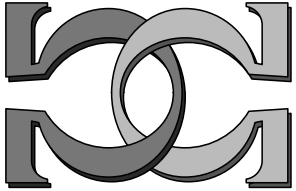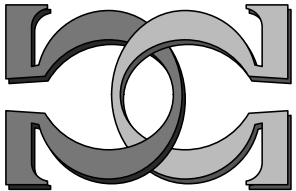# CDMTCS
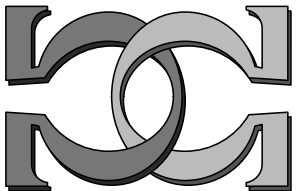# Research
Report
Series

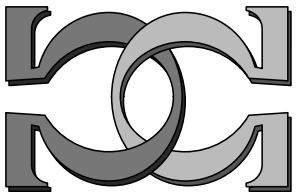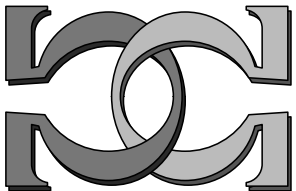# Inexpensive Linear-Optical Implementations of Deutsch's Algorithm

Michael Stay

Department of Computer Science,
University of Auckland

Centre for Discrete Mathematics and
Theoretical Computer Science

Inexpensive Linear-Optical Implementations of Deutsch's Algorithm

Michael Stay[1]

11 June 2004

Deutsch's algorithm was the first algorithm proposed for which quantum computers could outperform classical computers. It requires only a single qubit; since photons make very stable qubits, and expensive materials are only needed for multi-qubit gates, one can implement Deutsch's algorithm using inexpensive, readily available parts. Here we describe two implementations. Such a computer can be useful in demonstrating simple quantum effects.

Brief history

Quantum computation is a relatively new field; Richard Feynman [F82] proposed the idea that one well-controlled quantum system could simulate another, more inaccessible system. Since then, several algorithms have been published specifically for quantum computers. In [D85], David Deutsch published a design for a universal quantum computer, and later published the first algorithm for which a quantum computer could outperform a classical computer [DJ92], of which we present an implementation below. Two years later, Peter Shor invented one of the two algorithms that justify all the money being spent in researching quantum computation: an algorithm to factor large integers in polynomial time [S94]; if quantum computers ever reach the point where they can control thousands of quantum bits for millions of steps, then the asymmetric

cryptography that protects nearly all of the world's financial transactions will be broken. One year later, Shor gave the first example of a quantum error-correcting code, a necessary tool for achieving that goal. Lov Grover published the next important algorithm in [G97], an unordered database search. This algorithm has the potential to affect the design of symmetric cryptosystems, since it effectively halves the length of a symmetric key.

Implementations

In the latter part of the 1990s and early part of this decade, considerable progress has been made towards the implementation of a quantum computer. In most implementations, like nuclear magnetic resonance (NMR) and ion traps, the quantum sytems are extremely sensitive to the environment and need to be cooled and shielded. Optical quantum computers are one strong possibility for scalable quantum computation, because photons are extremely stable quantum systems—so stable, in fact, that the major hurdle is getting the photons to interact with each other at all! One proposal [T03] for making an optical quantum computer involves the use of the optical Kerr effect. Kerr media can be used to form the so-called "controlled-phase rotation" gate.

Since Kerr media is bulky, difficult to work with, and expensive, other ways of doing optical quantum computation are being researched. In [KLM01], Knill, Laflamme, and Milburn describe quantum gates made entirely out of linear optics: cheap, reliable, and easy-to-use. The downside is that the gates are only probabalistic; the output channel decreases in brightness for each gate used. Deutsch's algorithm, however, requires only a

single qubit, so in implementing it, we can avoid all the problems with interaction between qubits.

Linear-optical quantum gates

The simplest quantum system is the quantum-bit, or *qubit*. We can describe a qubit mathematically by a normalized two-dimensional vector with complex elements:

$$\Psi = \begin{pmatrix} a \\ b \end{pmatrix}$$
$$aa* + bb* = 1$$

where * indicates complex conjugation. Also, there is a global phase factor that is unobservable: we can only measure the phase difference between *a* and *b*.

