Lecture 11.

1) Simon's Problem.

2) Period finding and Quantum Fourier Transform.

3) Circuit and complexity of the QFT (next time!).

In this chapter we begin with a variation of the Deutsch problem, that was originally proposed by Simon. As we will see the quantum Fourier transform will appear naturally as an attempt to generalize Simon's algorithm.

1) Simon's problem (and Hidden subgroups.)

Let us first give the statement of the simplest version originally considered by D. Simon.

Let $f : \{0,1\}^n \to X$ where X is a finite set of values. We suppose that we assured that f satisfies "Simon's promise":

$$f(\underline{x}) = f(\underline{y}) \quad \text{iff} \quad \underline{x} = \underline{y} \ \text{or} \ \underline{x} = \underline{y} \oplus \underline{a}$$

for some fixed $\underline{a} \in \{0,1\}^n = \mathbb{F}_2^n$. (mod 2 sum of n-dimensional vectors).

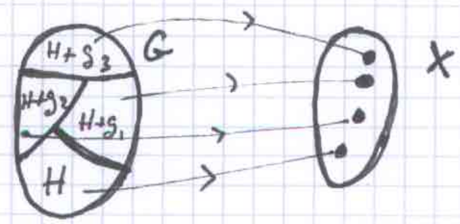
The problem is: given a black box that computes f find $\underline{a}$ in a minimal number of queries of f.

- It can be shown that if the black box is classical then we need at least $O(2^{cn})$ queries to find $\underline{a}$ with finite probability $\sim O(1)$.

- We will show that if the black box is quantum, there is an algorithm such that $O(\mathrm{poly}(n))$ queries suffice to find $\underline{a}$ with Prob $\sim 1 - O(2^{-cn})$.

We note that $\{\underline{0}, \underline{a}\}$ forms a subgroup of $(\mathbb{Z}_2^n, \oplus)$. [In fact it is even a vector sub-space] This motivates the more general <u>Hidden Subgroup Problem</u>:

Let G be a finite group (abelian) and H a subgroup. Let $f : G \to X$ (X a finite set) which satisfies Simon's promise:

f is constant on the cosets G/H : 

The problem is to find a set of generators for H.

- If the elements of G admit a binary representation of size $O(n)$; $n = \log |G|$ then there exist a quantum algorithm solving the problem with Prob $\sim 1 - O(2^{-cn})$ with $O(n)$ queries.

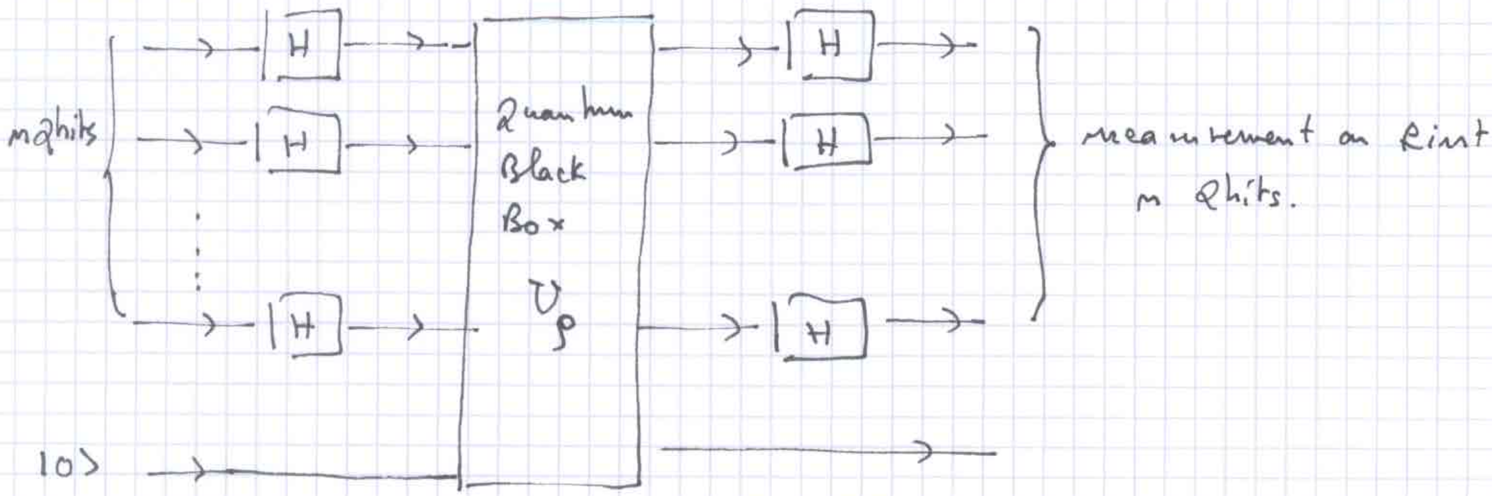
- If G is non-abelian the problem is still open.

