rangle + b|1\rangle) = a|0\rangle - b|1\rangle$.

Let us assume for a moment that we are sitting in a completely dark optical lab. Our friend Apollo adjusts the phase shifters in an arbitrary position (he either slides the phase shifters into the path or removes them). Since we cannot see anything in the dark lab, we do not know the positions of the phase shifters. However, if we send only one single photon through the input port 0, then Detector I will register if only one phase shifter is in the path, and Detector II will register if either none or both phase shifters are in the optical paths. We can calculate this behavior rather quickly by evaluating the corresponding setups:

$f(0)$	$f(1)$	Behavior
0	0	$HSH\,\|0\rangle = -\|0\rangle$
1	0	$HST_0H\,\|0\rangle = -i\,\|1\rangle$
0	1	$HST_1H\,\|0\rangle = i\,\|1\rangle$
1	1	$HST_0T_1H\,\|0\rangle = \|0\rangle$

In fact, this can be viewed as a solution to Deutsch's problem. The values of the black box function f are coded into the positions of the phase shifters. We only need one single evaluation of this function by sending a single photon through input port 0. And the outcome is completely deterministic, as can be seen from the table above.

This very simple example showed that the use of superpositions helped to reduce the number of queries to the black box function f. And we did not gain the "speed-up" at the cost of certainty.

Quantum Computing. We could try to use multiport interferometers to solve some more elaborate problems. In fact, it is not difficult to see that any unitary operator acting on a state space $\mathbf{C}^N$ can be realized with the help of beam splitters and (slightly more general) phase shifters. The downside is that the number of optical paths increases with N, since a superposition is encoded into which-path eventualities. Thus, the setup of such an interferometer gets too large to be of practical interest.

There are numerous proposed device technologies for quantum information processing that do not have those drawbacks. For example, in the nuclear magnetic resonance technology the information is encoded in the states

of coupled spin-one-half nuclei in a molecule. Another technology uses ions in a Paul radio frequency trap. No matter what kind of microscopic system is used, all technologies try to implement an abstract model of quantum computation.

The basic unit of quantum information is the quantum bit, or shortly qubit. A qubit has two reliably distinguishable states $|0\rangle$ and $|1\rangle$, resembling the classical bits 0 and 1. The state of a qubit can be a superposition $a|0\rangle + b|1\rangle$, where the coefficients satisfy $|a|^2+|b|^2 = 1$. The normalization condition on the coefficients means that this qubit behaves after a measurement like $|0\rangle$ with probability $|a|^2$, and like $|1\rangle$ with probability $|b|^2$.

If we look at a system of n qubits, say a molecule with n spin-one-half nuclei, then the state of this system can be described by a linear combination

$$\sum a_x|x\rangle \in \mathbf{C}^{2^n},$$

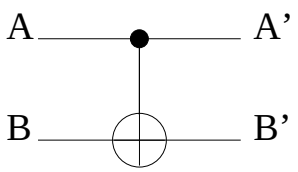
where the standard basis vectors $|x\rangle$ are labeled by bit strings of length n. The coefficient a_x are arbitrary complex numbers, assumed to be normalized such that $\sum |a_x|^2 = 1$.

It is remarkable that we do have $2^n - 1$ degrees of freedom in a system of n qubits. Basically, this means that the capacity of the memory doubles by adding a single qubit. The extraordinary size of available memory is the main advantage of quantum computing over classical computing.

Quantum Circuits. The most popular model of quantum computation is the quantum circuit model. It allows a description of algorithms as a sequence of elementary gates, somewhat similar to classical digital circuits. We cannot implement arbitrary operations, since quantum mechanics requires the operations to be unitary. This means, in particular, that it is always possible to undo an operation.

