An Introduction to Quantum Algorithms: Shor's Algorithm

M. V. Panduranga Rao

Indian Institute of Technology Hyderabad

Outline

- Some Quantum Computing
- Some Number Theory
- Shor's algorithm for integer factoring

Quantum State Vector

- State of a Classical Deterministic Bit: Either 0 or 1
- Classical Probabilistic: $a\overline{0} + b\overline{1}$ such that $a + b = 1$.
- A Quantum Bit (qubit!!): $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

  where $\alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1$
- In general, n qubits $\Rightarrow$ 2^n-dimensional Hilbert space
- A quantum state vector is a ray in the 2^n-dimensional Hilbert space:
- $|\psi\rangle = \sum_{i=0}^{2^n-1} \alpha_i|i\rangle$
- where $\alpha_i \in \mathbb{C}$ and $\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1$

Classical Deterministic Evolution

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

$M_{ij} = 1$ whenever there is a transition from configuration i to j.

Classical Probabilistic Evolution

$$M = \begin{pmatrix} 0 & 3/4 & 0 & 0 \\ 1/2 & 1/4 & 0 & 0 \\ 1/2 & 0 & 1/3 & 0 \\ 0 & 0 & 2/3 & 1 \end{pmatrix}$$

$\sum_i M_{ij} = 1.$

Quantum Evolution

- The trajectory of a closed quantum system is described by the famous Schroedinger equation

$$i\frac{h}{2\pi}\frac{d}{dt}|\psi\rangle = H|\psi\rangle.$$

- If the system evolves from time t_0 through t_1, the solution of Schroedinger equation is

$$|\psi(t_1)\rangle = e^{-iH(t_1-t_0)}|\psi(t_0)\rangle$$

where $U(t_1, t_0) = e^{-iH(t_1-t_0)}$ is a unitary operator:
$U^\dagger U = UU^\dagger = I$.

(Projective) Measurements

"Opening" the closed system (peeking in for information):

- Observable: Hermitian Operator H defined as $\sum mP_m$ such that
- $\sum P_m = I$ and
- $P_m^2 = P_m$ but $P_m P_{m'} = 0$ for $m \neq m'$.
- Probability of obtaining $m = ||P_m|\psi\rangle||^2$
- Post-measurement, the state collapses to $\frac{P_m|\psi\rangle}{||P_m|\psi\rangle||^2}$.

Example

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

- $$P_0 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \text{ and } P_1 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$
- Probability of observing a 0 = $|\alpha|^2$ at which point the system collapses to $|0\rangle$.
- Probability of observing a 1 = $|\beta|^2$ at which point the system collapses to $|1\rangle$.

Circuit Model of Quantum Computation

- A sequence of “gates” applied on qubit registers
- Measurements performed to extract information
- Gates, whatever function they implement, need to be unitary
- Can be decomposed into basic gates from universal sets of (unitary) gates, each of which operate on a small constant number of qubits
- Example– Discrete Fourier Transform:

$$DFT_q \sum_a f(a)|a\rangle \quad = \quad \sum_c \tilde{f}(c)|c\rangle$$

where $$\tilde{f}(c) = \frac{1}{\sqrt{q}} \sum_a e^{\frac{2\pi i a c}{q}} f(a)$$

Strange features of the quantum world

- Superposition
- Entanglement E.g: $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$
- Interference of probability amplitudes

Integer factoring and its importance

- Given a natural number N that is a product of two prime numbers p_1 and p_2
- Find p_1 and p_2
- In time $O(poly(\log N))$, for efficiency.
- Security of popular cryptosystems like RSA depends on the fact that we don't yet know an efficient classical algorithm for doing this!

Integer factoring reduces to order finding

- Let $1 \leq y \leq N$ and $\gcd(y, N) = 1$. The order r of $y \mod N$ is the least power of y congruent to $1 \mod N$.

- Choose a y such that $\gcd(y, N) = 1$. Then

- Theorem: If r is even for the y chosen and $x = y^{r/2} \neq \pm 1 \mod N$, then $\gcd(x \pm 1, N)$ is a non-trivial factor of N.

- Theorem: $Prob[\, r$ is even and $y^{r/2} \neq \pm 1 \mod N] \geq 1/2$

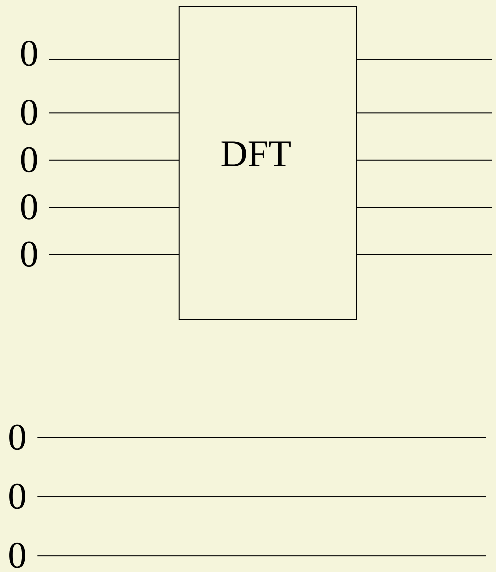
An Example

- Let us try to factorize $N = 15$.
- Candidate y's are $\{2, 4, 7, 8, 11, 13, 14\}$.
- Say we pick 11.
- $11^a \mod N$ for $a = 1, 2, 3, 4, \ldots$ are $11, 1, 11, 1, \ldots$
- Thus $r = 2$, and $x = y^{\frac{r}{2}} = 11$
- $\gcd(10, 15) = 5$ and $\gcd(12, 15) = 3$, which are the factors we are looking for.

