CMPE598 - Lecture 10

Bahar Hilal Yüksel

April 24, 2018

We want to factor a large integer N.

- FACTORING is reduced to finding a nontrivial square root of 1 modulo N.

$y^2 \equiv 1(mod N)$

if N = 15

$$\text{trivial square roots of 1 modulo N} \begin{cases} 1^2 \equiv 1(mod 15) \text{ not exciting} \\ (-1)^2 \equiv 1(mod 15) \text{ not exciting} \\ 14^2 \equiv 1(mod 15) \text{ not exciting} \end{cases} \tag{1}$$

$$\text{nontrivial square root of 1 modulo N} \Leftarrow 4^2 \equiv 1(mod 15)$$

If y is a nontrivial square root of 1 mod N, then N divides $y^2 - 1 = (y+1)(y-1)$, but N does not divide neither $(y+1)$ nor $(y-1)$.

So, this means that $gcd(y-1, N)$>1 because if $y-1$ and N were relatively prime, then since N divides $(y+1)(y-1)$ it would have to divide $(y+1)$.

If we can find y, then we can calculate $gcd(y-1, N)$ and if it is bigger than 1, it means we found a nontrivial factor of N. Now, all we have to do is finding a y.

- Finding such a root is reduced to computing the order of a random integer modulo N.

Pick a random number x (mod N)
The order of x (mod N) is the smallest number r such that

$$x^r \equiv 1(mod N)$$

ex:
$2^1 \equiv 2(mod 15)$
$2^2 \equiv 4(mod 15)$
$2^3 \equiv 8(mod 15)$
$2^4 \equiv 1(mod 15) \Rightarrow$ The order of 2 mod15 is 4.

- The order of an integer is precisely the period of a particular periodic superposition.

2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	...	
2,	4,	8,	1,	2,	4,	8,	1,	...	$\Rightarrow$ periodic sequence

period = order = 4

- And, periods of superpositions can be found by quantum FFT.

Classical FFT's input is on M-dimensional, complex-valued vector α (where M is a power of 2, say 2^m). Output is an M-dimensional, complex-valued vector β.

$$\begin{bmatrix} \beta_0 \\ \beta_1 \\ . \\ . \\ . \\ . \\ . \\ . \\ \beta_{M-1} \end{bmatrix} = \frac{1}{\sqrt{M}} \begin{bmatrix} 1 & 1 & 1 & 1 & . & . & . & 1 \\ 1 & \omega & \omega^2 & \omega^3 & . & . & . & \omega^{M-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & . & . & . & \omega^{2(M-1)} \\ 1 & \omega^3 & \omega^6 & \omega^9 & . & . & . & \omega^{3(M-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \omega^j & \omega^{2j} & \omega^{3j} & . & . & . & \omega^{j(M-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \omega^{M-1} & \omega^{2(M-1)} & \omega^{3(M-1)} & . & . & . & \omega^{(M-1)(M-1)} \end{bmatrix} \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ . \\ . \\ . \\ . \\ . \\ . \\ \alpha_{M-1} \end{bmatrix}$$

where ω is a complex M^{th} root of unity.

FFT runs in O(MlogM) steps.

Quantum Fourier Sampling

Input: A superposition of m = logM qubits $|\alpha>=\sum_{j=0}^{M+1}\alpha_j|j>$.

Method: We'll use O(m^2) quantum operations to obtain the superposition $|\beta>=\sum_{j=0}^{M-1}\beta_j|j>$.

Output: A random m-bit number j (i.e. $0 \le j \le M-1$), from the probability distribution $Pr[j]=|\beta_j|^2$.

$$\begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{M-1} \end{bmatrix} = \alpha_0 \begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} + \alpha_1 \begin{bmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} + \alpha_2 \begin{bmatrix} 0 \\ 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix} + \cdots + \alpha_{M-1} \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}$$

Suppose the input to quantum Fourier sampling is periodic with period k, for some k that divides M.

