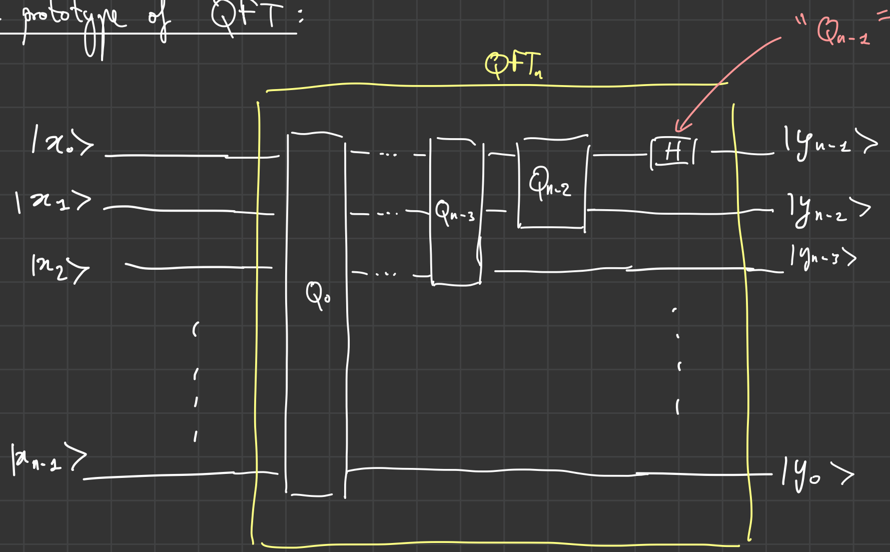
General prototype of QFT:



IV Shor algorithm : General case

$f : \mathbb{Z} \to X$ s.t f is periodic of period r and $f(0), \dots, f(r-1)$ are pairwise distincts.

Problem : find r.

Application: $X = G$ is a group, pick $g \in G$

Take $f : \mathbb{Z} \to G$, $r =$ order of g
$\quad\quad n \mapsto g^n$

$\longrightarrow$ For this, we use the same circuit!

We need to know in advance an upper bound N on r.

Then choose n such that $2^n \geq N^2$ i.e. $n \geq 2 \cdot \log_2 N$

Analysis of the circuit:

① $$\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle |0\rangle$$

② $$\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle |f(x)\rangle$$

③ $$\frac{1}{2^n} \sum_{x=0}^{2^n-1} \sum_{y=0}^{2^n-1} \zeta_n^{xy} |y\rangle |f(x)\rangle = \sum_{y=0}^{2^n-1} |y\rangle \otimes q_y$$

with $$q_y = \frac{1}{2^n} \sum_{x=0}^{2^n-1} \zeta_n^{xy} |f(x)\rangle$$

We need to estimate $\|q_y\|^2$.

Write $$q_y = q_{y,0}|f(0)\rangle + q_{y,1}|f(1)\rangle + \cdots + q_{y,r-1}|f(r-1)\rangle$$

$$q_{y,b} = \frac{1}{2^n} \sum_{a=0}^{m_b-1} \zeta_n^{(ar+b)y} \in \mathbb{C}$$

$$\left(\begin{array}{l} x = ar+b \\ ar+b \leq 2^n-1 \\ a \leq \frac{2^n-1-b}{r} \end{array} \right)$$

with $$m_b = \left\lfloor \frac{2^n-1-b}{r} \right\rfloor + 1$$

Note: $$\underbrace{1 + \left\lfloor \frac{2^n-r}{r} \right\rfloor}_{= \left\lfloor \frac{2^n}{r} \right\rfloor} \leq m_b \leq \left\lfloor \frac{2^n-1}{r} \right\rfloor + 1$$

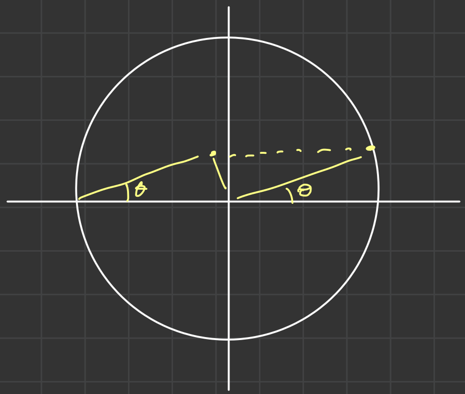
$\longrightarrow$ remember that $$m_b \simeq \frac{2^n}{r} + 1$$

