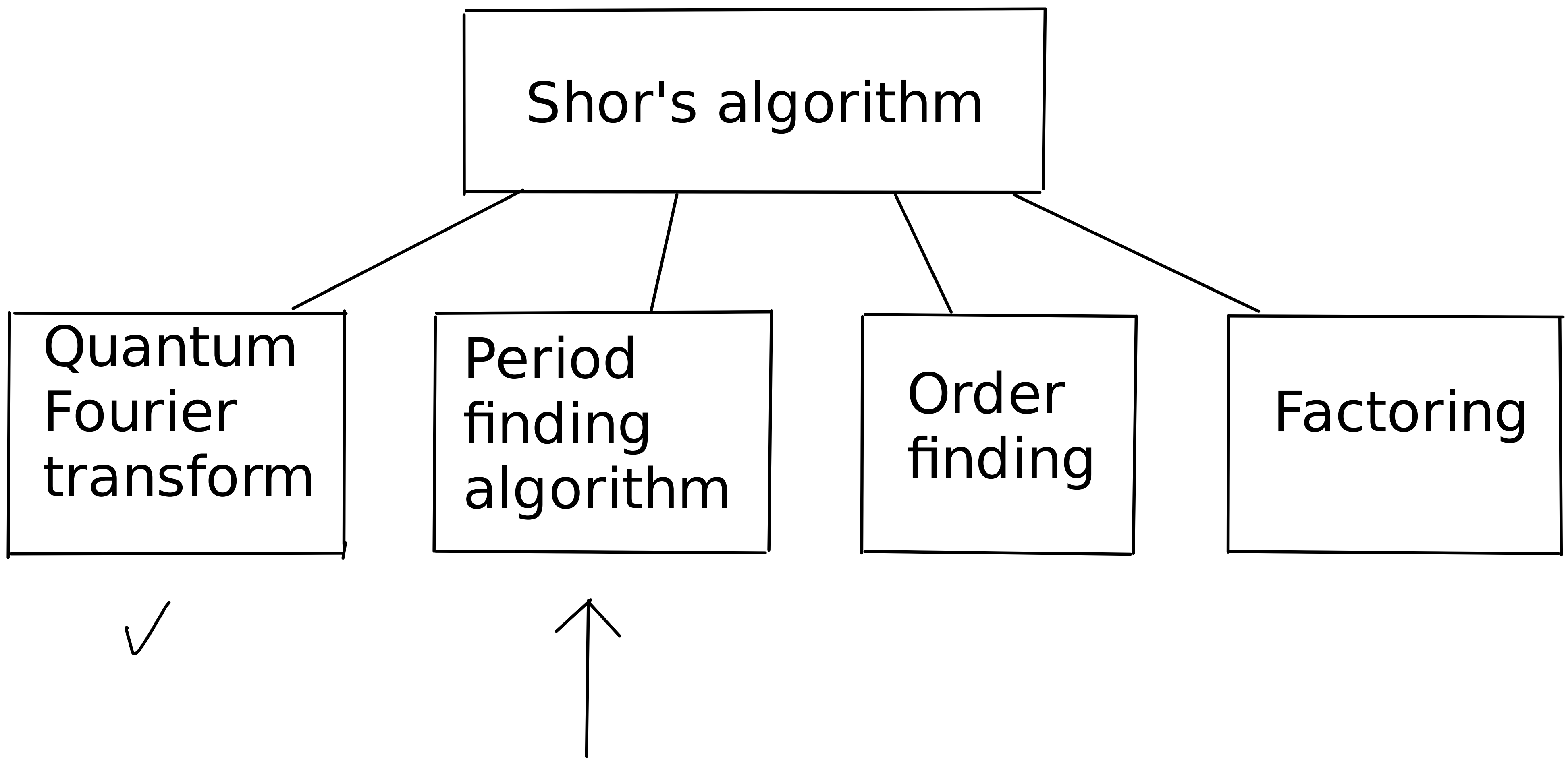


Shor's algorithm
Quantum Fourier transform
Period finding algorithm
Order finding
Factoring

Period finding:

Given: $d \in \mathbb{N}$, and a black box for a function

$$f: \{0,1,\ldots,d-1\} \longrightarrow \{0,1,\ldots,m-1\}.$$

Promise: $\exists$ r s.t.

$f(x) = f(y)$ iff $x \equiv y \bmod r$ (let $r|d$ for now*)

Problem: determine r

Period finding:

Given: $d \in \mathbb{N}$, and a black box for a function $f:\{0,1,\ldots,d-1\} \longrightarrow \{0,1,..,m-1\}$.

Promise: $\exists$ r s.t.
$f(x) = f(y)$ iff $x \equiv y \bmod r$ (let r|d for now*)

Problem: determine r

* Note f can only be periodic with period r if r|d.
But r is unknown to the problem solver ...
So, this assumption trivializes the problem.

Period finding:

Given: $d \in \mathbb{N}$, and a black box for a function
$$f:\{0,1,\ldots,d-1\} \longrightarrow \{0,1,\ldots,m-1\}.$$

Promise: $\exists$ r s.t.
$f(x) = f(y)$ iff $x \equiv y \bmod r$ (let r|d for now*)

Problem: determine r

* Note f can only be periodic with period r if r|d.
But r is unknown to the problem solver ...
So, this assumption trivializes the problem.

Plan: (1) find an algorithm "PF1" for the r|d case;
(2) take large d to approximate r|d, modify algorithm "PF1" to "PF2" and show the latter works.

