Shor's algorithm

<u>Objective:</u> let $f : \mathbb{Z}/2^n\mathbb{Z} \longrightarrow X$ a function s.t.

$\exists\, d \leq n$: - f is 2^d-periodic

- $f(x) = f(y)$ iff $2^d \mid x - y$

$\longrightarrow$ Find d.

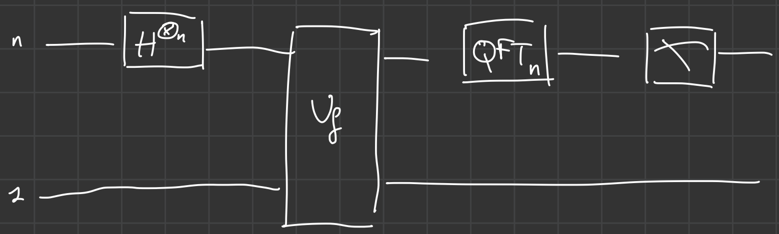
<u>Example:</u> $n = 3$

- f is $1, 2, 3, 4, 1, 2, 3, 4$

$\rightsquigarrow$ should output $d = 2$

- f can't be $1, 2, 3, 4, 5, 1, 2, 3$

<u>Shor's circuit:</u>



I The QFT-gate

Definition:

$$QTF_n(|x\rangle) = \frac{1}{2^{n/2}} \sum_{y \in \mathbb{Z}/2^n\mathbb{Z}} \zeta_n^{xy} |y\rangle \quad \text{where } \zeta_n = e^{\frac{2i\pi}{2^n}} \text{ and } y = y_0 + 2y_1 + 2^2 y_2 + \dots + 2^{n-1} y_{n-1}$$

Basic checking:

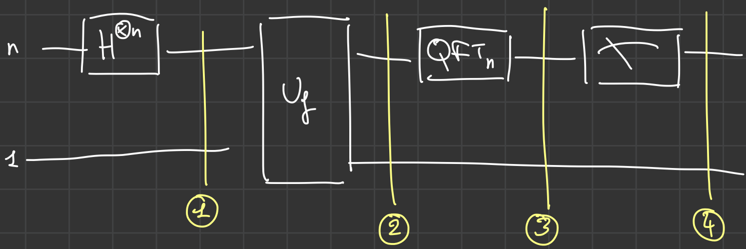
QFT_n is a unitary transformation, we check that it preserves the hermitian product, we only have to check it on the canonical basis.

Pick $x, x' \in \mathbb{Z}/2^n\mathbb{Z}$, compute hermitian product of $QFT_n(|x\rangle)$ and $QFT_n(|y\rangle)$:

$$A = \frac{1}{2^n} \sum_{y \in \mathbb{Z}/2^n\mathbb{Z}} \zeta_n^{xy} \overline{\zeta_n^{x'y}} = \frac{1}{2^n} \sum_{y=0}^{2^n-1} \left(\zeta_n^{x-x'}\right)^y$$

- If $x = x'$, get $A = \frac{2^n}{2^n} = 1$
- If $x \neq x' \pmod{2^n}$, then $\zeta_n^{x-x'} \neq 1$ so $A = \frac{1}{2^n} \dfrac{\left(\zeta_n^{x-x'}\right)^{2^n} - 1}{\zeta_n^{x-x'} - 1} = 0$

(II) Analysis of Shor's circuit



(1) $\frac{1}{2^{n/2}} \sum_{x \in \mathbb{Z}/2^n\mathbb{Z}} |x\rangle |0\rangle$

(2) $\frac{1}{2^{n/2}} \sum_{x \in \mathbb{Z}/2^n\mathbb{Z}} |x\rangle |f(x)\rangle$

(3) $\frac{1}{2^n} \sum_{x \in \mathbb{Z}/2^n\mathbb{Z}} \sum_{y \in \mathbb{Z}/2^n\mathbb{Z}} \zeta_n^{xy} |y\rangle |f(x)\rangle = \sum_{y \in \mathbb{Z}/2^n\mathbb{Z}} |y\rangle \otimes q_y$

with $q_y = \frac{1}{2^n} \sum_{x \in \mathbb{Z}/2^n\mathbb{Z}} \zeta_n^{xy} |f(x)\rangle$