Since $\rho(0), \dots, \rho(r-1)$ are pairwise distincts,

$$\|q_y\|^2 = |q_{y,0}|^2 + \dots + |q_{y,r-1}|^2$$

$$q_{y,b} = \frac{1}{2^n} \zeta_n^{by} \sum_{a=0}^{m_b-1} \left(\zeta_n^{ry}\right)^a = \frac{1}{2^n} \zeta_n^{by} \frac{\zeta_n^{rym_b} - 1}{\zeta_n^{ry} - 1}$$

$$|q_{y,b}| = \frac{1}{2^n} \left| \frac{\zeta_n^{rym_b} - 1}{\zeta_n^{ry} - 1} \right|$$



How do we compute $|e^{i\theta} - 1| = |e^{i\theta/2}(e^{i\theta/2} - e^{-i\theta/2})|$

$$= |e^{i\theta/2} - e^{-i\theta/2}|$$

$$= 2\,|\sin \tfrac{\theta}{2}|$$

Recall : $\zeta_n = e^{\frac{2i\pi}{2^n}}$

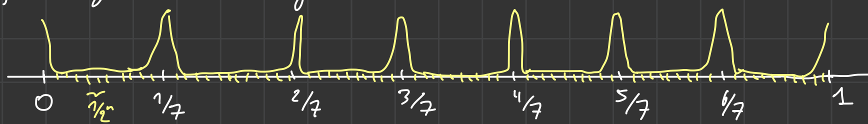
$$\zeta_n^{rym_b} = \exp\left(\frac{2i\pi r y m_b}{2^n}\right) \text{ and } \zeta_n^{ry} = \exp\left(\frac{2i\pi r y}{2^n}\right)$$

$$\Rightarrow |q_{y,b}| = \frac{1}{2^n} \left| \frac{\sin\left(\frac{\pi r y m_b}{2^n}\right)}{\sin\left(\frac{\pi r y}{2^n}\right)} \right|$$

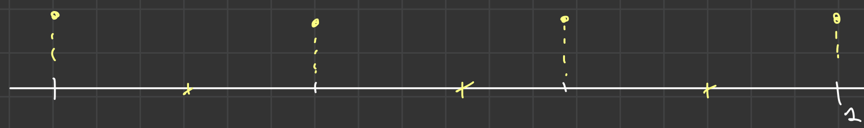
Expectation: $|q_{y,b}|$ will be "large" when $\frac{\pi r y}{2^n}$ close to $j\pi$ with $j \in \mathbb{Z}$.

that is $\frac{y}{2^n}$ close to $\frac{j}{r}$.

Ex: $(r=7)$ and you rescale to get results in $[0,1]$



$\begin{pmatrix} r=4 \\ n=3 \end{pmatrix}$



Lemma. We assume $2^n \geq 5r$ and $\left|\frac{y}{2^n} - \frac{j}{r}\right| \leq \frac{1}{2^{n+1}}$

Then $\|q_y\|^2 \geq \frac{0{,}16}{r}$

Proof: (sketch)

Write $\frac{y}{2^n} - \frac{j}{r} = \frac{\delta}{2^n}$ with $|\delta| \leq \frac{1}{2}$

$$\frac{yr}{2^n} = j + \frac{\delta r}{2^n}$$

$$|q_{y,b}| = \frac{1}{2^n}\left|\frac{\sin\left(\pi m_b\left(j + \frac{\delta r}{2^n}\right)\right)}{\sin\left(\pi\left(j + \frac{\delta r}{2^n}\right)\right)}\right| = \frac{1}{2^n}\left|\frac{\sin\left(\pi m_b \frac{\delta r}{2^n}\right)}{\sin\left(\pi \frac{\delta r}{2^n}\right)}\right|$$

Write $\frac{m_b r}{2^n} = 1 + \varepsilon$ with $|\varepsilon| < \frac{r}{2^n} \leq \frac{1}{5}$

Now use that $\frac{x}{2} \leq \sin x \leq x$ when $x \in [0, \frac{3\pi}{5}]$. ∎

Conclusion: The outcome of Shor's circuit provides an approximation of some fraction with denominator r at $\frac{1}{2^{n+1}}$.

Continued fractions:

Let $x \in \mathbb{R}$. We want to find a good approx of x with rational number.

$$x = a_0 + y_1 \quad \text{with } a_0 = \lfloor x \rfloor, \ 0 \leq y_1 < 1$$

and $y_1 = \frac{1}{x_1}$ with $x_1 \geq 1$ (if $y_1 = 0$, do nothing)

continue with x_1: $x_1 = a_1 + x_2$, $a_1 = \lfloor x_1 \rfloor$

$$y_2 = \frac{1}{x_2}$$

At this point $x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{x_2}}$

continue with x_1, etc...

