Quantum Computing

James A. Foster

October 29, 1997

List of Slides

Slide 1

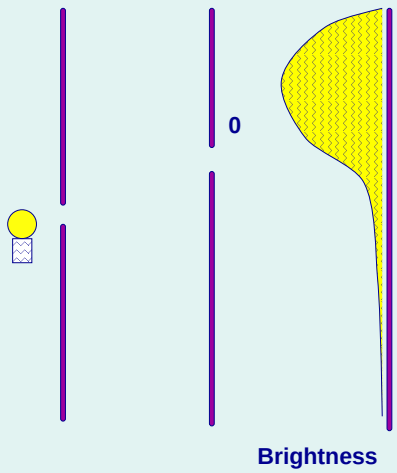
Outline

- Quantum states
- Quantum registers
- Quantum programs
- Factoring in polynomial time
- Computational complexity
- Problems
- Possibilities
- Further reading

Quantum Computing

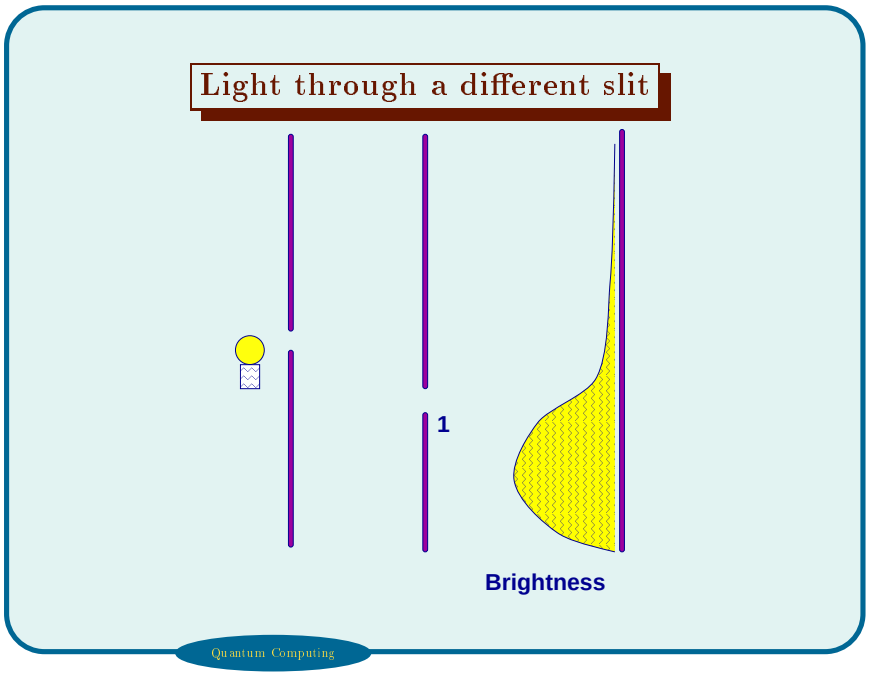
Slide 2

Light through a single slit

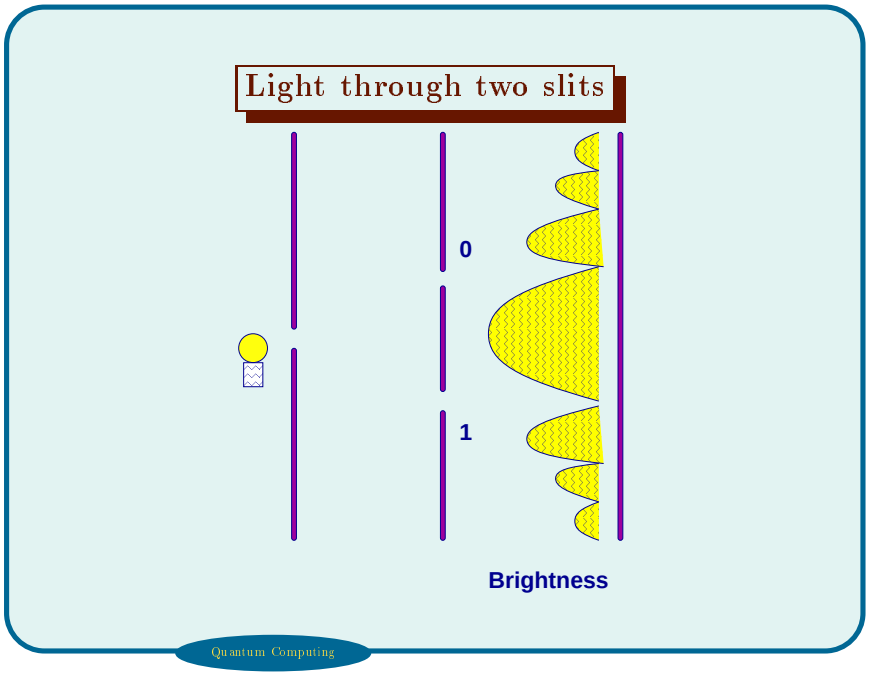