Since all operations are linear, we just need to consider the action of a gate on the basis $|x\rangle$. Let us consider a system of two qubits. A **controlled not gate** acts on the four basis vectors as follows:

$$\begin{array}{lcl} |00\rangle & \mapsto & |00\rangle \\ |01\rangle & \mapsto & |01\rangle \\ |10\rangle & \mapsto & |11\rangle \\ |11\rangle & \mapsto & |10\rangle \end{array}$$

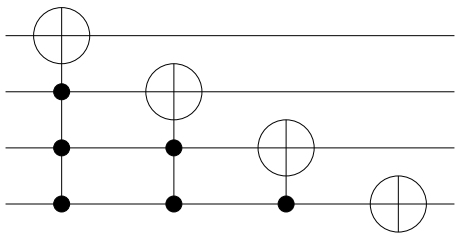


Thus, if the highest significant bit is 1, then the lowest significant bit is flipped, that is, $|A'\,B'\rangle = |A\,A \oplus B\rangle$. The most significant bit A is said to

be the **control bit** and the least significant bit B is called the **target bit** of this gate.

A controlled not operation acting on a system of n qubits can have several control bits and one target bit. The target bit is flipped if and only if all control bits are 1. For example, suppose that we have a controlled not operation on three qubits, where the two least significant bits are the control bits and the highest significant bit is the target bit $|A', B', C'\rangle = |A \oplus (B \wedge C), B, C\rangle$. In other words, this operation swaps the basis vectors $|011\rangle$ and $|111\rangle$ and leaves all other basis vectors invariant.

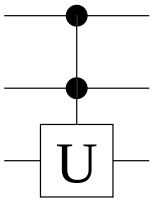
Let us construct a simple circuit with these controlled not gates. The following circuit adds 1 modulo 2^4 on the labels of the basis states, that is, $|x\rangle \mapsto |x + 1 \bmod 2^4\rangle$:



For example, if the input is $|0111\rangle$, then the leftmost gate will map this to the state $|1111\rangle$, and the next three gates change this state as follows: $|1111\rangle \mapsto |1011\rangle \mapsto |1001\rangle \mapsto |1000\rangle$. Hence $7 = 0111_2$ is mapped to $8 = 1000_2$.

The controlled not gates are basically classical reversible operations. We also have operations available that act on a single qubit by a unitary operation U, say given by $|0\rangle \mapsto a|0\rangle + b|1\rangle$, $|1\rangle \mapsto c|0\rangle + d|1\rangle$. A **controlled U gate** applies this single qubit operation only if the conditions on the control bits are satisfied. For example, the following gate applies the operation U on the least significant bit if the two most significant bits are 1:

$$\begin{array}{lcl} |110\rangle & \mapsto & a|110\rangle + b|111\rangle \\ |111\rangle & \mapsto & c|110\rangle + d|111\rangle \end{array}$$



All other basis vectors are left invariant. We obtain a controlled not gate as a special case if we set $a = 0$, $b = 1$, $c = 1$, and $d = 0$.

Universality. The controlled U gates implement rather special unitary operators. It is natural to ask what kind of operations can be implemented by sequences of such gates.

> *All unitary operators acting on $\mathbf{C}^{2^n}$ can be implemented by a finite number of controlled U operations, where $U \in U(2)$.*

A simple proof goes as follows. Let us convince ourselves that we can realize all permutations of the basis vectors $|x\rangle, x \in \mathbf{F}_2^n$. We know that the transposition $(0, 1)$ can be realized with a single controlled not operation. The full cycle $(0, 1, \ldots, 2^n - 1)$ can be realized by the circuit $|x\rangle \mapsto |x + 1 \bmod 2^n\rangle$, which is just a sequence of n controlled not gates, as shown in the previous section. However, it is a well-known fact that the symmetric group is generated by the full cycle and a transposition. Thus, we can indeed construct all operations that permute the basis vectors.