(4) Remember that f is 2^d-periodic

$x = a + 2^d b$ with $0 \leq a \leq 2^d - 1$
$0 \leq b \leq 2^{n-d} - 1$

$$q_y = \frac{1}{2^n} \sum_{a=0}^{2^d-1} \underbrace{\left(\sum_{b=0}^{2^{n-d}-1} \zeta_n^{(a+2^d b)y} \right)}_{c_{a,y}} |f(a)\rangle$$

so $\|q_y\|^2 = \frac{1}{2^{2n}} \sum_{a=0}^{2^d-1} |c_{a,y}|^2$

$$C_{a,y} = \sum_{b=0}^{2^{n-d}-1} \zeta_n^{(a+2^d b)y} = \sum_{a=0}^{2^{n-d}-1} \zeta_n^{ay}\left(\zeta_n^{2^d y}\right)^b$$

- if $\zeta_n^{2^d y} = 1$ i.e. $2^n \mid 2^d y$ i.e $2^{n-d} \mid y$

then $C_{a,y} = \zeta_n^{ay}\, 2^{n-d}$ so $|C_{a,y}|^2 = 2^{2n-2d}$

- Otherwise (i.e. if $2^{n-d} \nmid y$)

$$C_{a,y} = \zeta_n^{ay} \frac{\left(\zeta_n^{2^d y}\right)^{2^{n-d}} - 1}{\zeta_n^{2^d y} - 1} = \zeta_n^{ay} \frac{\zeta_n^{2^n y} - 1}{\zeta_n^{2^d y} - 1} = 0$$

Conclusion:

* If $2^{n-d} \mid y$, then $\|q_y\|^2 = \frac{1}{2^{2n}} 2^d 2^{2n-2d} = \frac{1}{2^d}$

* If $2^{n-d} \nmid y$, then $\|q_y\|^2 = 0$

Hence: The outcome of the measure is a random uniformaly distributed multiple of 2^{n-d}.

What do we do now?

(1) We run Shor's algorithm several times and record the outputs (say $y_1, \dots, y_s$)

(2) Return: $d = \max_{1 \le i \le s} (n - v_2(y_i))$

Proposition: The output is correct with probability $1 - \frac{1}{2^s}$.

Proof: Write $y_i = 2^{n-d} z_i$, $0 \le z_i \le 2^d - 1$

The algorithm fails if all the z_i are even numbers.

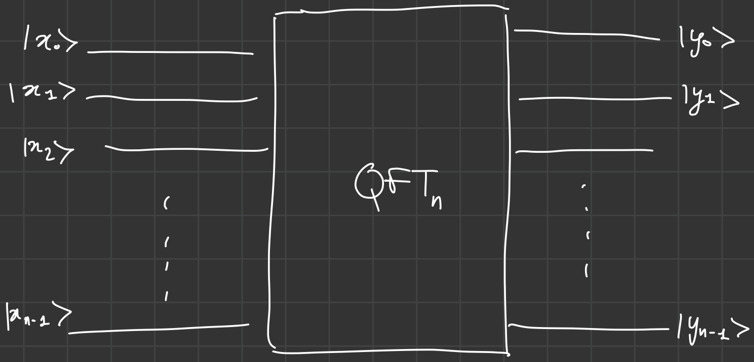
But z_i is even with proba $1/2$

So the algo fails with proba $1/2^s$

■

III Construction of the QFT-gate

General prototype:



$$QFT_n(|x\rangle) = \frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} \zeta_n^{xy} |y\rangle$$

$$x = x_0 + 2x_1 + \cdots 2^{n-1} x_{n-1}, \quad y = y_0 + \cdots + 2^{n-1} y_{n-1}$$

$$QFT(|x\rangle) = \frac{1}{2^{n/2}} \sum_{y_0, \dots, y_{n-1} \in \{0,1\}} \zeta_n^{x(y_0 + 2y_1 + \cdots + 2^{n-1} y_{n-1})} |y_{n-1} \cdots y_0\rangle$$

$$= \frac{1}{2^{n/2}} \underbrace{\left(\sum_{y_{n-1}=0}^{1} \zeta_n^{2^{n-1} x y_{n-1}} |y_{n-1}\rangle \right)}_{= |0\rangle + (-1)^x |1\rangle} \cdots \underbrace{\left(\sum_{y_1=0}^{1} \zeta_n^{2xy_1} |y_1\rangle \right)}_{= |0\rangle + \zeta_{n-1}^{x} |1\rangle} \underbrace{\left(\sum_{y_0=0}^{1} \zeta_n^{xy_0} |y_0\rangle \right)}_{= |0\rangle + \zeta_n^{x} |1\rangle}$$