- Here we will limit ourselves to $G = (\mathbb{F}_2^m, \oplus)$ and $H \subset G$ is subgroup of $\mathbb{F}_2^m$. In fact H is also a vector sub-space since $\mathbb{F}_2^m$ is a vector space. That is H has dimension $D = \dim H$ and we look for a set of basis vectors.
- Equivalently we could look for a set of basis vectors of $H^\perp$ (the orthogonal complement of H : $\mathbb{F}_2^m = H \oplus H^\perp$). Indeed once a basis of $H^\perp$ is known it is possible to find a basis for H in $O(\text{poly}(m))$ steps by methods of linear algebra (e.g Gauss-Jordan).

For further use we note that the number of vectors in $\mathbb{F}_2^m$ is 2^m ; the nb of vectors in H is $2^{\dim H}$; the nb of vectors in $H^\perp$ is $2^{\dim H^\perp}$.

The cosets $\mathbb{F}_2^m / H$ all have one representative that we denote by $\underline{t}$. Given a coset with representative $\underline{t}$, all vectors in the coset are $\{\underline{t} + \underline{h} \mid \underline{h} \in H\}$. So the number of vectors in each coset is $2^{\dim H}$ and the number of cosets is $\frac{2^m}{2^{\dim H}} = 2^{\dim H^\perp}$.

The quantum circuit for Simon's algorithm is



Let us perform all operation step by step.

<u>initialisation</u> : $\underbrace{|0\rangle \otimes \ldots \otimes |0\rangle}_{m \text{ qbits.}} \otimes |0\rangle$.

<u>Hadamard trsf</u> : $\rightarrow$

$$(H|0\rangle \otimes \ldots \otimes H|0\rangle) \otimes |0\rangle$$

$$= \frac{1}{2^{m/2}} (|0\rangle + |1\rangle) \otimes \ldots \otimes (|0\rangle + |1\rangle) \otimes |0\rangle$$

$$= \frac{1}{2^{m/2}} \sum_{\underline{b}} |\underline{b}\rangle \otimes |0\rangle \quad . \quad ; \quad \underline{b} = (b_1 \ldots b_m) \ ; \ b_i \in \{0,1\} .$$

$$= \frac{1}{2^{m/2}} \sum_{\underline{t} \in \mathbb{F}_2^m/H} \ \sum_{\underline{h} \in H} |\underline{t} + \underline{h}\rangle \otimes |0\rangle .$$

<u>Quantum Blac Box</u> : $U_\rho |\underline{b}\rangle \otimes |0\rangle = |\underline{b}\rangle \otimes |\rho(\underline{b})\rangle$.

As usual this can be checket to be unitary.

The output of U_f is :

$$= \frac{1}{2^{m/2}} \sum_{\underline{t} \in \mathbb{F}_2^m / H} \sum_{\underline{h} \in H} | \underline{t} + \underline{h} \rangle \otimes | \rho(\underline{t}) \rangle .$$

since ρ is constant on cosets $\mathbb{F}_2^m / H$.

<u>Final Hadamard</u> $\underbrace{H \otimes H \ldots \otimes H}_{m \text{ times}} \otimes \mathbb{1}$. :

We get the output quantum superposition :

$$\frac{1}{2^{m/2}} \sum_{\underline{t} \in \mathbb{F}_2^m / H} \sum_{\underline{h} \in H} \left(H | t_1 + h_1 \rangle \otimes \cdots \otimes H | t_m + h_m \rangle \right) \otimes | \rho(\underline{t}) \rangle$$

using

$$H | x_i \rangle = \frac{1}{\sqrt{2}} \sum_{y_i = 0,1} (-1)^{x_i y_i} | y_i \rangle \qquad (\text{check this !})$$

we obtain

$$\frac{1}{2^{m/2}} \sum_{\underline{t} \in \mathbb{F}_2^m / H} \sum_{\underline{h} \in H} \frac{1}{2^{m/2}} \sum_{\underline{y}} (-1)^{(\underline{t} + \underline{h}) \cdot \underline{y}} | \underline{y} \rangle \otimes | \rho(\underline{t}) \rangle .$$

$$= \frac{1}{2^m} \sum_{\underline{t} \in \mathbb{F}_2^m / H} \sum_{\underline{y}} \left(\sum_{\underline{h} \in H} (-1)^{\underline{h} \cdot \underline{y}} \right) (-1)^{\underline{t} \cdot \underline{y}} | \underline{y} \rangle \otimes | \rho(\underline{t}) \rangle$$