By assumption, we have all controlled U operations available that operate just on the least significant bit, with all other bits as control bits. In other words, these are plane unitary operation that act only in the plane spanned by the basis vectors $|00\ldots00\rangle$ and $|00\ldots01\rangle$. By conjugating with permutation matrices we get all plane unitary operations, that is, unitary operators that act in a plane spanned by two basis vectors, leaving all other basis vectors invariant. However, it is well-known that each unitary operator in the unitary group $U(2^n)$ is a product of a finite number of plane unitary operations [2], which completes the proof.

Sometimes it is undesirable to have an interaction between many qubits. In this case one would like to use only gates with few (if any) control bits. It is not difficult to show that unitary operations acting on a single qubit (without controls) and the controlled not operation with a single control bit generate the unitary group $U(2^n)$, see [1].

Error Control. So far we have assumed that our qubits are perfectly isolated from the environment. Such an assumption is of course completely unrealistic. For example, if we want to simulate a complex system on a quantum computer, then the memory needs to be protected against decoherence.

The advantage of a quantum computer is that superpositions of basis vectors, like

$$\frac{1}{\sqrt{2}}|00\ldots0\rangle + \frac{1}{\sqrt{2}}|11\ldots1\rangle \in \mathbf{C}^{2^n},$$

are available. However, if a single qubit is observed in this superposition, then it collapeses either to $|00\ldots0\rangle$ or to $|11\ldots1\rangle$.

A very simple code that encodes one qubit into nine qubits was proposed by Peter Shor [5]. This code is not particularly efficient, but it illustrates all essential features of a quantum error control code. I just give a rough outline, more details can be found in [3, 4, 5].

The two states $|0\rangle$ and $|1\rangle$ are encoded as follows:

$$|0\rangle \;\mapsto\; |\mathbf{0}\rangle = \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle)$$

$$|1\rangle \;\mapsto\; |\mathbf{1}\rangle = \frac{1}{2\sqrt{2}}(|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle)$$

Suppose that a single qubit is affected by some error, say the highest significant bit flips between 0 and 1. Then the state $|\mathbf{0}\rangle$ is distorted

$$\frac{1}{2\sqrt{2}}(|100\rangle + |011\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle)$$

However, it is easy to construct a circuit implementing the majority logic to undo this kind of error. A similar circuit can be implemented that corrects an error in the sign – a phase flip. Both circuits will use some additional qubits to calculate the parity checks. Thus, we will be able to correct a single bit flip X, or a single phase flip Z, or a combined bit and phase flip error Y. However, a general error affecting only a single qubit is a linear combination of the identity operator I, and the three error operators X, Y, and Z. Basically, the additional parity qubits will be in a superposition of states reporting the various kinds of errors. Measuring these parity bits and restoring the indicated error restores the previous (undistorted) state.

It is possible to implement the gate operations fault-tolerantly using such error control techniques with a poly-logarithmic overhead.

Conclusions. This paper gave a short introduction to the main principles of quantum computing. The quantum mechanical principles allow rapid computation of certain problems. The famous integer factoring algorithm by Shor indicates that some problems can be rapidly solved on a quantum computer which do not seem to have polynomial time algorithms on a classical computer. The proof of the universality of quantum gates that I have given here seems to be simpler and – in my opinion – more transparent than other proofs.

Acknowledgments. I thank the Santa Fe Institute for support though their Fellow-at-Large program, and the European Community for support through the grant IST-1999-10596 (Q-ACTA).

References

[1] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter. Elementary gates for quantum computation. *Physical Review A*, 52(5):3457–3467, 1995.

[2] W. Givens. Computation of plane unitary rotations transforming a general matrix to triangular form. *J. Soc. Indust. Appl. Math.*, 6(1):26–50, 1958.

[3] D. Gottesman. An introduction to quantum error correction. Eprint: quant-ph/0004072, April 2000.

[4] A.Y. Kitaev. Quantum computations: algorithms and error correction. *Russian Math. Surveys*, 52(6):1191–1249, 1997.

[5] P. Shor. Scheme for reducing decoherence in quantum memory. *Phys. Rev. A*, 2:2493–2496, 1995.