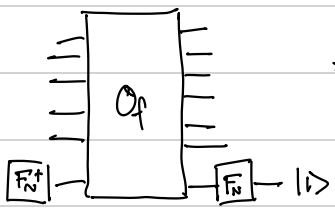
Alternate pf:

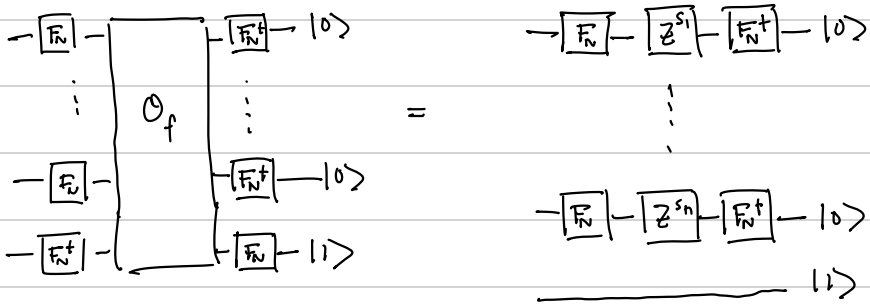
①



$$= \sum_{x_1,\dots,x_n} \omega^{-s_1 x_1} |x_1\rangle\langle x_1| \otimes \dots \otimes \omega^{-s_n x_n} |x_n\rangle\langle x_n| \otimes |1\rangle$$

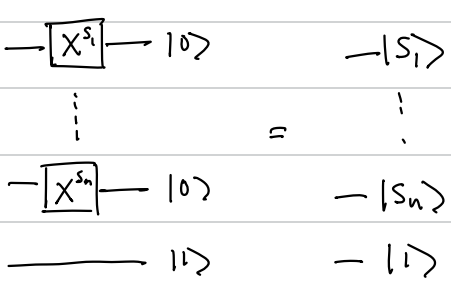
$$= Z^{s_1} \otimes \dots \otimes Z^{s_n} \otimes |1\rangle.$$

② $S o_1$



$Z = F_N^\dagger X F_N \Rightarrow F_N Z^s F_N^\dagger = X^s$

note $F_N^\dagger |0\rangle = F_N |0\rangle$.



Lessons:

① Diagonalize unitaries to generate phases

② Produce interference patterns to generate good outcomes.

How do we efficiently implement F_N?

Possible for all N but we will study here $N = 2^n$. In HW, feel free to assume we can implement efficiently for all N.

$$F_N |x\rangle = \bigotimes_{j=1}^{n} \frac{1}{\sqrt{2}} \left(|0\rangle + \omega^{x 2^{n-j}} |1\rangle \right) =: \bigotimes_{j=1}^{n} |\psi_j^{(x)}\rangle$$

Pf. $\langle y | \bigotimes_{j=1}^{n} \frac{1}{\sqrt{2}} \left(|0\rangle + \omega^{x 2^{n-j}} |1\rangle \right)$

$$= \prod_{j : y_j = 1} \omega^{x 2^{n-j}}$$

$$= \omega^{\left(\sum_{j=\gamma_j=1} x\,2^{n-j}\right)}$$

$$= \omega^{\left(x \cdot \underbrace{\sum_{j=1}^{n} \gamma_j 2^{n-j}}_{\text{binary decomposition of } \gamma}\right)}$$

$$= \omega^{x \cdot \gamma}. \qquad \blacksquare$$

Notice $\omega^{x\,2^{n-j}} = \omega^{(x\,2^{n-j} \bmod N)}$

$$x \cdot 2^{n-j} \bmod N = \sum_{k=1}^{n} x_k\, 2^{n-k} \cdot 2^{n-j} \bmod N$$

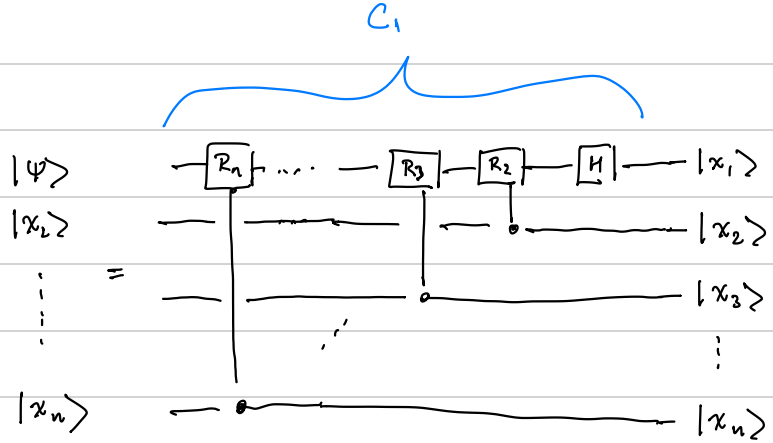
$$= \sum_{k \geq n-j}^{n} x_k\, 2^{2n-k-j}.$$