Period finding algorithm: "PF1 for the case r|d"

(I) The quantum subroutine (essentially same as Simon's alg)

1. Prepare superposition of inputs on 1st register

$$F|0\rangle = \frac{1}{\sqrt{d}} \sum_{x=0}^{d-1} |x\rangle \quad , \text{ where } F = \text{QFT over } \mathbb{Z}_d .$$

Period finding algorithm: "PF1 for the case r|d"

(I) The quantum subroutine (essentially same as Simon's alg)

1. Prepare superposition of inputs on 1st register

$$F|0\rangle = \frac{1}{\sqrt{d}} \sum_{x=0}^{d-1} |x\rangle \quad , \text{ where } F = \text{QFT over } \mathbb{Z}_d .$$

2. Prepare $|0\rangle$ in 2nd register and apply blackbox U_f .

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

$$= \frac{1}{\sqrt{d}} \sum_{x_0=0}^{r-1} \sum_{k=0}^{\frac{d}{r}-1} |x_0+kr\rangle |f(x_0)\rangle$$

Period finding algorithm: "PF1 for the case r|d"

(I) The quantum subroutine (essentially same as Simon's alg)

1. Prepare superposition of inputs on 1st register

$$F|0\rangle = \frac{1}{\sqrt{d}} \sum_{x=0}^{d-1} |x\rangle \quad , \quad \text{where } F = \text{QFT over } \mathbb{Z}_d .$$

2. Prepare $|0\rangle$ in 2nd register and apply blackbox U_f .

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

$$= \frac{1}{\sqrt{d}} \sum_{x_0=0}^{r-1} \sum_{k=0}^{\frac{d}{r}-1} |x_0+kr\rangle|f(x_0)\rangle$$

e.g., d=6, r=3, f(x) = x mod r.

$$U_f\left(\frac{1}{\sqrt{6}} \sum_{x=0}^{5} |x\rangle|0\rangle\right) = \frac{1}{\sqrt{6}}\begin{pmatrix} +|0\rangle|0\rangle + |1\rangle|1\rangle + |2\rangle|2\rangle \\ +|3\rangle|0\rangle + |4\rangle|1\rangle + |5\rangle|2\rangle \end{pmatrix}$$

$$\begin{array}{ccc} x_0=0 & x_0=1 & x_0=2 \\ f(x_0)=0 & f(x_0)=1 & f(x_0)=2 \end{array}$$

2. $$U_f\left(\frac{1}{\sqrt{d}}\sum_{x=0}^{d-1}|x\rangle|0\rangle\right) = \frac{1}{\sqrt{d}}\sum_{x_0=0}^{r-1}\sum_{k=0}^{\frac{d}{r}-1}|x_0+kr\rangle|f(x_0)\rangle$$

3. Measure 2nd register.

If outcome y = f(s), post-meas state on 1st register:

$$|\psi_{r,s}\rangle = \frac{\sqrt{r}}{\sqrt{d}}\sum_{k=0}^{\frac{d}{r}-1}|s+kr\rangle$$

"periodic state" with period r, shift s, d/r repetitions.

2. $$U_f\left(\frac{1}{\sqrt{d}}\sum_{x=0}^{d-1}|x\rangle|0\rangle\right) = \frac{1}{\sqrt{d}}\sum_{x_0=0}^{r-1}\sum_{k=0}^{\frac{d}{r}-1}|x_0+kr\rangle|f(x_0)\rangle$$

3. Measure 2nd register.

If outcome y = f(s), post-meas state on 1st register:

$$|\psi_{r,s}\rangle = \frac{\sqrt{r}}{\sqrt{d}}\sum_{k=0}^{\frac{d}{r}-1}|s+kr\rangle$$

"periodic state" with period r, shift s, d/r repetitions.

e.g., meas $$\frac{1}{\sqrt{6}}\begin{pmatrix} +|0\rangle|0\rangle + |1\rangle|1\rangle + |2\rangle|2\rangle \\ +|3\rangle|0\rangle + |4\rangle|1\rangle + |5\rangle|2\rangle \end{pmatrix}$$

$x_0=0$, $f(x_0)=0$ $\quad$ $x_0=1$, $f(x_0)=1$ $\quad$ $x_0=2$, $f(x_0)=2$

Question: if outcome = 1, post-meas state = ?

(a) $|1\rangle$ (b) $\frac{1}{\sqrt{2}}(|0\rangle+|3\rangle)$ (c) $\frac{1}{\sqrt{2}}(|1\rangle+|4\rangle)$

2. $U_f\left(\frac{1}{\sqrt{d}}\sum_{x=0}^{d-1}|x\rangle|0\rangle\right) = \frac{1}{\sqrt{d}}\sum_{x_0=0}^{r-1}\sum_{k=0}^{\frac{d}{r}-1}|x_0+kr\rangle|f(x_0)\rangle$

3. Measure 2nd register.

If outcome y = f(s), post-meas state on 1st register:

$$|\psi_{r,s}\rangle = \frac{\sqrt{r}}{\sqrt{d}}\sum_{k=0}^{\frac{d}{r}-1}|s+kr\rangle$$

"periodic state" with period r, shift s, d/r repetitions.

e.g.2, $\frac{1}{\sqrt{2}}(|x\rangle+|x\oplus p\rangle)$ from Simon's algorithm has multi-dim period "p" (equivalent to d/2), random shift x, and d/r = 2 repetitions.

NB: For $s \in \{0,1,\ldots,r-1\}$ each f(s) occurs with prob 1/r.

3. $|\psi_{r,s}\rangle = \frac{\sqrt{r}}{\sqrt{d}} \sum_{k=0}^{\frac{d}{r}-1} |s + kr\rangle$

As before, computational basis meas yields a random outcome (over the range of f) with no info on r.

3. $|\psi_{r,s}\rangle = \frac{\sqrt{r}}{\sqrt{d}} \sum_{k=0}^{\frac{d}{r}-1} |s+kr\rangle$

As before, computational basis meas yields a random outcome with no info on r.

To learn about r: measure in Fourier basis
i.e., invert F (QFT) (step 4), and
measure in computational basis (step 5).