Since H is a group:

$$\sum_{\underline{h} \in H} (-1)^{\underline{h} \cdot \underline{z}} = \begin{cases} |H| = 2^{\dim H} & \text{if } \underline{z} \in H^{\perp} \ (\text{i.e. } \underline{h} \cdot \underline{z} = 0). \\ 0 & \text{otherwise}. \end{cases}$$

Note that to get the "otherwise" we use the group property:

$$\sum_{\underline{h} \in H} (-1)^{\underline{h} \cdot \underline{z}} = \sum_{\underline{h} \in H} (-1)^{(\underline{h} + \underline{g}) \cdot \underline{z}}$$

$$= (-1)^{\underline{g} \cdot \underline{z}} \sum_{\underline{h} \in H} (-1)^{\underline{h} \cdot \underline{z}}$$

for some fixed $\underline{g} \in H$. If $\underline{z} \notin H^{\perp}$ $(-1)^{\underline{g} \cdot \underline{z}} \neq 0$ so that $\sum_{\underline{h} \in H} (-1)^{\underline{h} \cdot \underline{z}} = 0$.

Summarizing, the output of the quantum circuit is:

$$|\psi\rangle = \frac{2^{\dim H}}{2^{m}} \cdot \sum_{\underline{t} \in \mathbb{F}_2^m / H} \sum_{\underline{y} \in H^{\perp}} (-1)^{\underline{t} \cdot \underline{z}} \, |\underline{z}\rangle \otimes |g(\underline{t})\rangle .$$

This the state just before the measurement. The quantum black box has been queried only once to prepare this state.

Measurement of first m Qbits:

We measure in the computational basis $\{|0\rangle, |1\rangle\}$ so that the outcome is $\underline{y} \in H^\perp$. By the measurement postulate

$$\text{Prob}(y) = \langle\psi| \underbrace{(|\underline{y}\rangle\langle\underline{y}| \otimes \mathbb{1})}_{\text{Projector.}} |\psi\rangle .$$

$$= \frac{2^{2\dim H}}{2^{2m}} \sum_{\underline{t},\underline{t}'} (-1)^{\underline{t}\cdot\underline{y}} (-1)^{\underline{t}'\cdot\underline{y}} \langle \rho(\underline{t}) | \rho(\underline{t}') \rangle$$

Now since ρ takes different values on different cosets we have

$$\langle \rho(\underline{t}) | \rho(\underline{t}') \rangle = \delta_{\underline{t},\underline{t}'}$$

so that the probability of outcome y becomes:

$$\text{Prob}(y) = \frac{2^{2\dim H}}{2^{2m}} \cdot \#(\text{of cosets}) . \quad \longrightarrow 2^{\dim H^\perp}$$

$$= \frac{2^{\dim H}}{2^{2m}} \cdot 2^{m} \qquad \text{use } \dim H + \dim H^\perp = m.$$

$$= \frac{2^{\dim H}}{2^{m}} = \frac{1}{2^{\dim H^\perp}} = \frac{1}{|H^\perp|} .$$

$$\boxed{\text{So we get some state } |\underline{y}\rangle_{\in H^\perp} \text{ with uniform probability } \frac{1}{2^{\dim H^\perp}} .}$$

In other words, when we query the quantum black box we obtain surely ~~on~~ a vector in $H^\perp$. Moreover we get a random vector in $H^\perp$. So if we query $O(n)$ ~~and~~ times the quantum black box we get a set of random vectors $\underline{y}_1, \dots \underline{y}_{O(n)}$ ~~and~~ surely in $H^\perp$.

It remains to estimate the probability that $\underline{y}_1 \dots \underline{y}_{O(n)}$ form a linearly independent set.