Using this, let's write a q. circuit for QFT.

gates: H, $R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{pmatrix}$ and $CR_k = \begin{pmatrix} \mathbb{1}_2 & \\ & R_k \end{pmatrix}$

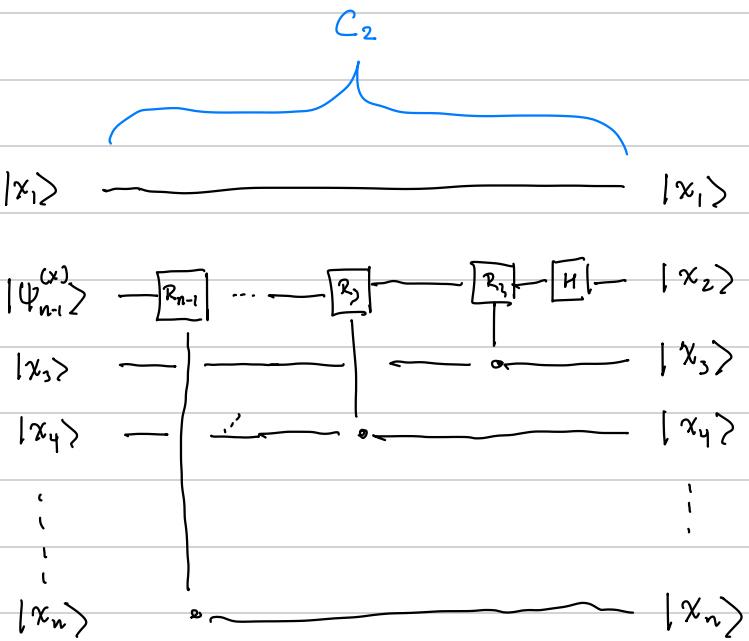
$$e^{2\pi i/2^k} = \omega^{(2^{n-k})}$$

Subcircuit:

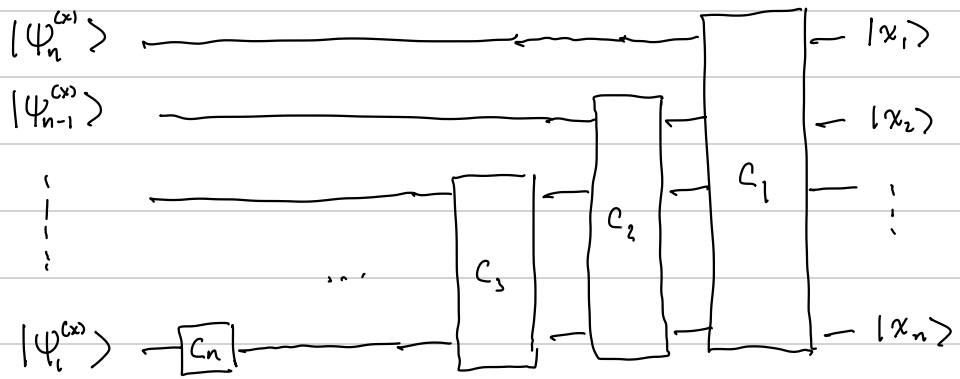


$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + \omega^{\left(\sum_{k=1}^{n} 2^{n-k} x_k\right)}|1\rangle\right) = |\psi_n^{(x)}\rangle$$

Similarly,



So,



Correct up to permutation of gates.

Need to append $\text{SWAP}_{1,n}$ $\text{SWAP}_{2,n-1}$, ... $\text{SWAP}_{\frac{n}{2},\frac{n}{2}+1}$.

This produces F_N transform for any fixed $N = 2^n$.

C_1 has n gates, C_2 has $n-1$ gates, ...

total $O(n^2)$ gates + n swap gates.

There is still a fundamental issue: $C\text{-}R_k$ gates may be expensive to apply.

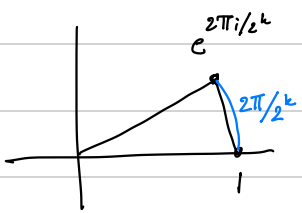
Not all $C\text{-}R_k$ gates may be necessary.

Consider replacing gates g in ckt with g' s.t.

$$\|g - g'\| \leq \epsilon.$$

By unitarity, total change in output POVM is also ϵ.

$$C\text{-}R_k = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & e^{2\pi i/2^k} \end{pmatrix} \quad \text{so}$$



$$\| C\text{-}R_k - \mathbb{1}_4 \| = \left| e^{2\pi i/2^k} - 1 \right| \leq \frac{2\pi}{2^k}.$$

Notice $C\text{-}R_k$ gate appears $n-k$ times in QFT circuit.