4. Invert F (QFT) on the first register.

* Finding $F^{\dagger}$:

$$F : |x\rangle \longrightarrow |\tilde{x}\rangle = \frac{1}{\sqrt{d}} \sum_{y=0}^{d-1} e^{\frac{2\pi i}{d} x y} |y\rangle$$

$$F = \sum_{x=0}^{d-1} |\tilde{x}\rangle\langle x|$$

4. Invert F (QFT) on the first register.

* Finding $F^{\dagger}$:

$$F : |u\rangle \longrightarrow |\tilde{u}\rangle = \frac{1}{\sqrt{d}} \sum_{w=0}^{d-1} e^{\frac{2\pi i}{d} uw} |w\rangle$$

$$F = \sum_{u=0}^{d-1} |\tilde{u}\rangle\langle u|$$

Use new symbols, $x \rightarrow u$, $y \rightarrow w$

4. Invert F (QFT) on the first register.

* Finding $F^\dagger$:

$$F : |u\rangle \longrightarrow |\tilde{u}\rangle = \frac{1}{\sqrt{d}} \sum_{w=0}^{d-1} e^{\frac{2\pi i}{d} uw} |w\rangle$$

$$F = \sum_{u=0}^{d-1} |\tilde{u}\rangle\langle u|$$

$$\therefore F^\dagger = \sum_{u=0}^{d-1} |u\rangle\langle \tilde{u}| = \frac{1}{\sqrt{d}} \sum_{u=0}^{d-1} \sum_{w=0}^{d-1} e^{-\frac{2\pi i}{d} uw} |u\rangle\langle w|$$

4. Invert F (QFT) on the first register.

* Finding $F^\dagger$:

$$F : |u\rangle \rightarrow |\tilde{u}\rangle = \frac{1}{\sqrt{d}} \sum_{w=0}^{d-1} e^{\frac{2\pi i}{d} uw} |w\rangle$$

$$F = \sum_{u=0}^{d-1} |\tilde{u}\rangle\langle u|$$

$$\therefore F^\dagger = \sum_{u=0}^{d-1} |u\rangle\langle\tilde{u}| = \frac{1}{\sqrt{d}} \sum_{u=0}^{d-1} \sum_{w=0}^{d-1} e^{-\frac{2\pi i}{d} uw} |u\rangle\langle w|$$

* Inverting F:

$$F^\dagger |\psi_{r,s}\rangle = F^\dagger \frac{\sqrt{r}}{\sqrt{d}} \sum_{k=0}^{\frac{d}{r}-1} |s+kr\rangle$$

periodic state from step 3

4. Invert F (QFT) on the first register.

* Finding $F^\dagger$:

$$F : |u\rangle \longrightarrow |\tilde{u}\rangle = \frac{1}{\sqrt{d}} \sum_{w=0}^{d-1} e^{\frac{2\pi i}{d} uw} |w\rangle$$

$$F = \sum_{u=0}^{d-1} |\tilde{u}\rangle\langle u|$$

$$\therefore F^\dagger = \sum_{u=0}^{d-1} |u\rangle\langle\tilde{u}| = \frac{1}{\sqrt{d}} \sum_{u=0}^{d-1} \sum_{w=0}^{d-1} e^{-\frac{2\pi i}{d} uw} |u\rangle\langle w|$$

* Inverting F:

$$F^\dagger |\psi_{r,s}\rangle = F^\dagger \frac{\sqrt{r}}{\sqrt{d}} \sum_{k=0}^{\frac{d}{r}-1} |s+kr\rangle$$

$$= \frac{\sqrt{r}}{d} \sum_{k=0}^{\frac{d}{r}-1} \sum_{u=0}^{d-1} \sum_{w=0}^{d-1} e^{-\frac{2\pi i}{d} uw} |u\rangle\langle w|s+kr\rangle$$

4. Invert F (QFT) on the first register.

* Finding $F^{\dagger}$:

$$F : |u\rangle \longrightarrow |\tilde{u}\rangle = \frac{1}{\sqrt{d}} \sum_{w=0}^{d-1} e^{\frac{2\pi i}{d} uw} |w\rangle$$

$$F = \sum_{u=0}^{d-1} |\tilde{u}\rangle\langle u|$$

$$\therefore F^{\dagger} = \sum_{u=0}^{d-1} |u\rangle\langle\tilde{u}| = \frac{1}{\sqrt{d}} \sum_{u=0}^{d-1} \sum_{w=0}^{d-1} e^{-\frac{2\pi i}{d} uw} |u\rangle\langle w|$$

* Inverting F:

$$F^{\dagger} |\psi_{r,s}\rangle = F^{\dagger} \frac{\sqrt{r}}{\sqrt{d}} \sum_{k=0}^{\frac{d}{r}-1} |s+kr\rangle$$

$$= \frac{\sqrt{r}}{d} \sum_{k=0}^{\frac{d}{r}-1} \sum_{u=0}^{d-1} \sum_{w=0}^{d-1} e^{-\frac{2\pi i}{d} uw} |u\rangle \underbrace{\langle w | s+kr\rangle}_{\therefore w = s+kr}$$

$$= \frac{\sqrt{r}}{d} \sum_{k=0}^{\frac{d}{r}-1} \sum_{u=0}^{d-1} e^{-\frac{2\pi i}{d} u(s+kr)} |u\rangle$$

4. $$F^{\dagger}|\psi_{r,s}\rangle = \frac{\sqrt{r}}{d}\sum_{k=0}^{\frac{d}{r}-1}\sum_{u=0}^{d-1} e^{-\frac{2\pi i}{d}u(s+kr)}|u\rangle$$

The amplitude for u =

$$\frac{\sqrt{r}}{d}\sum_{k=0}^{\frac{d}{r}-1} e^{-\frac{2\pi i}{d}u(s+kr)}$$

4. $F^\dagger |\psi_{r,s}\rangle = \frac{\sqrt{r}}{d} \sum_{k=0}^{\frac{d}{r}-1} \sum_{u=0}^{d-1} e^{-\frac{2\pi i}{d} u(s+kr)} |u\rangle$