Lemma: Let $\underline{y}_1 \dots \underline{y}_K$ randomly chosen vectors from $H^\perp$ with a uniform distribution.

Then for K

$$\mathrm{Prob}\,(\underline{y}_1 \dots \underline{y}_K \text{ lin indipendant}) \geq \frac{1}{4}$$

Proof: Choose $\underline{y}_1$. $\mathrm{Prob}\,(\underline{y}_1 \neq 0) = \dfrac{2^{\dim H^\perp} - 1}{2^{\dim H^\perp}}$

Suppose that $(\underline{y}_1 \dots \underline{y}_{i-1})$ have been chosen lin indep.

Choose $\underline{y}_i$: $\mathrm{Prob}\,(\underline{y}_i \text{ lin indip of } (\underline{y}_1 \dots \underline{y}_{i-1}))$

$$= \frac{2^{\dim H^\perp} - 2^{i-1}}{2^{\dim H^\perp}}$$

$\Big($Indeed #(of vectors lin dep in $y_1 \dots y_{i-1}$ subspace) $= 2^{i-1}$. So $\underline{y}_i$ must be in complement.$\Big)$.

Thus we get

$$\mathrm{Prob}(y_1 \dots y_K \text{ lin indep}) = \prod_{i=0}^{K-1} \frac{2^{\dim H^\perp} - 2^i}{2^{\dim H^\perp}}$$

$$= \prod_{i=0}^{K-1} \left(1 - 2^{i - \dim H^\perp}\right).$$

For $K \leq \dim H^\perp$ we can show that this product is $\geq \frac{1}{4}$.

[write it as exp log and expand the log ...]. ∎

Remark:

Finaly if we run the algorithm M times we are assured that $\sim \frac{M}{4}$ we will have an independent set of vectors spanning $H^\perp$. Each time we make a check to see if we are succesful. (If we are we stop; if we are not we continue). The total number of queries is $O(M, n)$. If $M \sim n$ we can show that we will be succesful with probability exponentialy close to 1.

2) Period Finding and Quantum Fourier Transform.

Consider the following variation of the Hidden Subgroup problem. Let $G = (\mathbb{Z}, +)$ and $H = \frac{\mathbb{Z}}{r\mathbb{Z}}$, r some fixed unknown integer.

We have a function $f : \mathbb{Z} \to \mathbb{Z}$ which is r-periodic:

$$f(x) = f(x+r) \quad , \quad x \in \mathbb{Z}.$$

and we want to find the period.

Here the group G is infinite so that Simon's algorithm does not work. The first idea is to assume that we know $r < M$ for some very large integer M and then restrict $G = \mathbb{Z}$ to the set $\{0, 1, \ldots, N-1\}$ with some $N \gg M$ (later on we will choose $N \sim M^2$). The problem now is that $\{0, 1, \ldots N-1\}$ does not have the group structure so Simon's algorithm again does not quite work. We will see that a very similar algorithm works which is based on the QFT. <u>The net result will be that we can find the period r with exponentially high probability $1 - O(2^{-cn})$ in poly(n) time where $n = \log_2 N$.</u>

We use the following notation. Integers in $\{0, 1, \dots N-1\}$ are denoted by x, y. Corresponding quantum states are $|x\rangle$; $|y\rangle$. If $N = 2^M$ these states are in the space $\mathbb{C}_2 \otimes \dots \otimes \mathbb{C}_2$. More precisely if we use the binary expansion

$$x = 2^{M-1} \cdot x_{M-1} + \dots + 2^2 \cdot x_2 + 2 \cdot x_1 + 2^0 \cdot x_0 \quad ; \ x_i \in \{0, 1\}$$

we have
$$|x\rangle = |x_{M-1} \dots x_2 x_1 x_0\rangle$$
$$= |x_{M-1}\rangle \otimes \dots \otimes |x_2\rangle \otimes |x_1\rangle \otimes |x_0\rangle .$$

As usual one can form superpositions of such states that have no classical analog.