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \dots}}}}$$

convergents of x:

$$\underset{\frac{p_0}{q_0}}{\overset{\shortparallel}{a_0}}, \quad \underset{\frac{p_1}{q_1}}{\overset{\shortparallel}{a_0 + \frac{1}{a_1}}}, \quad \underset{\frac{p_2}{q_2}}{\overset{\shortparallel}{a_0 + \cfrac{1}{a_1 + \frac{1}{a_2}}}}, \quad \dots$$

Theorem A:

$$\left|x - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2}$$ (we say that $\frac{p_n}{q_n}$ is a good approx of x)

Theorem B:

If $\frac{p}{q}$ is a fraction s.t. $\left|x - \frac{p}{q}\right| < \frac{1}{2q^2}$

Then $\exists n$ s.t. $\frac{p}{q} = \frac{p_n}{q_n}$.

Examples: * $$\pi = 3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1 + \cfrac{1}{292 + \cdots}}}}$$

$\hookrightarrow$ $3, \frac{22}{7}, \frac{333}{106}, \frac{355}{113}, \ldots$

* $$\frac{1+\sqrt{5}}{2} = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cdots}}}}}$$

$1, \frac{3}{2}, \frac{5}{3}, \frac{8}{5}, \frac{13}{8}, \ldots$

Application to Shor's algorithm:

Final algorithm is:

① Run Shor's circuit and get the outcome $y \in \{0, \dots, 2^n - 1\}$

② compute $\frac{y}{2^n} \in [0,1]$ and its convergents $\frac{p_1}{q_1}, \dots, \frac{p_m}{q_m}$

③ for each q_i, check if $f(0) = f(q_i)$, if it's the case return q_i.

(Remark: if q_i is even, it's also interesting to try with $2q_i$)

Analysis: ① We proved that, with proba $\geq 16\%$ (in fact it's at least 60%)

$$\exists j \text{ s.t. } \left| \underbrace{\frac{y}{2^n}}_{x} - \frac{j}{r} \right| \leq \frac{1}{2^{n+1}}$$

② By theorem B, we know that $\frac{j}{r}$ is a convergent of $x := \frac{y}{2^n}$ if $2^n \geq r^2$,

which is true because we assumed $2^n \geq N^2 \geq r^2$.

i.e. $\frac{j}{r} = \frac{p_i}{q_i}$ for some i

So r is a multiple of q_i

Moreover, any j appears with proba at least $\frac{16\%}{r}$

Euler function

So the probability that j/r is irreducible is at least $0,16 \frac{\varphi(r)}{r}$,

which might unfortunately be small if r is really badly chosen.

However, if $n = p_1^{e_1} \cdots p_s^{e_s}$ (prime factorisation)

then $\dfrac{\varphi(n)}{n} = \left(1 - \dfrac{1}{p_1}\right) \cdots \left(1 - \dfrac{1}{p_s}\right)$

So $\dfrac{\varphi(n)}{n}$ can be as small as we want, but this requires n to be very large.

V Generalization to multivariate functions

Let $f : \mathbb{Z}^m \longrightarrow X$ ($m \in \mathbb{N}$, X is a set)

Definition:

A period of f is an element $a \in \mathbb{Z}^m$ s.t. $f(x+a) = f(x)$ $\forall x \in \mathbb{Z}^m$.

We will work with $P_f = \{a \in \mathbb{Z}^m$ s.t. a is a period of $a\}$

it's a subgroup of $\mathbb{Z}^m$.

In what follows, I will assume that P_f is a lattice, i.e. it contains a $\mathbb{Q}$-basis of $\mathbb{Q}^m$, or equivalently, the quotient $\mathbb{Z}^m / P_f$ is finite.

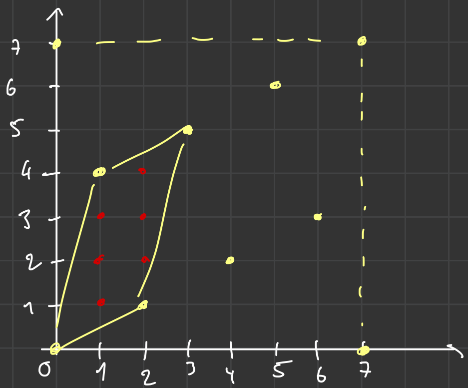
Example:

$$\begin{aligned} \mathbb{Z}^2 &\longrightarrow \mathbb{Z}/7\mathbb{Z} \\ (x,y) &\longmapsto 2x+3y \end{aligned}$$

(a,b) is a period $\Leftrightarrow 2a + 3b = 0 \pmod 7$

e.g. $(a,b) = (1,4)$

$(a,b) = (0,7)$



7
6
5
4
3
2
1
0
1
2
3
4
5
6
7