The amplitude for u =

$$\frac{\sqrt{r}}{d} \sum_{k=0}^{\frac{d}{r}-1} e^{-\frac{2\pi i}{d} u(s+kr)} = e^{-\frac{2\pi i}{d} us} \frac{\sqrt{r}}{d} \sum_{k=0}^{\frac{d}{r}-1} \left(e^{-\frac{2\pi i}{d} ur}\right)^k$$

4. $F^{\dagger}|\Psi_{r,s}\rangle = \frac{\sqrt{r}}{d}\sum_{k=0}^{\frac{d}{r}-1}\sum_{u=0}^{d-1} e^{-\frac{2\pi i}{d}u(s+kr)}|u\rangle$

The amplitude for u =

$$\frac{\sqrt{r}}{d}\sum_{k=0}^{\frac{d}{r}-1} e^{-\frac{2\pi i}{d}u(s+kr)} = e^{-\frac{2\pi i}{d}us}\,\frac{\sqrt{r}}{d}\sum_{k=0}^{\frac{d}{r}-1}\left(e^{-\frac{2\pi i}{d}ur}\right)^{k}$$

$$\sum_{k=0}^{\frac{d}{r}-1}\left(e^{-\frac{2\pi i}{d}ur}\right)^{k} = \begin{cases} \dfrac{e^{-2\pi i u}-1}{e^{-2\pi i u\frac{r}{d}}-1} = 0 & \text{if } u \not\equiv 0 \bmod \frac{d}{r} \\[2ex] \dfrac{d}{r} & \text{if } u \equiv 0 \bmod \frac{d}{r} \end{cases}$$

4. $$F^\dagger|\Psi_{r,s}\rangle = \frac{\sqrt{r}}{d}\sum_{k=0}^{\frac{d}{r}-1}\sum_{u=0}^{d-1} e^{-\frac{2\pi i}{d}u(s+kr)}|u\rangle$$

The amplitude for u =

$$\frac{\sqrt{r}}{d}\sum_{k=0}^{\frac{d}{r}-1} e^{-\frac{2\pi i}{d}u(s+kr)} = e^{-\frac{2\pi i}{d}us}\frac{\sqrt{r}}{d}\sum_{k=0}^{\frac{d}{r}-1}\left(e^{-\frac{2\pi i}{d}ur}\right)^k$$

$$\sum_{k=0}^{\frac{d}{r}-1}\left(e^{-\frac{2\pi i}{d}ur}\right)^k = \begin{cases} \dfrac{e^{-2\pi i u}-1}{e^{-2\pi i u\frac{r}{d}}-1} = 0 & \text{if } u \not\equiv 0 \bmod \frac{d}{r} \\ \dfrac{d}{r} & \text{if } u \equiv 0 \bmod \frac{d}{r} \end{cases}$$

$$\therefore F^\dagger|\Psi_{r,s}\rangle = \sum_{\substack{u=0 \\ u\equiv 0 \bmod \frac{d}{r}}}^{d-1} \frac{1}{\sqrt{r}} e^{-\frac{2\pi i}{d}us}|u\rangle$$

$$4.\quad F^\dagger|\psi_{r,s}\rangle = \frac{\sqrt{r}}{d}\sum_{k=0}^{\frac{d}{r}-1}\sum_{u=0}^{d-1} e^{-\frac{2\pi i}{d}u(s+kr)}|u\rangle$$

The amplitude for u =

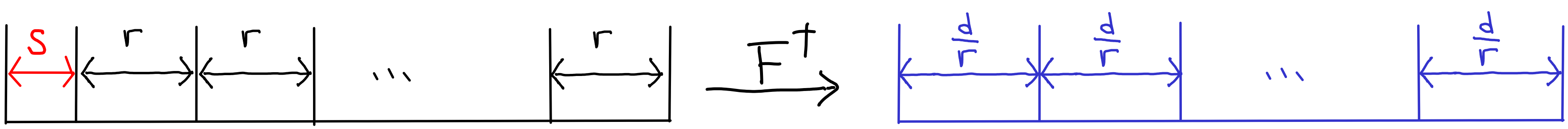
$$\frac{\sqrt{r}}{d}\sum_{k=0}^{\frac{d}{r}-1} e^{-\frac{2\pi i}{d}u(s+kr)} = e^{-\frac{2\pi i}{d}us}\,\frac{\sqrt{r}}{d}\sum_{k=0}^{\frac{d}{r}-1}\left(e^{-\frac{2\pi i}{d}ur}\right)^k$$

$$\sum_{k=0}^{\frac{d}{r}-1}\left(e^{-\frac{2\pi i}{d}ur}\right)^k = \begin{cases} \dfrac{e^{-2\pi i u}-1}{e^{-2\pi i u\frac{r}{d}}-1} = 0 & \text{if } u \not\equiv 0 \bmod \frac{d}{r} \\[2ex] \dfrac{d}{r} & \text{if } u \equiv 0 \bmod \frac{d}{r} \end{cases}$$

$$\therefore\ \underbrace{F^\dagger|\psi_{r,s}\rangle}_{\frac{\sqrt{r}}{\sqrt{d}}\sum_{k=0}^{\frac{d}{r}-1}|s+kr\rangle} = \sum_{\substack{u=0 \\ u\equiv 0 \bmod \frac{d}{r}}}^{d-1} \frac{1}{\sqrt{r}}\, e^{-\frac{2\pi i}{d}us}\,|u\rangle$$

make random s irrelevant by meas u

info on r carried by u



4. $$F^\dagger |\Psi_{r,s}\rangle = \sum_{\substack{u=0 \\ u \equiv 0 \bmod \frac{d}{r}}}^{d-1} \frac{1}{\sqrt{r}} e^{-\frac{2\pi i}{d} us} |u\rangle$$

4. $F^\dagger |\psi_{r,s}\rangle = \sum_{\substack{u=0 \\ u \equiv 0 \bmod \frac{d}{r}}}^{d-1} \frac{1}{\sqrt{r}} e^{-\frac{2\pi i}{d} us} |u\rangle$

5. Measure the first (above) register, outcome = z.

$$\Pr(z) = \begin{cases} 0 & \text{if } z \not\equiv 0 \bmod \frac{d}{r} \\ \frac{1}{r} & \text{if } z \equiv 0 \bmod \frac{d}{r} \end{cases}$$

End of quantum subroutine in PF1 for r|d.
It outputs one sample of z = jd/r for some j uniformly chosen from {0,1,...,r-1}.