Quantum Computing

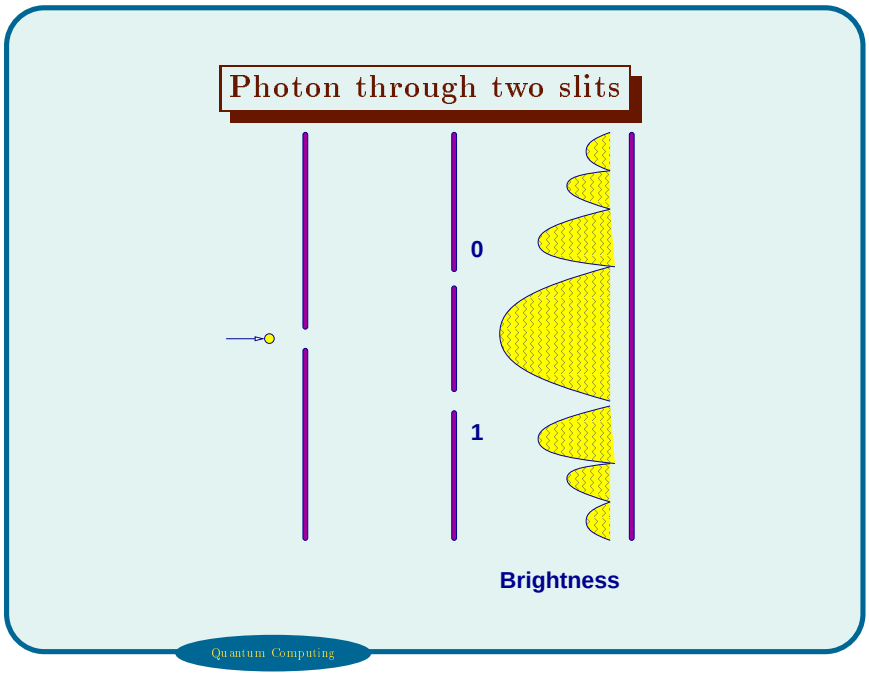
Slide 3



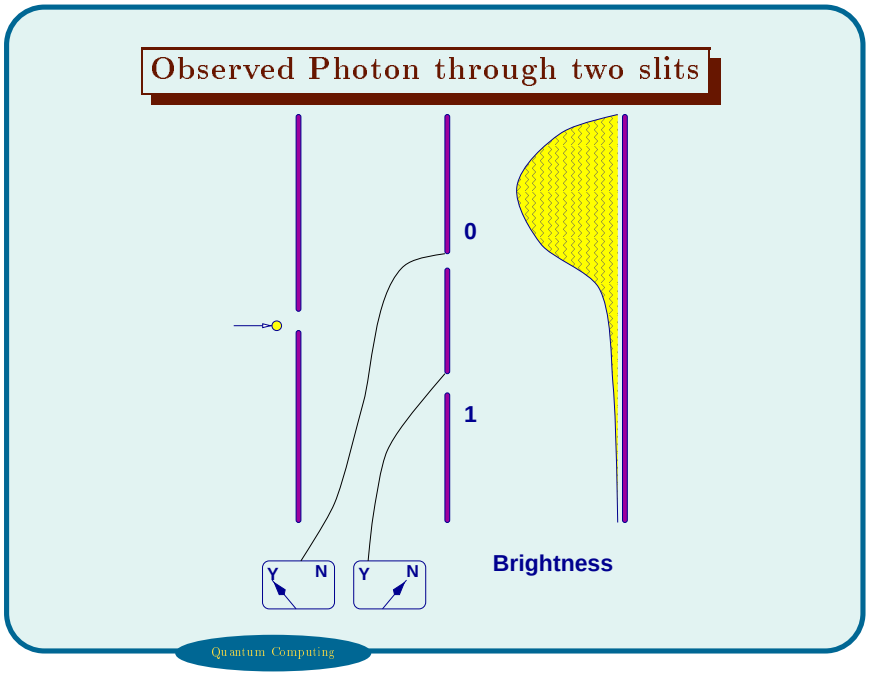
Slide 4



Slide 5



Slide 6



Slide 7

Quantum States

Quantum particles *interfere* (constructively or destructively) with themselves

Quantum state: linear combination of possible observations

Qubit (quantum bit): $\boxed{B} = \alpha \cdot \boxed{0} + \beta \cdot \boxed{1}$