One-bit gates are represented mathematically as 2x2 matrices. The first gate we consider is the polarizer. It implements a projection operator that transmits an impinging photon in the state $\Psi = \begin{pmatrix} a \\ b \end{pmatrix}$ with probability *aa**, or absorbs the photon with probability *bb**. Written as a matrix, the polarizer is

$$P = \begin{vmatrix} 1 & 0 \\ 0 & 0 \end{vmatrix}.$$

Polarized film was invented in the mid 1930's by a scientist named Edwin Land. Before Land's invention, polarizers were made from two clear crystals of calcite, carefully cut and arranged such that, due to the birefringence, oppositely polarized beams of light exited at right angles to each other. They were large and expensive, and people

were trying to figure out another way to achieve the same effect. Land had a tradition of reading old science journals with his wife. They came across the account of a physician, Dr. Willam Herapath, who was researching the effect of the anti-malaria drug quinine on dogs. Herapath noted that microscopic crystals had formed in the dog's urine, and that when parallel to one another, the crystals were transparent. When they crossed at right angles, however, the crystals were dark. Herapath recognized the phenomenon as polarization and was able to grow some slightly larger crystals, but the process was inefficient and unwieldy. Land came up with the idea of embedding the crystals in a plastic sheet and aligning them—originally with a large electromagnet, and later by stretching the film. Land went on to form the very successful Polaroid company, providing these new, inexpensive polarizers.

The long molecules in the crystals act like antennae for optical wavelengths; an electron moving in response to the electric field of a photon will absorb the photon, but will only feel a restoring force perpendicular to the molecule; thus any photon reemitted by the electron will be polarized perpendicularly to the molecule.

Next, mirrors implement phase inversion. A beam of light reflecting off a mirror as aligned in Fig. 1 will have left-right polarization switched, while up-down polarization remains unaffected:

$$F = \begin{vmatrix} -1 & 0 \\ 0 & 1 \end{vmatrix}.$$

Phase inversion is a special case of phase shift. More general phase shift is implemented with cellophane: light polarized along the same axis as the stretch of the

cellophane is unaffected, whereas light polarized perpendicularly to the stretch is shifted slightly. The amount of shifting depends on the color of the light, similar to the creation of a rainbow by a prism. The difference in phase is visible as a strong blue color when viewed through a polarizer. The matrix representation of a phase shift of ? radians is as follows:

$$S = \begin{vmatrix} e^{iq} & 0 \\ 0 & 1 \end{vmatrix}.$$

Rotation of the cellophane, mirror, or polarizer is represented with the usual rotation matrix:

$$R_q = \begin{vmatrix} \cos q & \sin q \\ -\sin q & \cos q \end{vmatrix}.$$

Deutsch's Problem

Deutsch's problem was the following. Given one of the functions $f(x)$ from the sets $\{0, 1\}$ ("constant" functions) or $\{x, \neg x\}$ ("balanced" functions) as a black box, determine from which set it came by computing f on one input. One bit of information is enough to distinguish the two sets, but classically there's no way of calculating the bit we need, since it's the XOR of two function outputs. With a quantum computer, we get qubits for input and output, and we can do better.

Implementation

In the mirror-based quantum version, we have four boxes that do the following:

$$0 \rightarrow \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix} : \text{No reflections.}$$

$$x \rightarrow \begin{vmatrix} -1 & 0 \\ 0 & 1 \end{vmatrix} : \text{Horizontal reflection.}$$

$$\neg x \rightarrow \begin{vmatrix} 1 & 0 \\ 0 & -1 \end{vmatrix} : \text{Vertical reflection.}$$

$$1 \rightarrow \begin{vmatrix} -1 & 0 \\ 0 & -1 \end{vmatrix} : \text{Both horizontal and vertical reflections.}$$

or, most concisely

$$f(x) \rightarrow \begin{vmatrix} (-1)^{f(0)} & 0 \\ 0 & (-1)^{f(1)} \end{vmatrix} .$$

If we choose a horizontally or vertically polarized photon, we won't be able to tell if it was reflected: they're both symmetric horizontally and vertically. These qubits correspond to the classical inputs zero and one, and as before, we gain no information about which function it is. However, if we choose a diagonally polarized photon, then each reflection makes the resulting state perpendicular to the state immediately before:

$$F\Psi = \begin{vmatrix} -1 & 0 \\ 0 & 1 \end{vmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} -1 \\ 1 \end{pmatrix}$$

$$\Psi \cdot F\Psi = \frac{1}{2}(-1 \cdot 1 + 1 \cdot 1) = 0$$

Deutsch's algorithm, then, proceeds like this:

1. Turn the input polarizer to 45 degrees.

2. Turn the output polarizer to 45 degrees.

3. Shine light into the box. If we don't see any light coming out, it's a constant function; otherwise it's a balanced function.

Mathematically, the algorithm can be represented as

$$D=(R_{p/4}P)(R_{p/2}F)^{f(0)}F^{f(1)}(R_{p/4}P)$$

See figures 1, 2, and 3.