Shor's algorithm (preparations)

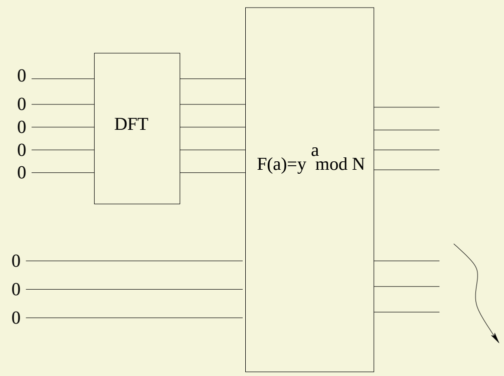
- Given N choose $q = 2^L$ between N^2 and $2N^2$
- Choose a random $y \mod N$
- Prepare two quantum registers of L bits and $range()$ qubits each as follows: $|00\ldots0\rangle|00\ldots0\rangle$

Apply DFT on first register



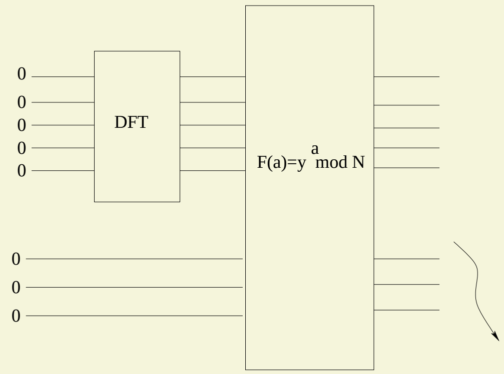
$$|00\ldots0\rangle|00\ldots0\rangle \to \frac{1}{\sqrt{q}}\sum_{a=0}^{q-1}|a\rangle|00\ldots0\rangle$$

Evaluate function



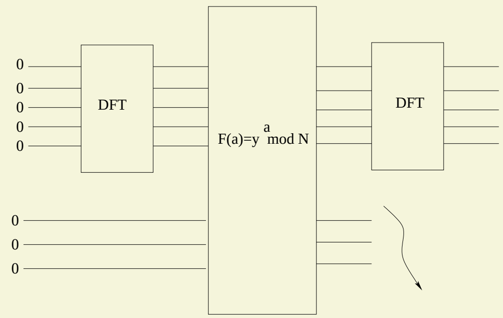
$$\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle |00\ldots0\rangle \rightarrow \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle |y^a \mod N\rangle$$

Measure second register



- $|\phi_l\rangle = \frac{1}{\sqrt{A+1}} \sum_{j=0}^{A} |jr + l\rangle (|z \mod N\rangle)$
  where A is the largest integer smaller than $\frac{q-l}{r} \sim \frac{q}{r}$.
- We make the simplifying assumption that r divides q exactly.

Apply DFT again on first register

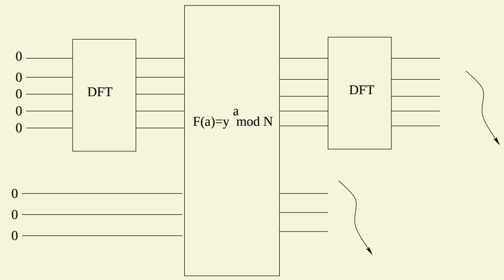


$$DFT_q \frac{1}{\sqrt{A+1}} \sum_{j=0}^{A} |jr+l\rangle = \sum_{c} \tilde{f}(c)|c\rangle$$

$$\tilde{f}(c) = \frac{\sqrt{r}}{q} \sum_{j=0}^{\frac{q}{r}-1} e^{\frac{2\pi i(jr+l)c}{q}}$$

Basically, $\tilde{f}(c) = \frac{e^{\frac{2\pi ilc}{q}}}{\sqrt{r}}$ if c is a multiple of $\frac{q}{r}$ and 0 otherwise.

Measure first register



- We see only those c that are integral multiples of $\frac{q}{r}$
- Thus, $\frac{c}{q} = \frac{j}{r}$
- If $\gcd(j, r) = 1$, we are done!
- Thankfully, $Prob(\gcd(j, r) = 1) \geq \frac{1}{\log r}$ when j is chosen uniformly at random.
- Repeat $O(\log r)$ times for arbitrarily high success probability

Epilogue

- The case when r does not divide q exactly needs some more analysis
- But this is the general idea!
- Thus, we have a quantum algorithm that yields the prime factors of an integer in polynomial time with high probability.
- This is an example of the Hidden Subgroup Problem (for commutative groups)!

- Michael Nielsen and Isaac Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, 2010.
- Peter Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*. SIAM J. Comput., 26(5), pp. 1484–1509, 1997.
- Artur Ekert and Richard Jozsa, *Shor's Quantum Algorithm for Factorizing Numbers*. Reviews of Modern Physics, 1995.

Thanks, Questions?