

What's the deal with Quantum Computing

How to break RSA

Maksim Levental

January 12, 2015

- A single qubit is a (unit length) linear combination of the basis vectors

$$\psi = \alpha |0\rangle + \beta |1\rangle$$

- Measurement \iff non-deterministic wave function collapse
 \iff all information lost
- Unitary transformations correspond to gates. 1-qubit gates are matrices

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

- n -qubit systems (registers) are represented by vectors (tensors) in the tensor product of the vector spaces that each of the individual qubits are elements of

$$\left(\frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \right) \otimes \left(\frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \right) = \frac{1}{2} \left(|0\rangle |0\rangle + |0\rangle |1\rangle + |1\rangle |0\rangle + |1\rangle |1\rangle \right)$$

- Gates on single qubit systems also map to “ n -gates” on n -qubit systems (entrywise)

$$\begin{aligned} H^{\otimes 2} |0\rangle |0\rangle &= (H |0\rangle) \otimes (H |0\rangle) \\ &= \left(\frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \right) \otimes \left(\frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \right) \end{aligned}$$

- Entangled states are important: for $\psi \in V \otimes W$ there **do not exist** $\phi \in V$ and $\varphi \in W$ such that

$$\psi = \frac{|0\rangle |0\rangle + |1\rangle |1\rangle}{\sqrt{2}} = \phi \otimes \varphi$$

“Reversible computation without can be done **efficiently**, without the production of garbage bits whose values depend on the input to the computation. That is, if there is an irreversible circuit computing a function f , then there is an efficient simulation of this circuit by a reversible [unitary transformation/quantum] circuit with action” [4]

$$|x\rangle |y\rangle \rightarrow |x\rangle |y \oplus f(x)\rangle$$

Deutsch's Problem

Let $f(x) : \{0, 1\} \rightarrow \{0, 1\}$ and suppose we are guaranteed that f is either balanced (1 on half of its domain and 0 on the other half) or constant (1 or 0 on the entire domain). How many evaluations classically to discriminate? “Quantumly” you only need to evaluate f once! Let U_f be the quantum circuit such that

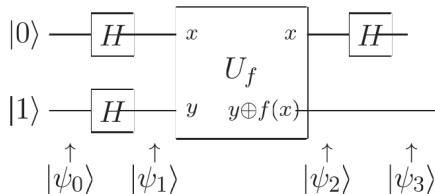
$$U_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle$$

With some algebra (keeping in mind the small-ish domain and range of f)

$$U_f \left(|x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \right) = (-1)^{f(x)} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

Deutsch's Algorithm

Construct the quantum circuit



$$|\psi_1\rangle = H^{\otimes 2} (|0\rangle \otimes |1\rangle)$$

$$\psi_2 = U_f |\psi_1\rangle = \begin{cases} \pm \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) & \text{if } f(0) = f(1) \\ \pm \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) & \text{if } f(0) \neq f(1) \end{cases}$$

The final Hadamard gate on the first qubit gives

$$\psi_3 = \begin{cases} \pm |0\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) & \text{if } f(0) = f(1) \\ \pm |1\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) & \text{if } f(0) \neq f(1) \end{cases}$$

Now if we measure the first qubit we know whether $f(0) = f(1)$ or $f(0) \neq f(1)$ (depending on whether we get $|0\rangle$ or $|1\rangle$).

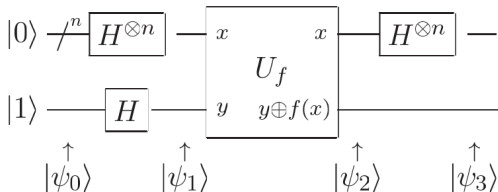
Succinctly stated this allows us to measure a global property: since $f(0) \oplus f(1) = 0$ if $f(0) = f(1)$ and 1 otherwise

$$\psi_3 = \pm |f(0) \oplus f(1)\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

Naive interpretation is that this is a randomized algorithm but in truth interference effects (the final Hadamard gate) are used to discern global properties (H is a generalized DFT).

Deutsch-Jozsa Algorithm

Generalize to $f(x) : \{0, 1\}^n \rightarrow \{0, 1\}$ and still f is either balanced or constant. How many evaluation classically? $2^n + 1$ but quantumly still 1!



$$\psi_0 = |0\rangle^{\otimes n} |1\rangle$$

then

$$\psi_1 = \sum_{x \in \{0,1\}^n} \frac{|x\rangle}{\sqrt{2^n}} \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

Deutsch-Jozsa Algorithm

The first register is a superposition of all basis states in the n -qubit computational basis. Using the simplification above again we have that

$$\psi_2 = U_f \psi_1 = \sum_{x \in \{0,1\}^n} \frac{(-1)^{f(x)} |x\rangle}{\sqrt{2^n}} \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

and the last Hadamard operator

$$\psi_3 = H^{\otimes n} \psi_2 = \sum_{z \in \{0,1\}^n} \sum_{x \in \{0,1\}^n} \frac{(-1)^{x \cdot z + f(x)} |x\rangle}{2^n} \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

where $x \cdot z$ is bitwise inner product mod 2.