- Complex α, β (*amplitudes* of $\boxed{0}$ and $\boxed{1}$)
- Such that $\alpha^2 + \beta^2 = 1$
- $O(\boxed{0}) = \alpha^2$, $O(\boxed{1}) = \beta^2$

$O(\boxed{x})$ is probability of observing $\boxed{x}$ (which *collapses* the given quantum object to $\boxed{x}$)

Quantum Computing

Slide 8

Possible Qubits

Qubit	$O(\boxed{0})$	$O(\boxed{1})$
$\frac{1}{\sqrt{2}}\boxed{0} + \frac{1}{\sqrt{2}}\boxed{1}$	$\frac{1}{2}$	$\frac{1}{2}$
$\frac{1}{\sqrt{2}}\boxed{0} - \frac{1}{\sqrt{2}}\boxed{1}$	$\frac{1}{2}$	$\frac{1}{2}$
$-\frac{1}{\sqrt{2}}\boxed{0} + \frac{1}{\sqrt{2}}\boxed{1}$	$\frac{1}{2}$	$\frac{1}{2}$
$-\frac{1}{\sqrt{2}}\boxed{0} - \frac{1}{\sqrt{2}}\boxed{1}$	$\frac{1}{2}$	$\frac{1}{2}$
$\boxed{1} = 0 \cdot \boxed{0} + 1 \cdot \boxed{1}$	0	1
$\boxed{0} = 1 \cdot \boxed{0} + 0 \cdot \boxed{1}$	0	1
$\frac{1}{2}\boxed{0} - \frac{\sqrt{3}}{2}\boxed{1}$	$\frac{1}{4}$	$\frac{3}{4}$

Quantum Computing

Slide 9

Registers

Quantum Register $\boxed{\vec{x_n}}$: n qubits

Example: $\boxed{\vec{x_2}} = \frac{1}{2}\boxed{00} + \frac{1}{2}\boxed{01} + \frac{1}{2}\boxed{10} + \frac{1}{2}\boxed{11}$

Note: $O(\boxed{00}) = O(\boxed{01}) = O(\boxed{10}) = O(\boxed{11}) = \frac{1}{4}$ so observing $\boxed{\vec{x_2}}$ gives a (truely) random number from $\{0 \ldots 3\}$

Example: $\boxed{\vec{x_2}} = \frac{1}{\sqrt{2}}\boxed{00} + \frac{1}{\sqrt{2}}\boxed{11}$

Note: $O(\boxed{00}) = O(\boxed{11}) = \frac{1}{2}$, but $O(\boxed{01}) = O(\boxed{10}) = 0$

So, observing first bit *fixes value of second bit* (even if the bits are light years apart)

Quantum Computing

Slide 10

Entanglement and Interference

Bits in $\boxed{\vec{x_n}}$ are *entangled* if observing some causes amplitudes of others to collapse

Entangled bits can interfere with each other *constructively* (amplitudes increase) or *destructively* (decrease)

Quantum Computing (for algorithm U):

`Entangle all possible inputs into` $\boxed{\vec{x_n}}$ `with`
  `''yes'' answers interfering constructively`
  `''no'' answers interfering destructively`
`Compute` $U(\boxed{\vec{x_n}}) \mapsto \boxed{U(\vec{x_n})}$
`Observe` $\boxed{U(\vec{x_n})}$

Quantum Computing

Slide 11

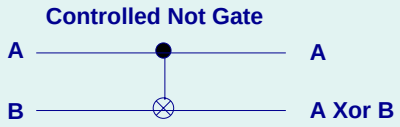
Computing with quantum registers

Algorithm $U(\boxed{x}) \mapsto \boxed{U(x)}$: U Transforms input quantum state to output quantum state—U must be *unitary*: no information loss

Example: controlled not (reversible XOR)

C-Not Truth Table

Input		Output	
A	B	A	B
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0



`C-not` $(\boxed{A}\boxed{B}) \equiv$ `if` $(\boxed{A} = 1)$ `then` $\boxed{B} \leftarrow \neg \boxed{B}$