The cellophane-based implementation is similar:

$$0 \rightarrow \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix}$$: No layers of cellophane.

$$x \rightarrow \begin{vmatrix} e^{iq} & 0 \\ 0 & 1 \end{vmatrix}$$: One layer, aligned horizontally.

$$\neg x \rightarrow \begin{vmatrix} 1 & 0 \\ 0 & e^{iq} \end{vmatrix}$$: One layer, aligned vertically.

$$1 \rightarrow \begin{vmatrix} e^{iq} & 0 \\ 0 & e^{iq} \end{vmatrix}$$: Two layers, aligned horizontally and vertically, respectively.

or,

$$f(x) \rightarrow \begin{vmatrix} e^{iqf(0)} & 0 \\ 0 & e^{iqf(1)} \end{vmatrix}.$$

As before, horizontally and vertically polarized photons pass through visibly unaffected; while the phase does get shifted, the shift is global, and therefore unmeasurable. Diagonally polarized photons acquire a phase difference between the components when there's a single layer of cellophane and only blue photons pass through unabsorbed.

The only difference between the outcomes in this case is that instead of blocking the light completely in the balanced case, it blocks all colors but blue. See figures 4, 5.

Mathematically, the algorithm can be represented as

$$D = (R_{p/4}P)(R_{p/2}S)^{f(0)} S^{f(1)} (R_{p/4}P)$$

Conclusion

Since photons are such stable qubits, and since Deutsch's algorithm only requires one, a linear-optical implementation of his algorithm is well within even the most restricted budgets and can help to illustrate some of the basic concepts of quantum computation.

[D85] Deutsch, D. "Quantum Theory, the Church-Turing Principle, and the Universal Quantum Computer" Proc. Roy. Soc. Lond. A400 (1985) pp. 97-117.

[DJ92] David Deutsch, Richard Jozsa. Rapid solutions of problems by quantum computation. Proceedings of the Royal Society of London, Series A, vol. 439, pp. 553, 1992.

[F82] Feynman, R. P. "Simulating Physics with Computers" International Journal of Theoretical Physics, Vol. 21 (1982) pp. 467-488.

[G96] Grover, L. K. "A Fast Quantum Mechanical Algorithm for Database Search" Proceedings of the 28th Annual ACM Symposium on the Theory of Computing, Philadelphia, (1996) pp. 212-219.

[KLM01] Knill E., Laflamme R. and Milburn G. "A scheme for efficient quantum computation with linear optics" Nature 409 (2001) pp. 46-52

[S94] Shor, P. "Algorithms for quantum computation: discrete logarithms and factoring" Proceedings 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, USA, 20-22 Nov. 1994, IEEE Comput. Soc. Press (1994) pp. 124-134.