$|\alpha>=\begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{M-1} \end{pmatrix}$ is such that $\alpha_i=\alpha_j$ whenever i = j mod k where k is a particular integer that divides M. So there are $\frac{M}{k}$ repetitions of some sequence $(\alpha_0,\alpha_0,\ldots,\alpha_{M-1})$ of input k.

AND SUPPOSE EXACTLY ONE OF THE K NUMBERS IS NONZERO, say α_j.

$\Rightarrow$ Then the output will be a multiple of $\frac{M}{k}$, and it is equally likely to be any of the k multiplies of $\frac{M}{k}$.

So, the vector β will contain 1's only in the places which correspond to multiples of $\frac{M}{k}$, where k is the period that we are looking for.

It is possible to make some probabilistic experiments on this setup to understand what $\frac{M}{k}$ is, and since we already know M, then we can calculate k.

Suppose the vector $|\alpha>=(\alpha_0,\alpha_1,\ldots,\alpha_{M-1})^T$ is periodic with period k with no offset (that is, the nonzero terms are $\alpha_0,\alpha_k,\alpha_{2k},\ldots$). Thus,

$$|\alpha>=\sum_{j=0}^{\frac{M}{k}-1}\sqrt{\frac{k}{M}}|jk>$$

Claim:

$$|\beta>=\frac{1}{\sqrt{k}}\sum_{j=0}^{k-1}|\frac{jM}{k}>$$

In the input vector, the coeffient of α_l is $\sqrt{\frac{k}{M}}$ if k divides l and zero otherwise.

The j^{th} coefficient of $|\beta>$ is

$$\beta_j = \frac{1}{\sqrt{M}} \sum_{l=0}^{M-1} \omega^{jl} \alpha_l = \frac{\sqrt{k}}{M} \sum_{i=0}^{\frac{M}{k}-1} \omega^{jik}$$

So, this sum is the geometric series $1 + \omega^{jk} + \omega^{2jk} + \dots$ containing $\frac{M}{k}$ terms and with ratio ω^{jk}. There are two cases. If the ratio is exactly 1, which happens if $jk = 0 mod M$, then the sum of the series is just the number of terms. If the ratio is not 1, apply the usual formula for geometric series to find that the sum is

$$\frac{1 - \omega^{jk(\frac{M}{k})}}{1 - \omega^{jk}} = \frac{1 - \omega^{Mj}}{1 - \omega^{jk}} = 0$$

So $\beta_j = \frac{1}{\sqrt{k}}$ if M divides jk, and is zero otherwise.

This was only for the case with no offset. Also works(with little modification) for the case where the offset is nonzero.

Suppose s independent samples are drawn uniformly from

$$\{0, \frac{M}{k}, \frac{2M}{k}, \dots, \frac{(k-1)M}{k}\}$$

Then, with probability at least $1 - \frac{k}{2^s}$, the greatest common divisor of these samples is $\frac{M}{k}$.

Proof: The only way this can fail is if all the samples are multiples of $j\frac{M}{k}$, for some $j > 1$. So, fix any integer $j \geq 2$.