Quantum Fourier Transform:

QFT is a unitary operator defined on basis vectors as

$$QFT\, |x\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i \frac{xy}{N}} |y\rangle \quad ; \quad N = 2^M$$

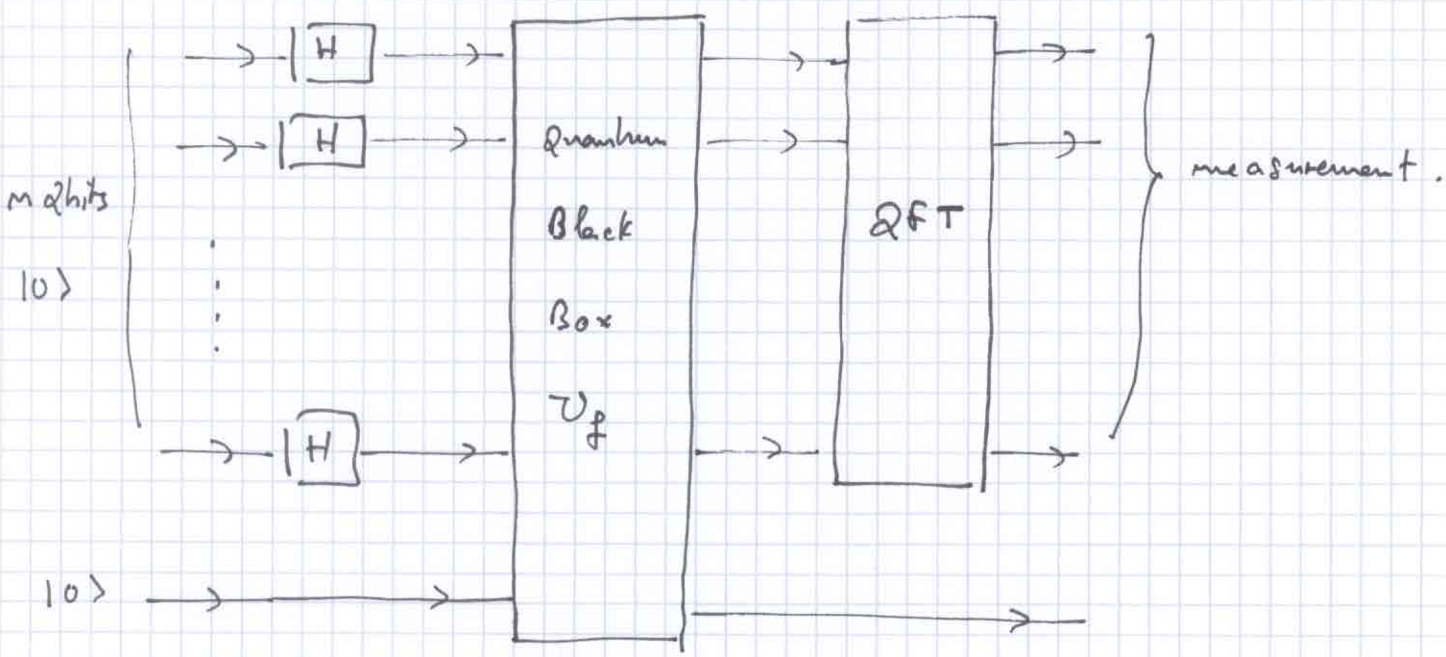
Its action on general state is obtained by linearity:

$$QFT \left(\sum_{x=0}^{N-1} c_x |x\rangle \right) = \sum_{x=0}^{N-1} c_x \, QFT\, |x\rangle .$$

Thanks to the general results of lecture 10 we know that it can be implemented using only one & two bit elementary gates. In fact as we will show later the size of the circuit for QFT can be chosen $O(m^2) = O((\log_2 N)^2)$.

For the moment we just suppose that we have such a circuit at our disposal and look at the algorithm for period finding.

<u>Quantum Circuit for Period finding.</u>



With respect to Simon's algorithm we see that the second column of Hadamard gates has been changed for a QFT.

Let us look at the operations performed by this circuit at each stage. The input is $\underbrace{|0\rangle \otimes \dots \otimes |0\rangle}_{m \text{ times.}} \otimes |0\rangle$

input: $\underbrace{|0\rangle \otimes \cdots \otimes |0\rangle}_{n \text{ times}} \otimes |0\rangle$.