Total error of replacing each $C\text{-}R_k$ gate with $\mathbb{1}$ for $k \geq K$:

$$\leq \frac{2\pi}{2^K} \frac{(n-K)(n-K+1)}{2} \leq \frac{n^2}{2^K}$$

If we tolerate ϵ error in our QFT unitary, we can ignore every $C\text{-}R_k$ gates for $K \geq \log\left(\frac{n^2}{\epsilon}\right)$.

We have reduced from $O(n^2)$ gates to $O(n \log \frac{n}{\epsilon})$ gates.

Time permitting, we will see how to generate any remaining gates approximately from a family of standard gates.

This is called the Solovay-Kitaev theorem

We saw how when the info of the problem is hidden in the Fourier basis, we can use the q. computers ability to switch bases to access the info faster.

Simon's problem advances the separation from the Bernstein-Vazirani problem to an exponential advantage.

Def (Simon's problem)

Let $f: \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ be a fn s.t. $\forall\, x, y \in \mathbb{Z}_2^n$ with $x \neq y$,

$$f(x) = f(y) \iff x = y \oplus s.$$

for some hidden secret $s \neq 0^n$. Find s. ← "hidden shift"

Classical lower bound:

If we have a guess for s, we can check it by checking for any x if $f(x) = f(x \oplus s)$.

Decision problem: Decide if f has a "hidden shift" vs if f is a permutation.

Consider queries at location $x_1, \ldots, x_j, \ldots$ until we find a collision $(f(x_i) = f(x_j))$, then fn f is indistinguishable from some permutation π.

Birthday paradox tells us that it will take $\Theta(\sqrt{2^n})$ random queries until a collision is found.

gives optimal classical algorithm.

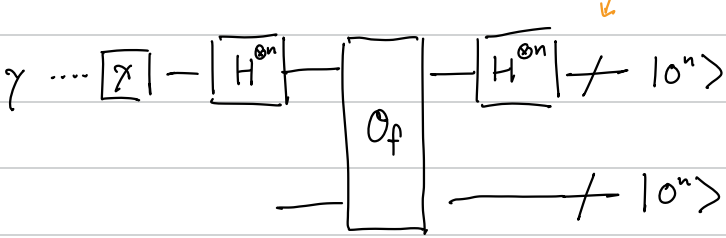
Q. alg.: Construct a subroutine that outputs a uniformly random y s.t. $s \cdot y = 0$.

given this subroutine, we can calculate s after $\sim O(n)$ iterations of this subroutine. (After $O(n)$ iterations, whp there is a unique sol. to the set of eqs.)

Access: $O_f |x\rangle|y\rangle \mapsto |x\rangle|y + f(x)\rangle$

Alg:

refer to many qubits



Analysis:

Before oracle, state is $\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \otimes |0^n\rangle$

After, $\frac{1}{\sqrt{2^n}} \sum_x |x\rangle \otimes |f(x)\rangle$.

$$= \frac{1}{\sqrt{2^{n-1}}} \sum_{y \in \text{im} f} \left(\underbrace{\frac{1}{\sqrt{2}} \sum_{x \in f^{-1}(y)} |x\rangle}_{:= |\psi_y\rangle} \right) \otimes |y\rangle$$

$$= \frac{1}{\sqrt{2^{n-1}}} \sum_{y \in \text{im} f} |\psi_y\rangle |y\rangle.$$

Tracing out 2nd register, ...

$$\rho = \frac{1}{2^{n-1}} \sum_{z \in \text{im} f} |\psi_z\rangle\langle\psi_z|.$$

$$H^{\otimes n} \rho H^{\otimes n} = \frac{1}{2^{n-1}} \sum_{z \in \text{im} f} H^{\otimes n} |\psi_z\rangle\langle\psi_z| H^{\otimes n}.$$

$$H^{\otimes n}|\psi_z\rangle = \frac{1}{\sqrt{2}} H^{\otimes n}\left(|x\rangle + |x+s\rangle\right)$$

for $x \in f^{-1}(z)$ as the two sols differ by s.

$$= \frac{1}{\sqrt{2^{n+1}}}\left(\sum_y (-1)^{x\cdot y}|y\rangle + \sum_y (-1)^{(x+s)\cdot y}|y\rangle\right)$$

$$= \frac{1}{\sqrt{2^{n+1}}}\left(\sum_y (-1)^{x\cdot y}\left(1 + (-1)^{s\cdot y}\right)|y\rangle\right)$$

$$= \frac{1}{\sqrt{2^{n+1}}} \sum_{y\,:\,s\cdot y = 0} (-1)^{x\cdot y}|y\rangle$$

measuring this pure state gives uniformly random y s.t. $s\cdot y = 0$. This is indep. of z, so full algorithm generates uniformly random y s.t. $s\cdot y = 0$.

What is going on? After tracing out 2nd register, resulting dist. is a uniform mixture over coset uniform superpositions. To describe this we need to introduce some group theory.