Period finding algorithm: "PF1 for the case r|d"

(I) Quantum subroutine summary

1. Prepare superposition of inputs $\overset{\text{QFT}}{F}|0\rangle = \frac{1}{\sqrt{d}}\sum_{x=0}^{d-1}|x\rangle$

2. Prepare $|0\rangle$ in 2nd register and apply blackbox U_f .

$$U_f\left(\frac{1}{\sqrt{d}}\sum_{x=0}^{d-1}|x\rangle|0\rangle\right) = \frac{1}{\sqrt{d}}\sum_{x_0=0}^{r-1}\sum_{k=0}^{\frac{d}{r}-1}|x_0+kr\rangle|f(x_0)\rangle$$

can be omitted!

3. Measure second register. 1st register left in state:

$$|\psi_{r,s}\rangle = \frac{\sqrt{r}}{\sqrt{d}}\sum_{k=0}^{\frac{d}{r}-1}|s+kr\rangle$$ for a random $s \in \{0,1,\dots,r-1\}$

4. Invert F (QFT) on the 1st register: $\displaystyle\sum_{\substack{u=0 \\ u\equiv 0 \bmod \frac{d}{r}}}^{d-1}\frac{1}{\sqrt{r}}\,e^{-\frac{2\pi i}{d}us}|u\rangle$

5. Measure the 1st register to get

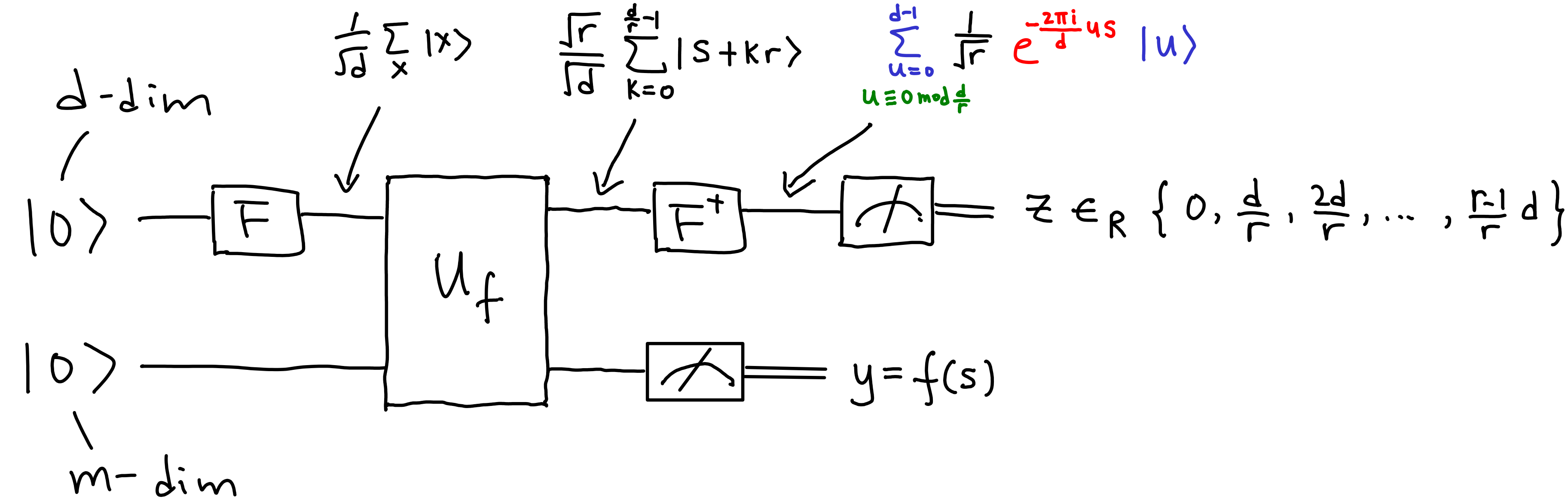
info on r

randomness

$z = j\frac{d}{r}$ for $j \in_R \{0,1,2,\dots,r-1\}$

Period finding algorithm: "PF1 for the case r|d"

(1) Quantum subroutine circuit:



Period finding algorithm: "PF1 for the case $r|d$"

(2) Classical processing:

Question: given $z = j\, d/r$,
with random j and r unknown,
how to find r ?

Period finding algorithm: "PF1 for the case r|d"

(2) Classical processing:

Question: given z = j d/r,
with random j and r unknown,
how to find r ?

(a) Need more samples !

Repeat quantum subroutine 2t times (tbd), get:

$$z_1 = \bar{j}_1 \frac{d}{r}, \quad z_2 = \bar{j}_2 \frac{d}{r}, \quad \ldots, \quad z_{2t} = \bar{j}_{2t} \frac{d}{r}$$

where $\bar{j}_1, \bar{j}_2, \ldots, \bar{j}_{2t}$ are random (and unknown).

Period finding algorithm: "PF1 for the case $r|d$"

(2) Classical processing:

Question: given $z = j\, d/r$,
with random j and r unknown,
how to find r ?

(a) Need more samples !

Repeat quantum subroutine 2t times (tbd), get:

$$z_1 = \bar{j}_1 \frac{d}{r}, \quad z_2 = \bar{j}_2 \frac{d}{r}, \quad \ldots, \quad z_{2t} = \bar{j}_{2t} \frac{d}{r}$$

where $\bar{j}_1, \bar{j}_2, \ldots, \bar{j}_{2t}$ are random (and unknown).