Deutsch-Jozsa Algorithm

Let's observe the top register (query register). Note that the amplitude for $|0\rangle^{\otimes n}$ is $\sum_x (-1)^{f(x)} / 2^n$. If f is constant then

$$\sum_{x \in \{0,1\}^n} \frac{(-1)^{f(x)}}{2^n} = \pm 1$$

and because ψ_3 must be unit length we will certainly measure ψ_3 to be in the $|0\rangle^{\otimes n}$ state. If f is balanced then by definition of balanced ($f(x)$ will be even as often as odd)

$$\sum_{x \in \{0,1\}^n} \frac{(-1)^{f(x)}}{2^n} = 0$$

and we will certainly measure something other than $|0\rangle^{\otimes n}$.

Factoring integers - reduction to order finding

Pick $x < N$. If x and N have a common factor then $\gcd(x, N)$ can be computed classically in polynomial time using Euclid's algorithm. Otherwise compute the order of x ; the least r such that

$$x^r \equiv 1 \pmod{N}$$

With probability $p > 1 - \left(\frac{1}{2}\right)^q$, where q is the number of prime factors in N , the order of x will be even. Then

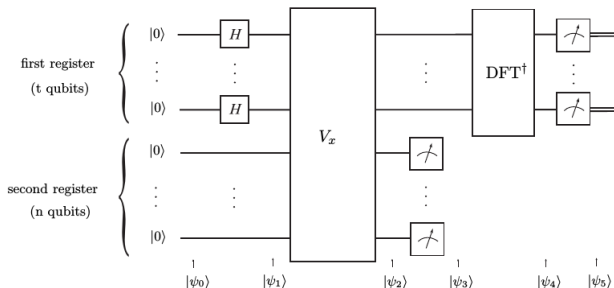
$$x^r - 1 \equiv (x^{r/2} - 1)(x^{r/2} + 1) \equiv 0 \pmod{N}$$

and hence N divides $(x^{r/2} - 1)(x^{r/2} + 1)$. If $1 < x^{r/2} < N - 1$ then

$$0 < (x^{r/2} - 1) < (x^{r/2} + 1) < N$$

and hence $(x^{r/2} - 1)$, $(x^{r/2} + 1)$ must each have a factor of N . Compute $\gcd(x^{r/2} - 1, N)$ and $\gcd(x^{r/2} + 1, N)$.

Shor's Algorithm



where

$$V_x (|j\rangle |k\rangle) = |j\rangle |k + x^j\rangle$$

and

$$DFT (|k\rangle) = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i j k / N} |j\rangle$$

Shor's Algorithm

Then

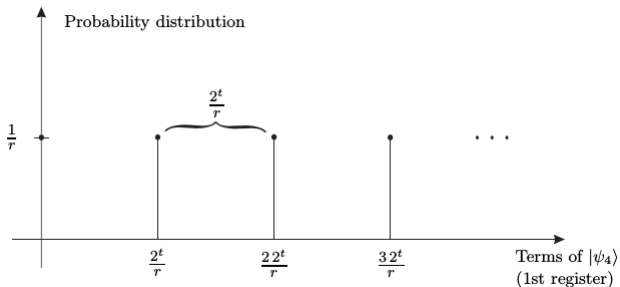
$$|\psi_2\rangle = \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle |x^j\rangle \stackrel{r|2^t}{=} \frac{1}{\sqrt{2^t}} \sum_{b=0}^{r-1} \sum_{a=0}^{\frac{2^t}{r}-1} |ar + b\rangle |x^b\rangle$$

$$|\psi_3\rangle = \sqrt{\frac{r}{2^t}} \sum_{a=0}^{\frac{2^t}{r}-1} |ar + b_0\rangle |x^{b_0}\rangle$$

$$|\psi_4\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{2\pi i \frac{k}{r} b_0} \left| \frac{k2^t}{r} \right\rangle |x^{b_0}\rangle$$

Shor's Algorithm

Assuming the order of x , r is a multiple of 2 (can be generalized), after measuring the first register we have $|\psi_5\rangle = |\frac{k_0 2^t}{r}\rangle$



If $k_0 = 0$ then we rerun. Otherwise divide $k_0 2^t / r$ by 2^t . If k_0, r are coprime then we can just take the denominator of k_0 / r . Otherwise $r = r_1 r_2$ and we can find the order of x^{r_1} to find r .

Simon's problem and complexity results

Let $f(x) : \{0, 1\}^n \rightarrow \{0, 1\}^n$ and we are guaranteed that $\exists s \in \{0, 1\}^n$ such that

$$f(y) = f(z) \iff (y = z \vee y \oplus z = s)$$

Find s . Classically $\Omega(2^{n/2})$ while quantumly $O(n)$. Also quantumly optimal; any quantum algorithm needs to make $\Omega(n)$.

Yields an oracle separation between **BPP** and **BQP**.

Deutsch-Josza only yields a separation between **P** and **EQP**

Let $f(x) : \{0, 1\}^n \rightarrow \{0, 1\}$ be the PARITY function. Classically how many operations must be performed for f to be computed? Quantumly only $n/2$ queries to the bit string need to be made [1].