Hadamard trof: we get the state,

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \otimes |0\rangle$$

One query with quantum black box (unitary):

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

Since f is r-periodic we can rewrite this state as

$$= \frac{1}{\sqrt{N}} \sum_{x_0=0}^{r-1} \sum_{j=0}^{A_{x_0}-1} |x_0 + jr\rangle\, |f(x_0)\rangle .$$

where A_{x_0} is an integer such that

$$N-r \leqslant x_0 + (A-1)r < N$$

Now we apply the QFT:

$$\rightarrow \frac{1}{N} \sum_{x_0=0}^{r-1} \sum_{j=0}^{A-1} \sum_{y=0}^{N-1} e^{2\pi i \frac{(x_0+jr)y}{N}} |y\rangle\, |f(x_0)\rangle$$

$$= \frac{1}{N} \sum_{x_0=0}^{r-1} \sum_{y=0}^{N-1} e^{2\pi i \frac{x_0 y}{N}} \sum_{j=0}^{A-1} e^{2\pi i \frac{jy}{N/r}} |y\rangle\, |f(x_0)\rangle .$$

Measurement: According to the measurement postulate when we measure the first n Qbits in the computational basis $\{|y\rangle\}$ we get an outcome y with probability:

$$\mathrm{Prob}(y) = \frac{1}{N^2}\sum_{x_0=0}^{r-1}\left| e^{2\pi i \frac{x_0 y}{N}} \sum_{j=0}^{A-1} e^{2\pi i \frac{jy}{N/r}} \right|^2$$

in other words the outcome is $y \in \{0, \dots, N-1\}$ with

$$\mathrm{Prob}(y) = \frac{1}{N^2}\sum_{x_0=0}^{r-1}\left| \sum_{j=0}^{A-1} e^{2\pi i \frac{jy}{N/r}} \right|^2$$

where A is an integer such that: $N-r \leq x_0+(A-1)r < N$

Analysis: We show that from the outcome y we can be the period r with finite probability. For this we distinguish two cases: $\frac{N}{r}$ is integer (easy case) and $\frac{N}{r}$ is not integer (harder case).

Easy Case: Suppose $\frac{N}{r}$ is an integer. Then

$$e^{2\pi i \frac{jy}{N/r}} = 1 \quad \text{if} \quad y = K \cdot \frac{N}{r} \quad \text{with}$$

$K \in \{0, 1, \dots, r-1\}$

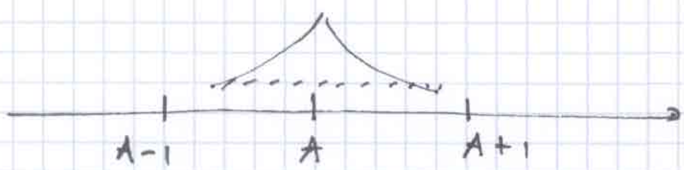
Moreover we have in general :

$$\frac{N}{r} \leq \underbrace{\frac{x_0}{r}}_{<1} + A < \frac{N}{r} + 1$$

$$\Rightarrow \quad A < \frac{N}{r} + 1 \quad \text{and} \quad \frac{N}{r} < A + 1 .$$

So A is in general the unique integer such that

$$A - 1 < \frac{N}{r} < A + 1 .$$



Here if $\frac{N}{r}$ is an integer we must have $\frac{N}{r} = A$. Putting these remarks together we find

$$\mathrm{Prob}(y) = \begin{cases} \frac{1}{N^2} \cdot r \cdot \left(\frac{N}{r}\right)^2 = \frac{1}{r} & \text{for } y \in \left\{ 0, \frac{N}{r}, \frac{2N}{r}, \ldots (r-1).\frac{N}{r} \right\} \\ 0 & \text{otherwise.} \end{cases}$$

We get y from the measurement. So we know $\frac{y}{N}$. And with a probability equal to one we have

$$\underbrace{\frac{y}{N}}_{\text{known.}} = \frac{k}{r} \quad , \quad k \in \{0, 1, 2 \ldots r-1\} .$$

Now if $PGCD(k, r) = 1$ we can get k & r by simplifying the fraction $\frac{y}{N}$. So we get r as long as $PGCD(k, r) = 1$.

Now the probability that $PGCD(k, r) = 1$ is $\frac{\varphi(r)}{r}$ where

$\varphi(r)$ is Euler's fct (# of coprimes to r that are $\leq r$). It

is known that

$$\varphi(r) \geq \frac{1}{4 \ln(\ln r)}.$$

Thus we have $\text{Prob}(PGCD(k, r) = 1) \geq \frac{1}{4r(\ln \ln r)} \geq \frac{1}{4n(\ln \ln n)}$.

Thus we succeed with probability at least $\left(\frac{1}{4n \ln \ln n}\right)$.