(b) How to convert $z_1, z_2, \ldots, z_{2t}$ to r ?

Known: $z_1, z_2, \ldots, z_{2t}$

Unknown: $\bar{j}_1, \bar{j}_2, \ldots, \bar{j}_{2t}, r$

How to obtain r from random samples of $j\frac{d}{r}$?

e.g. d=72, r=8, d/r = 9

j =	0	1	2	3	4	5	6	7
z = jd/r =	0	9	18	27	36	45	54	63

what you don't observe (e.g, j and r)

what you may sample from, 1 sample at a time tell r=8 from r=12

How to ~~obtain r~~ from random samples of $j\frac{d}{r}$?

e.g. d=72, r=8, d/r = 9

j =	0	1	2	3	4	5	6	7
z = jd/r =	0	9	18	27	36	45	54	63

e.g. d=72, r=12, d/r = 6

j =	0	1	2	3	4	5	6	7	8	9	10	11
z = jd/r =	0	6	12	18	24	30	36	42	48	54	60	66

what you don't observe (e.g, j and r)

what you may sample from, 1 sample at a time

How to obtain r from random samples of $j\frac{d}{r}$?

e.g. d=72, r=8, d/r = 9

j =	0	1	2	3	4	5	6	7
z = jd/r =	0	9	18	27	36	45	54	63

e.g. d=72, r=12, d/r = 6

j =	0	1	2	3	4	5	6	7	8	9	10	11
z = jd/r =	0	6	12	18	24	30	36	42	48	54	60	66

Say, z1 = 18, z2 = 36, z3 = 54. Is r = 8 or 12?

How to obtain r from random samples of $j \frac{d}{r}$?

e.g. d=72, r=8, d/r = 9

j =	0	1	2	3	4	5	6	7
z = jd/r =	0	9	18	27	36	45	54	63

e.g. d=72, r=12, d/r = 6

j =	0	1	2	3	4	5	6	7	8	9	10	11
z = jd/r =	0	6	12	18	24	30	36	42	48	54	60	66

Say, z1 = 18, z2 = 36, z3 = 54. Is r = 8 or 12?

Question: what if z4 = 30? (a) r=8, (b) r=12. (1min)

How to obtain r from random samples of $j\frac{d}{r}$?

e.g. d=72, r=8, d/r = 9

j =	0	1	2	3	4	5	6	7
z = jd/r =	0	9	18	27	36	45	54	63

e.g. d=72, r=12, d/r = 6

j =	0	1	2	3	4	5	6	7	8	9	10	11
z = jd/r =	0	6	12	18	24	30	36	42	48	54	60	66

Say, z1 = 18, z2 = 36, z3 = 54. Is r = 8 or 12?

Question: what if z4 = 30? (a) r=8, (b) r=12. (1min)

How to tell r=8 from r=12, or to find r EFFICIENTLY?

How to obtain r from random samples of $j\frac{d}{r}$?

e.g. d=72, r=8, d/r = 9

j =	0	1	2	3	4	5	6	7
z = jd/r =	0	9	18	27	36	45	54	63
$\frac{z}{d} = j/r =$	0	$\frac{1}{8}$	$\frac{1}{4}$	$\frac{3}{8}$	$\frac{1}{2}$	$\frac{5}{8}$	$\frac{3}{4}$	$\frac{7}{8}$

e.g. d=72, r=12, d/r = 6

j =	0	1	2	3	4	5	6	7	8	9	10	11
z = jd/r =	0	6	12	18	24	30	36	42	48	54	60	66
$\frac{z}{d} = j/r =$	0	$\frac{1}{12}$	$\frac{1}{6}$	$\frac{1}{4}$	$\frac{1}{3}$	$\frac{5}{12}$	$\frac{1}{2}$	$\frac{7}{12}$	$\frac{2}{3}$	$\frac{3}{4}$	$\frac{5}{6}$	$\frac{11}{12}$

How to obtain r from random samples of $j\frac{d}{r}$?

e.g. d=72, r=8, d/r = 9

j =	0	1	2	3	4	5	6	7
z = jd/r =	0	9	18	27	36	45	54	63
$\frac{z}{d} = j/r =$	0	$\frac{1}{8}$	$\frac{1}{4}$	$\frac{3}{8}$	$\frac{1}{2}$	$\frac{5}{8}$	$\frac{3}{4}$	$\frac{7}{8}$

e.g. d=72, r=12, d/r = 6

j =	0	1	2	3	4	5	6	7	8	9	10	11
z = jd/r =	0	6	12	18	24	30	36	42	48	54	60	66
$\frac{z}{d} = j/r =$	0	$\frac{1}{12}$	$\frac{1}{6}$	$\frac{1}{4}$	$\frac{1}{3}$	$\frac{5}{12}$	$\frac{1}{2}$	$\frac{7}{12}$	$\frac{2}{3}$	$\frac{3}{4}$	$\frac{5}{6}$	$\frac{11}{12}$

Bring z/d = j/r to lowest term, denominator = r/gcd(r,j).
r = some denominators and more often as lcm's of pairs of denominators !! (Proof later ...)

Period finding algorithm: "PF1 for the case $r|d$"

(2) Classical processing:

(a) Repeat quantum subroutine 2t times to get:

$$z_1 = \bar{j}_1 \frac{d}{r}, \quad z_2 = \bar{j}_2 \frac{d}{r}, \quad \ldots, \quad z_{2t} = \bar{j}_{2t} \frac{d}{r}$$

where $\bar{j}_1, \bar{j}_2, \ldots, \bar{j}_{2t}$ are random (and unknown).