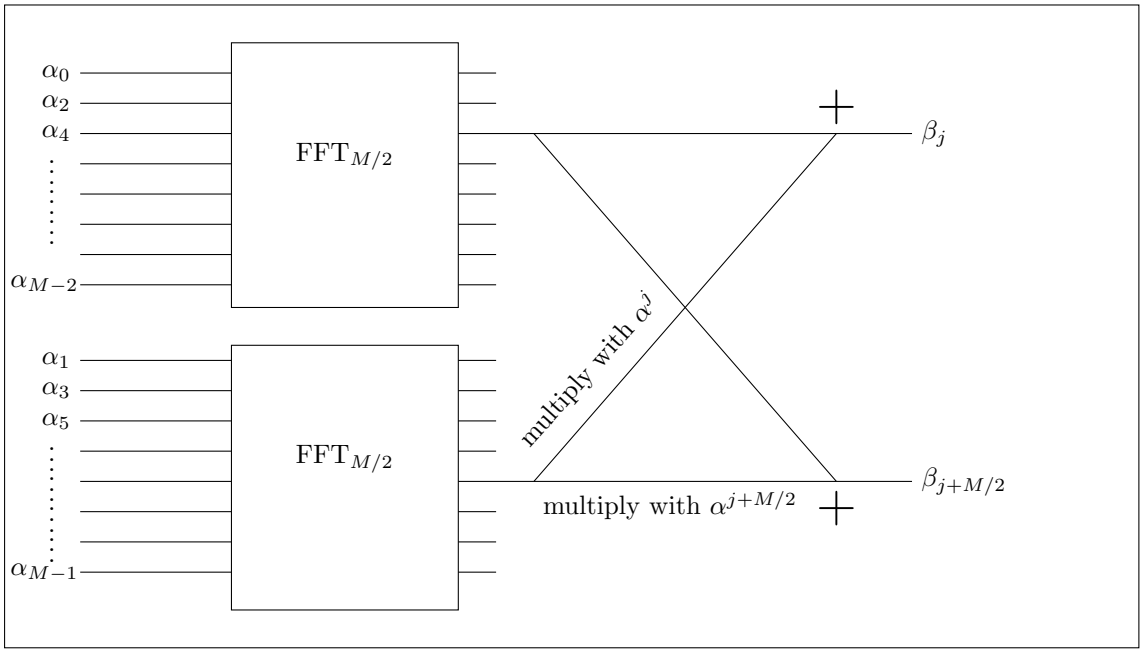
The chance that a particular sample is a multiple of $j\frac{M}{k}$ is at most $\frac{1}{j} \leq \frac{1}{2}$. So, the chance that ALL samples are multiples of $j\frac{M}{k}$ is at most $\frac{1}{2^s}$.

The probability that this bad thing will happen for some $j \leq k$ is at most $k\frac{1}{2^s}$, since there are k candidates for the number j.

How does the classical FFT work?

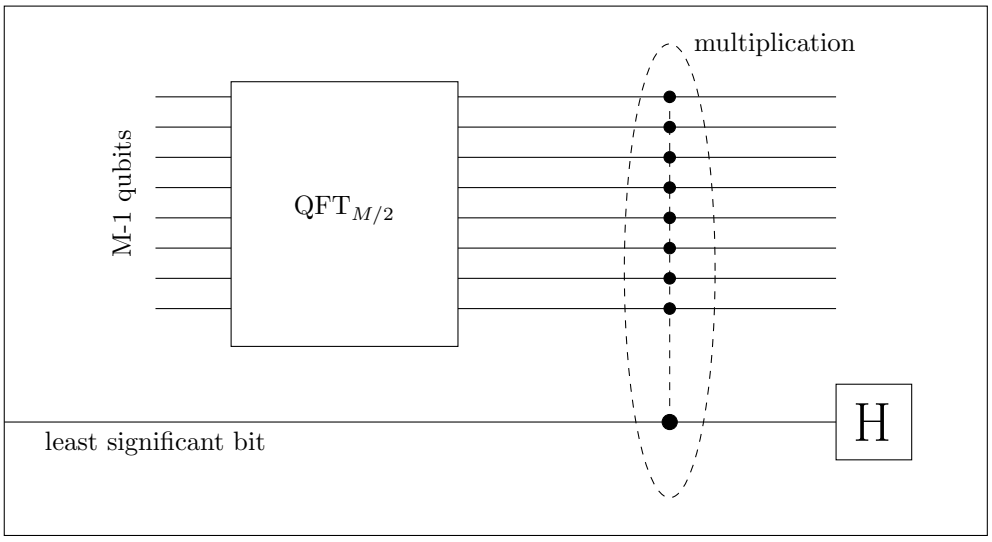
from input $(\alpha_0, \alpha_1, \dots, \alpha_{M-1})^T$ to output $(\beta_0, \beta_1, \dots, \beta_{M-1})^T$

FFT_M



In the quantum version, the input now encoded in the 2^m amplitudes of m=logM qubits. So, the decomposition of the inputs to evens and odds is determined by the least significant qubit. We will design a quantum circuit(subroutine) QFT_M. $\text{QFT}_{M/2}$ will be applied to the remaining m-1 qubits.