[T03] Tanas, R. "Nonclassical states of light propagating in Kerr media", in Theory of Non-Classical States of Light , eds. V. Dodonov and V. I. Man'ko (Taylor & Francis, London, 2003) p. 267
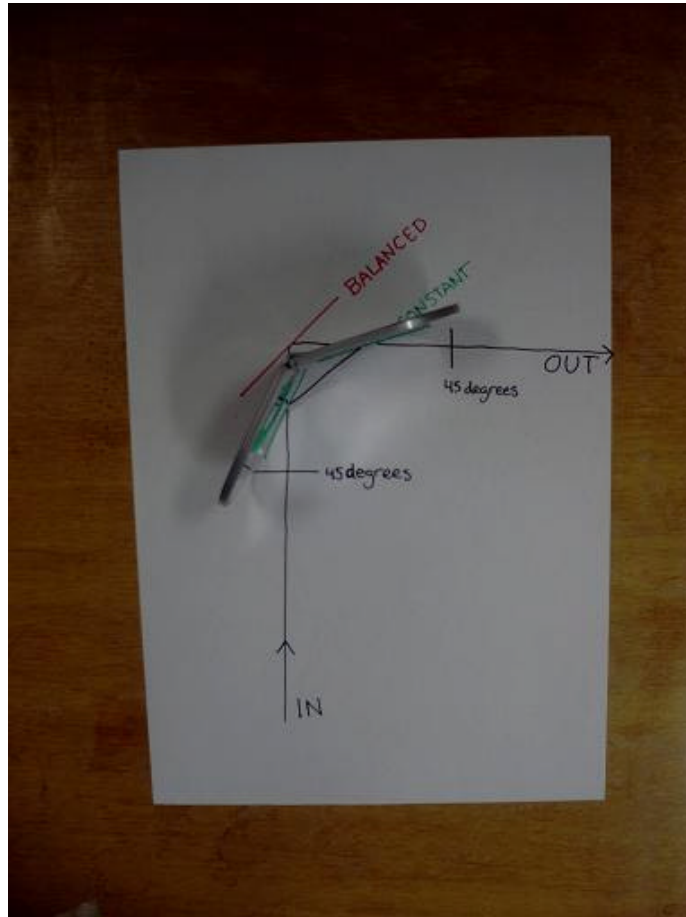
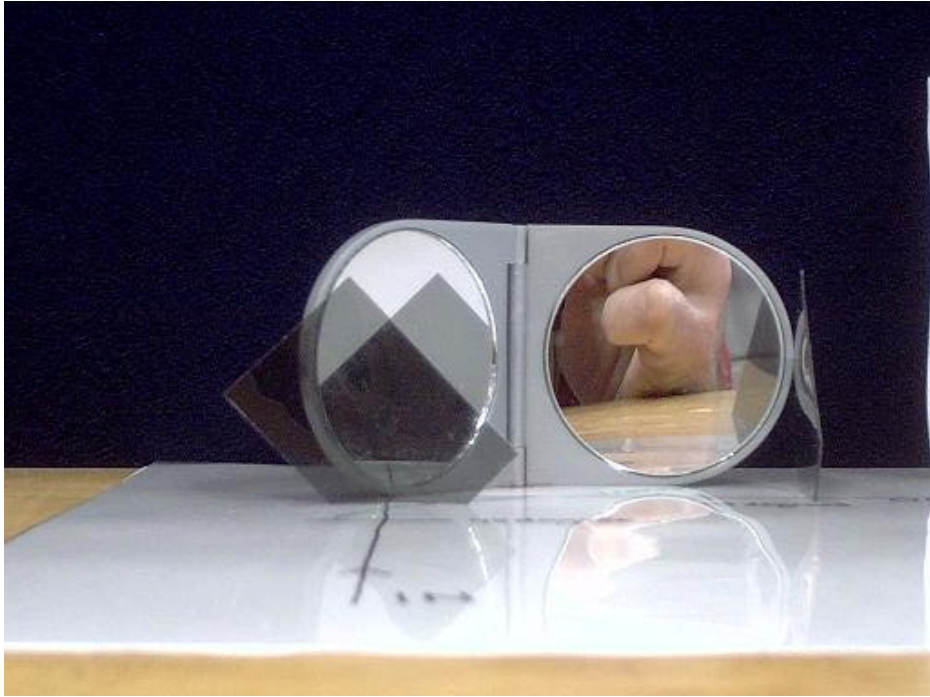Fig. 1: Layout of mirror-based implementation

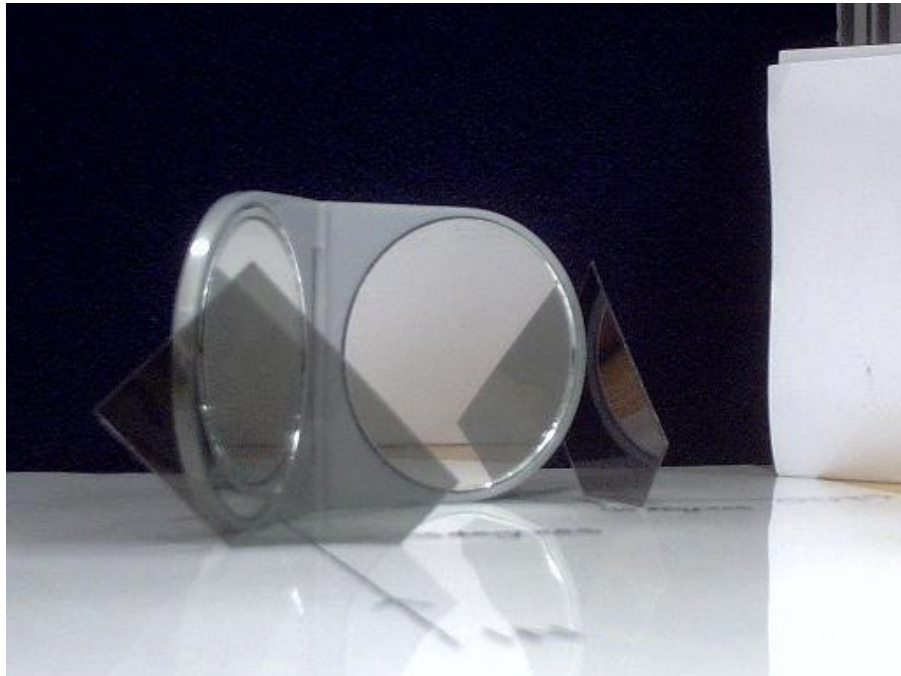Fig. 2: Balanced function

Fig. 3: Constant function

Fig. 4: Cellophane-based implementation. There are two layers of cellophane aligned perpendicularly. Where they overlap, both components of the phase are shifted the same amount, giving rise to an unobservable global phase shift.

Fig. 5: Cellophane aligned with the polarizer, simulating classical inputs; we gain

no information.