Period finding algorithm: "PF1 for the case $r|d$"

(2) Classical processing:

(a) Repeat quantum subroutine 2t times to get:

$$z_1 = \bar{j}_1 \frac{d}{r}, \quad z_2 = \bar{j}_2 \frac{d}{r}, \quad \dots, \quad z_{2t} = \bar{j}_{2t} \frac{d}{r}$$

where $\bar{j}_1, \bar{j}_2, \dots, \bar{j}_{2t}$ are random (and unknown).

(b) For each i : bring to lowest term

$$\frac{z_i}{d} = \frac{\bar{j}_i}{r} = \frac{\bar{j}_i / \gcd(r, \bar{j}_i)}{r / \gcd(r, \bar{j}_i)}$$

Period finding algorithm: "PF1 for the case r|d"

(2) Classical processing:

(a) Repeat quantum subroutine 2t times to get:

$$z_1 = \bar{j}_1 \frac{d}{r}, \quad z_2 = \bar{j}_2 \frac{d}{r}, \quad \ldots, \quad z_{2t} = \bar{j}_{2t} \frac{d}{r}$$

where $\bar{j}_1, \bar{j}_2, \ldots, \bar{j}_{2t}$ are random (and unknown).

(b) For each i : bring to lowest term

$$\frac{z_i}{d} = \frac{\bar{j}_i}{r} = \frac{\bar{j}_i / \gcd(r, \bar{j}_i)}{r / \gcd(r, \bar{j}_i)} \begin{array}{l} \leftarrow n_i \\ \leftarrow d_i \end{array}$$

both ni, di known

both zi, d known

both ji, r unknown

Period finding algorithm: "PF1 for the case r|d"

(2) Classical processing:

(a) Repeat quantum subroutine 2t times to get:

$$z_1 = \bar{j}_1 \frac{d}{r}, \quad z_2 = \bar{j}_2 \frac{d}{r}, \quad \ldots, \quad z_{2t} = \bar{j}_{2t} \frac{d}{r}$$

where $\bar{j}_1, \bar{j}_2, \ldots, \bar{j}_{2t}$ are random (and unknown).

(b) For each i : bring to lowest term

$$\frac{z_i}{d} = \frac{\bar{j}_i}{r} = \frac{j_i / \gcd(r, j_i)}{r / \gcd(r, j_i)} \begin{array}{l} \leftarrow n_i \\ \leftarrow d_i \end{array}$$

both ni, di known

both zi, d known

both ji, r unknown

(c) Let l_i = lcm(d_{2i-1}, d_{2i}) for i = 1,...,t.

Period finding algorithm: "PF1 for the case r|d"

(2) Classical processing:

(a) Repeat quantum subroutine 2t times to get:

$$z_1 = \bar{j}_1 \frac{d}{r}, \quad z_2 = \bar{j}_2 \frac{d}{r}, \quad \ldots, \quad z_{2t} = \bar{j}_{2t} \frac{d}{r}$$

where $\bar{j}_1, \bar{j}_2, \ldots, \bar{j}_{2t}$ are random (and unknown).

(b) For each i : bring to lowest term

$$\frac{z_i}{d} = \frac{\bar{j}_i}{r} = \frac{\bar{j}_i / \gcd(r, \bar{j}_i)}{r / \gcd(r, \bar{j}_i)} \begin{array}{l} \leftarrow n_i \\ \leftarrow d_i \end{array}$$

both ni, di known

both zi, d known

both ji, r unknown

(c) Let $l_i = \mathrm{lcm}(d_{2i-1}, d_{2i})$ for i = 1,...,t.

(d) Output r = max ($l_1, l_2, \ldots, l_t$).

denominators of z1/d = j1/r, z2/d = j2/r

<u>Lemma</u>: if $\gcd(\bar{j}_1, \bar{j}_2) = 1$

then $\operatorname{lcm}\left(\dfrac{r}{\gcd(r, \bar{j}_1)}, \dfrac{r}{\gcd(r, \bar{j}_2)}\right) = r.$

denominators of z1/d = j1/r, z2/d = j2/r

Lemma: if $\gcd(j_1, j_2) = 1$

then $\operatorname{lcm}\left(\dfrac{r}{\gcd(r, j_1)}, \dfrac{r}{\gcd(r, j_2)}\right) = r.$

So, our observation from the example is correct -- some pairs of denominators have lcm = r, when the pair of j's are coprime.

denominators of z1/d = j1/r, z2/d = j2/r

Lemma: if $\gcd(j_1, j_2) = 1$

then $\operatorname{lcm}\left(\dfrac{r}{\gcd(r, j_1)}, \dfrac{r}{\gcd(r, j_2)}\right) = r.$

Reading ex:

Proof: let $g_1 = \gcd(r, j_1)$, $g_2 = \gcd(r, j_2)$

Then $r = \underline{d_1 g_1 = d_2 g_2}$, d_1, d_2 : denominators from the samples

Also $\gcd(j_1, j_2) = 1 \Rightarrow \underline{\gcd(g_1, g_2) = 1}$

$\therefore g_2 \mid d_1$ (math 135) $\therefore d_1 = g_2 a$, $a \in \mathbb{N}$

$\therefore r = g_1 g_2 a$, $d_1 = g_2 a$, $d_2 = g_1 a$, $\therefore \gcd(d_1, d_2) = a$

$$\therefore \operatorname{lcm}(d_1, d_2) = \frac{d_1 d_2}{\gcd(d_1, d_2)} = \frac{g_2 a\, g_1 a}{a} = r$$

$\square$

Period finding algorithm: "PF1 for the case r|d"

(2) Classical processing: proof of correctness

(b) $\frac{\bar{z}_i}{d} = \frac{\bar{j}_i}{r} \approx \frac{\bar{j}_i / \gcd(r, \bar{j}_i)}{r / \gcd(r, \bar{j}_i)}$ $\leftarrow n_i$ $\leftarrow d_i$

(c) Let $l_i = \mathrm{lcm}(d_{2i-1}, d_{2i})$ for i = 1,...,t.