QFT_M



$$\begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & & & \ddots & \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix} \otimes \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 0 & \dots & 0 & 0 \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & \dots & 0 & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & \dots & 0 & 0 \\ \vdots & \vdots & & & & & \vdots \\ 0 & 0 & 0 & 0 & \dots & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ 0 & 0 & 0 & 0 & \dots & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$$

$$\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & & & & & \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & & & & & \\ & & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & & & \\ & & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & & & \\ & & & & \ddots & & \\ & & & & & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ & & & & & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \alpha_{y_0} \\ \alpha_{y_1} \end{pmatrix} = \begin{pmatrix} \frac{\alpha_{y_0}+\alpha_{y_1}}{\sqrt{2}} \\ \frac{\alpha_{y_0}-\alpha_{y_1}}{\sqrt{2}} \end{pmatrix}$$

$\Rightarrow$ Multiplication must happen before the H.

For each j, an operation is done in the classical FFT on the $(\frac{M}{2}+j)^{th}$ wire.

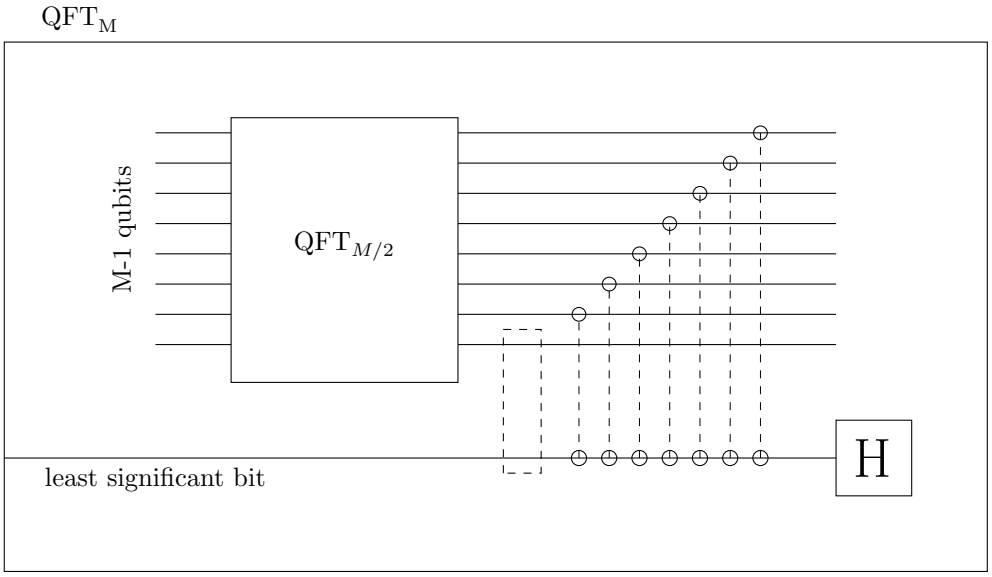
If j is represented by the m-1 bits j_1, j_2, …, j_{m-1}, then $\omega^j = \prod_{l=1}^{m-1} \omega^{2^{jl}}$.

Ex: m=3, m-1=2, j_2, j_1.

For the l_{th} qubit, consider ω^{2^l}
Qubit positions from least significant to most significant:

(	0,	1,	2,	3)
(	ω^1,	ω^2,	ω^4,	ω^8)

$\omega^{1010} = \omega^2.\omega^8$



$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \omega^{2^j} \end{bmatrix}$$