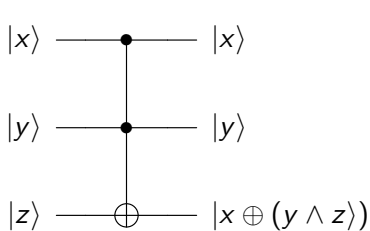
Compute the “square-free” part of an integer N , i.e. r such that

$$N = r \cdot s^2$$

No known polynomial time classical algorithm; “almost” as hard as factorization itself [?]. Quantumly in $O\left((\log \log N)^2\right)$ [?].

Interestingly while this algorithm uses the Fourier transform it is exact (as opposed to Shor’s).

Physical gates



$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Toffoli gate

Toffoli is classically universal but not quantum universal, but $\{TOF, H\}$ are quantum universal and both have successfully implemented [2, 3].

$$\begin{aligned} U_f \left(|x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \right) &= U_f \left(\frac{|x\rangle|0\rangle - |x\rangle|1\rangle}{\sqrt{2}} \right) \\ &= \frac{|x\rangle|0 \oplus f(x)\rangle - |x\rangle|1 \oplus f(x)\rangle}{\sqrt{2}} \end{aligned}$$

Now if $f(x) = 0$ then

$$\frac{|x\rangle|0 \oplus f(x)\rangle - |x\rangle|1 \oplus f(x)\rangle}{\sqrt{2}} = \frac{|x\rangle|0\rangle - |x\rangle|1\rangle}{\sqrt{2}}$$

and if $f(x) = 1$ then because \oplus is mod 2

$$\frac{|x\rangle|0 \oplus f(x)\rangle - |x\rangle|1 \oplus f(x)\rangle}{\sqrt{2}} = \frac{|x\rangle|1\rangle - |x\rangle|0\rangle}{\sqrt{2}}$$

and so

$$\begin{aligned} U_f \left(|x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \right) &= U_f \left(\frac{|x\rangle|0\rangle - |x\rangle|1\rangle}{\sqrt{2}} \right) \\ &= \frac{|x\rangle|0 \oplus f(x)\rangle - |x\rangle|1 \oplus f(x)\rangle}{\sqrt{2}} \end{aligned}$$

Succintly put

$$U_f \left(|x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \right) = (-1)^{f(x)} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

$$\begin{aligned} |\psi_1\rangle &= H^{\otimes 2}(|0\rangle \otimes |1\rangle) \\ &= (H|0\rangle) \otimes (H|1\rangle) \\ &= \left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right) \otimes \left(\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right) \\ &= |0\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} + |1\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \end{aligned}$$

Then

$$\psi_2 = U_f |\psi_1\rangle = \begin{cases} \pm \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) & \text{if } f(0) = f(1) \\ \pm \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) & \text{if } f(0) \neq f(1) \end{cases}$$

The final Hadamard gate on the first qubit gives

$$\psi_3 = \begin{cases} \pm |0\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) & \text{if } f(0) = f(1) \\ \pm |1\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) & \text{if } f(0) \neq f(1) \end{cases}$$

$$\psi_2 = U_f \psi_1 = \sum_{x \in \{0,1\}^n} \frac{(-1)^{f(x)} |x\rangle}{\sqrt{2^n}} \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

Now extrapolating from $H|0\rangle = \sum_{z \in \{0,1\}} (-1)^{0 \cdot z} |z\rangle / \sqrt{2}$ and $H|1\rangle = \sum_{z \in \{0,1\}} (-1)^{1 \cdot z} |z\rangle / \sqrt{2}$ applying to

$$\begin{aligned} H^{\otimes n} |x_1, \dots, x_n\rangle_{x_i \in \{0,1\}} &= \bigotimes_{i=1}^n (H |x_i\rangle)_{x_i \in \{0,1\}} \\ &= \left(\sum_{z \in \{0,1\}} \frac{(-1)^{x_i \cdot z}}{\sqrt{2}} |z\rangle \right)_{x_i \in \{0,1\}}^{\otimes n} \\ &= \sum_{z_1, \dots, z_n} \frac{(-1)^{x_1 z_1 + \dots + x_n z_n}}{\sqrt{2^n}} |z_1, \dots, z_n\rangle \end{aligned}$$

Bibliography



DE WOLF, R.

Quantum communication and complexity.

Theoretical Computer Science 287, 1 (2002), 337–353.



MOHAMMAD NEJAD, S., AND MEHMANDOOST, M.

Realization of quantum hadamard gate by applying optimal control fields to a spin qubit.

In *Mechanical and Electronics Engineering (ICMEE), 2010 2nd International Conference on* (Aug 2010), vol. 2, pp. V2–292–V2–296.



MONZ, T., KIM, K., HÄNSEL, W., RIEBE, M., VILLAR, A. S., SCHINDLER, P., CHWALLA, M., HENNRICH, M., AND BLATT, R.

Realization of the Quantum Toffoli Gate with Trapped Ions.

Physical Review Letters 102, 4 (Jan. 2009), 040501.



NIELSEN, M. A., AND CHUANG, I. L.

Quantum Computation and Quantum Information: 10th