By repeating the query of the quantum circuit $O(n \ln \ln n)$

we can make this probability $O(1)$. So we have a polynomial

algorithm at least as long as $\frac{N}{r}$ is an integer.

Harder Case : $\frac{N}{r}$ is not an integer.

In fact the formula for the probability favors values of

$y \in \{0, \dots, N-1\}$ that are close to $\frac{N}{r}$. We can prove the

following :

Lemma : $$\text{Prob}\Big(-\frac{1}{2} \leq y - \overbrace{\frac{kN}{r}}^{\text{for some } k} \leq \frac{1}{2}\Big) \geq \frac{2}{5}.$$

Remark : the $\frac{2}{5}$ above $\overbrace{}^{\text{can be made}}$ as close as we want to $\frac{4}{\pi^2}$.

Proof of Lemma:

By summing the complex exponentials with the help of formula for a geometric series we get:

$$\mathrm{Prob}(y) = \frac{1}{N^2} \sum_{x_0=0}^{r-1} \frac{\sin^2\left(\frac{\pi y r A}{N}\right)}{\sin^2\left(\frac{\pi y r}{N}\right)}.$$

$$= \frac{1}{N^2} \sum_{x_0=0}^{r-1} \frac{\sin^2 \frac{\pi A}{N}(yr - kN)}{\sin^2 \frac{\pi}{N}(yr - kN)} \qquad (\forall\ k \text{ by periodicity})$$

Now fix $k \in \{0 \ldots r-1\}$ s.t $-\frac{r}{2} \leq yr - kN \leq \frac{r}{2}$. Each ratio term in the sum takes it minimum for $yr - kN = \frac{r}{2}$. So:

$$\mathrm{Prob}\left(\left| y - \frac{kN}{r} \right| \leq \frac{1}{2} \right) \geq \frac{r}{N^2} \sum_{x_0=0}^{r-1} \frac{\sin^2 \frac{\pi A r}{2N}}{\sin^2 \frac{\pi r}{2N}}$$

for some k.

Since $\frac{N}{r} - 1 < A < \frac{N}{r} + 1$ we also have

$$\frac{\pi}{2}\left(1 - \frac{r}{N}\right) \leq \frac{\pi A r}{2N} \leq \frac{\pi}{2}\left(1 + \frac{r}{N}\right)$$

$$\Rightarrow \mathrm{Prob}\left(\left| y - \frac{kN}{r} \right| \leq \frac{1}{2} \right) \geq \frac{r^2}{N^2} \cdot \frac{\sin^2 \frac{\pi}{2}\left(1 - \frac{r}{N}\right)}{\sin^2 \frac{\pi}{2}\frac{r}{N}} \geq \frac{1}{N^2} \frac{r^2}{\frac{\pi^2}{4}\frac{r^2}{N^2}}$$

and since $\frac{r}{N} < \frac{M}{M^2} = \frac{1}{M}$ small $\qquad \approx \frac{4}{\pi^2}$.

Final argument when $\frac{N}{2}$ is not an integer :

With one query of the quantum circuit we observe an integer y s.t for some $k \in \{0, \ldots r-1\}$ we have $|y - k\frac{N}{r}| \leq \frac{1}{2}$ with probability at least $\frac{2}{5}$.

So with this probability :

$$\left|\frac{y}{N} - \frac{k}{r}\right| \leq \frac{1}{2N} \leq \frac{1}{2M^2} \ll \frac{1}{2r^2}$$ (Remember $r \ll M$; $N \geq M^2$).

A standard result of number theory following from Euclid's algorithm states that :

Lemma: Let $\frac{y}{N}$ and $\frac{k}{r}$ s.t $\left|\frac{y}{N} - \frac{k}{r}\right| \leq \frac{1}{2r^2}$.

If $PGCD(k, r) = 1$ then $\frac{k}{r}$ is unique and can be found from the continuous fraction expansion of $\frac{y}{N}$ in $O((\log_2 N)^3)$ steps (i.e $O(m^3)$ steps).

Combining this lemma with the previous results we see that with one query yielding y we can succesfuly compute r with a

$\text{Prob} \geq \frac{2}{5} \cdot \frac{1}{4r(\ln\ln r)}$ in $O(m^3)$ steps.

from QMechanics from $PGCD(k, r) = 1$

So by repeating the procedure $O(m \ln\ln m)$ times we can compute r with high probability. The total time is $\text{poly}(m)$.