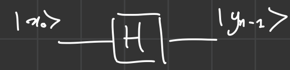
$$= \left(\frac{|0\rangle + (-1)^x |1\rangle}{\sqrt{2}} \right) \cdots \left(\frac{|0\rangle + \zeta_n^x |1\rangle}{\sqrt{2}} \right)$$

$\rightarrow$ Now our aim is to construct the 1-qubit $\dfrac{|0\rangle + \zeta_{n-i}^{x} |1\rangle}{\sqrt{2}}$

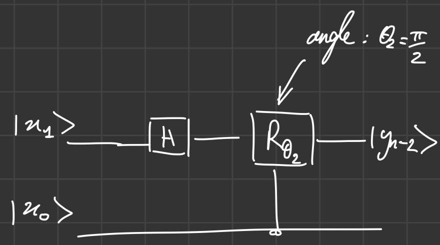
$$\frac{|0\rangle + \zeta_{n-i}^{x}|1\rangle}{\sqrt{2}} = \frac{|0\rangle + \zeta_{n-i}^{x_0+\dots+2^{n-1}x_{n-1}}|1\rangle}{\sqrt{2}}$$

$$= \frac{|0\rangle + \zeta_{n-i}^{x_0}\cdot \zeta_{n-i-1}^{x_1} \cdots \zeta_{1}^{x_{n-i-1}}|1\rangle}{\sqrt{2}}$$

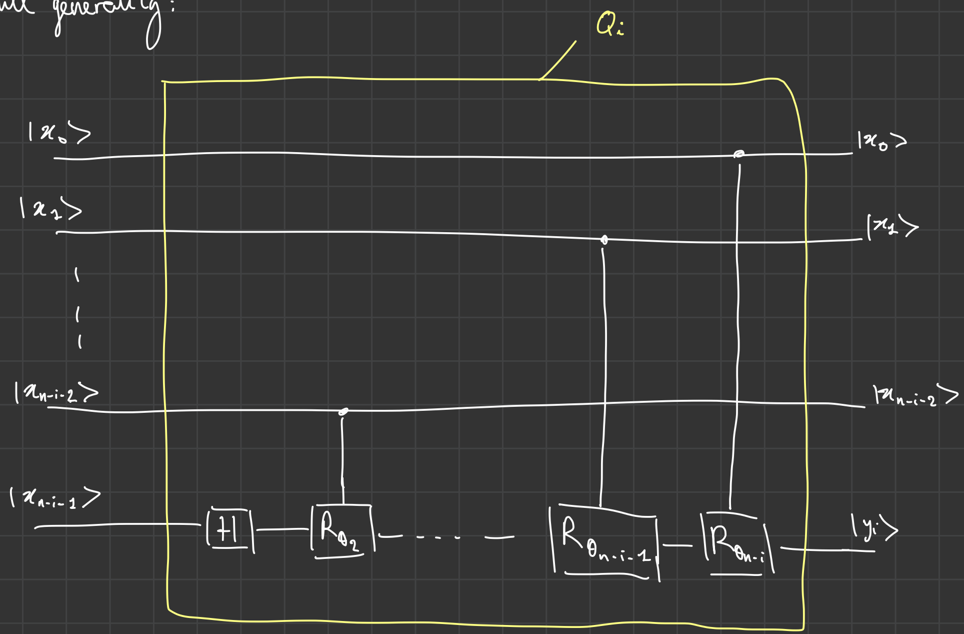
Case $n-i=1$ $(i=n-1)$: it's just $\frac{|0\rangle + (-1)^{x_0}|1\rangle}{\sqrt{2}}$



Case $n-i=2$: it's $\frac{|0\rangle + (-1)^{x_1}\zeta_2^{x_0}|1\rangle}{\sqrt{2}}$



In full generality:



$\left(\theta_i = \frac{2\pi}{2^i}\right)$

General prototype of QFT :