Slide 12

Example unitary transformation

$$\texttt{QCF}(\boxed{A}) = \begin{cases} \frac{1}{\sqrt{2}}\boxed{0} - \frac{1}{\sqrt{2}}\boxed{1} & \text{if } \boxed{A} = \boxed{0} \\ \frac{1}{\sqrt{2}}\boxed{0} + \frac{1}{\sqrt{2}}\boxed{1} & \text{if } \boxed{A} = \boxed{1} \end{cases}$$

Notice that `QCF`$(\boxed{0})$ and `QCF`$(\boxed{1})$ both randomize the input so that $O(\boxed{0}) = \frac{1}{2}$ using either

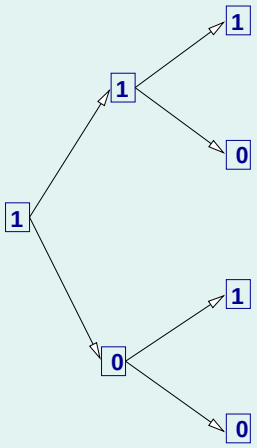
But, `QCF`(`QCF`$(\boxed{0})) = \boxed{1}$ and `QCF`(`QCF`$(\boxed{1})) = \boxed{0}$, so double application of `QCF` is an XOR

So, `QCF` can be used to entangle all possible values for a quantum register

Slide 13

Example of interference

Tracing Amplitudes from QCF(QCF(1))



Quantum Computing

Slide 14

General computation

If f is unitary, then

Input: Quantum register $X = \vec{x_n}$, qubit y

$X \leftarrow \vec{0}_n$

$X \leftarrow$ QCF(X)

// X superimposes all possible inputs

$y \leftarrow f(X)$

// y superimposes all possible outputs of $f(x)$

Observe y

If desirable (undesirable) outputs of f interfere positively (negatively) observation is the answer

Note: exponentially many inputs are computed simultaneously

Quantum Computing

Slide 15

Factoring in polynomial time

Thm: any number x can be factored in polynomial time using quantum registers and unitary operations

There is a unitary $E(x, n, \boxed{\vec{0}}) = \boxed{r}$ such that $x^r = 1 \pmod{n}$ (computes $x^a \pmod{n}$ for all possible a, uses qFFT to get construstive interference for multiples of r)

To find one factor of any x (whp):

Input: x
Choose a random y in $\{0 \ldots x\}$
Let $\boxed{r} \leftarrow \mathrm{QCF}(\vec{0_n})$ for appropriate n
Compute $r \leftarrow E(x, n, \boxed{\vec{0}})$
If r is odd or $x^{r/2} = -1 \pmod{n}$ then fail
  else return $\gcd(x^{r/2} - 1, n)$

Quantum Computing

Slide 16

Implications for cryptography

Quantum computers will be able to break public key encryption based on factoring (or discrete log)

They will not be able to break information theoretic encryption (such as one-time pads)

Quantum transformations have been used for *quantum cryptography*, which is secure from quantum attacks (but not from some classical attacks)

Quantum Computing

Slide 17

Complexity

Factoring is not known to be in P, but is in "quantum" P

Polynomial time on quantum computers is stronger than on Turing machines

The real world is quantum, so this is not hand waving

Quantum Computing

Slide 18

Problems

Decoherence: Quantum systems tend to decay into classical states

Time for unitary operations proportional to decoherence time

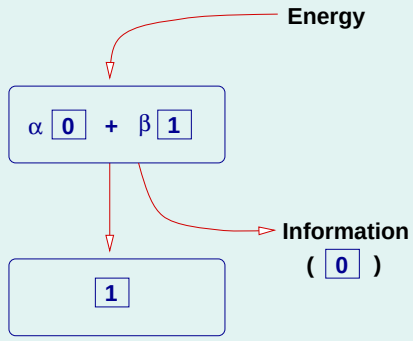
Proving an operation unitary is difficult

Programming is hard (you can't access variables indiscriminately)

Quantum Computing

Slide 19

Decoherence Illustration



Quantum Computing

Slide 20

Possibilities

A n qubit computer can perform 2^n operations simultaneously

True random numbers are possible

n qubits can store 2^n bits of data

May change the way we look at computation

Quantum Computing

Slide 21

Further reading

A. Barenco, "Quantum Physics and Computers", manuscript

E. Bernstein and U. Vazirani, "Quantum Complexity Theory", *Proc. 25th Symp. on Theory of Computing*, pp. 11–20, 1993.

A. Bertiaume, "Quantum Computation", manuscript

G. Brassard, "A Quantum Jump in Computer Science", *Computer Science Today*, J. van Leeuwen, ed., LNCS 1000, 1995.

See the links from the bookmarks on my homepage

Quantum Computing