From the lemma, if $\bar{j}_{2i-1}, \bar{j}_{2i}$ coprime, then, $l_i = r$.

How likely are 2 random j's to be coprime?

How likely are 2 random j's to be coprime?

KLM Thm 7.1.12. Let r be a (large) positive integer.
Draw j,k randomly & independently from {0,1,...,r-1}.

$$\text{Prob}(\ \gcd(j,k)=1\ ) \geq \frac{6}{\pi^2} \approx 0.6079\ldots$$

How likely are 2 random j's to be coprime?

KLM Thm 7.1.12. Let r be a (large) positive integer. Draw j,k randomly & independently from {0,1,...,r-1}.

$$\text{Prob}(\gcd(j,k)=1) \geq \frac{6}{\pi^2} \approx 0.6079\ldots$$

Proof: wp $\frac{3}{4}$, not both even

wp $\frac{8}{9}$, not both multiples of 3

wp $\frac{24}{25}$, not both multiples of 5

$\vdots$

wp $1-\frac{1}{p^2}$, not both multiples of p

How likely are 2 random j's to be coprime?

KLM Thm 7.1.12. Let r be a (large) positive integer.
Draw j,k randomly & independently from {0,1,...,r-1}.

$$\text{Prob(gcd(j,k)=1)} \geq \frac{6}{\pi^2} \approx 0.6079\ldots$$

Proof: wp $\frac{3}{4}$, not both even

wp $\frac{8}{9}$, not both multiples of 3

wp $\frac{24}{25}$, not both multiples of 5

$\vdots$

wp $1-\frac{1}{p^2}$, not both multiples of p

$$\text{Prob(gcd(j,k)=1)} = \prod_{\substack{i \\ p_i < r}} \left(1 - \frac{1}{p_i^2}\right)$$ where $p_i = i^{th}$ prime

How likely are 2 random j's to be coprime?

KLM Thm 7.1.12. Let r be a (large) positive integer.
Draw j,k randomly & independently from {0,1,...,r-1}.

$$\text{Prob}(\gcd(j,k)=1) \geq \frac{6}{\pi^2} \approx 0.6079\ldots$$

Proof: wp $\frac{3}{4}$, not both even

wp $\frac{8}{9}$, not both multiples of 3

wp $\frac{24}{25}$, not both multiples of 5

$\vdots$

wp $1-\frac{1}{p^2}$, not both multiples of p

$$\text{Prob}(\gcd(j,k)=1) = \prod_{\substack{i \\ p_i < r}} \left(1-\frac{1}{p_i^2}\right) \quad \text{where } p_i = i^{th} \text{ prime}$$

$$\geq \prod_i \left(1-\frac{1}{p_i^2}\right)$$

How likely are 2 random j's to be coprime?

KLM Thm 7.1.12. Let r be a (large) positive integer. Draw j,k randomly & independently from {0,1,...,r-1}.

$$\text{Prob(gcd(j,k)=1)} \geq \frac{6}{\pi^2} \approx 0.6079\ldots$$

Proof: wp $\frac{3}{4}$, not both even

wp $\frac{8}{9}$, not both multiples of 3

wp $\frac{24}{25}$, not both multiples of 5

$\vdots$

wp $1-\frac{1}{p^2}$, not both multiples of p

$$\text{Prob(gcd(j,k)=1)} = \prod_{\substack{i \\ p_i<r}} \left(1-\frac{1}{p_i^2}\right) \quad \text{where } p_i = i^{th} \text{ prime}$$

$$\geq \prod_i \left(1-\frac{1}{p_i^2}\right) = \prod_i \frac{1}{1+\frac{1}{p_i^2}+\frac{1}{p_i^4}+\ldots}$$

How likely are 2 random j's to be coprime?

KLM Thm 7.1.12. Let r be a (large) positive integer. Draw j,k randomly & independently from {0,1,...,r-1}.

$$\text{Prob}(\ \gcd(j,k)=1\ ) \geq \frac{6}{\pi^2} \approx 0.6079\ldots$$

Proof: wp $\frac{3}{4}$, not both even

wp $\frac{8}{9}$, not both multiples of 3

wp $\frac{24}{25}$, not both multiples of 5

$\vdots$

wp $1-\frac{1}{p^2}$, not both multiples of p

$$\text{Prob}(\ \gcd(j,k)=1\ ) = \prod_{\substack{i \\ p_i < r}} \left(1-\frac{1}{p_i^2}\right) \quad \text{where } p_i = i^{th} \text{ prime}$$

$$\geq \prod_i \left(1-\frac{1}{p_i^2}\right) = \prod_i \frac{1}{1+\frac{1}{p_i^2}+\frac{1}{p_i^4}+\ldots} = \frac{1}{\sum_{n\in\mathbb{N}} \frac{1}{n^2}} = \frac{6}{\pi^2}.$$

Period finding algorithm: "PF1 for the case $r|d$"

(2) Classical processing: proof of correctness

(b) $\dfrac{\bar{z}_i}{d} = \dfrac{\bar{j}_i}{r} = \dfrac{\bar{j}_i / \gcd(r, \bar{j}_i)}{r / \gcd(r, \bar{j}_i)}$ $\begin{array}{l} \leftarrow n_i \\ \leftarrow d_i \end{array}$

(c) Let $\ell_i = \mathrm{lcm}\left(d_{2i-1}, d_{2i}\right)$ for i = 1,...,t.

From the lemma, if $\bar{j}_{2i-1}, \bar{j}_{2i}$ coprime, then, $\ell_i = r$.

From KLM Thm 7.1.12, this happens with prob > 0.6.

Period finding algorithm: "PF1 for the case $r|d$"

(2) Classical processing: proof of correctness

(b) $\frac{z_i}{d} = \frac{\bar{j}_i}{r} = \frac{\bar{j}_i / \gcd(r, \bar{j}_i)}{r / \gcd(r, \bar{j}_i)}$ $\begin{matrix} \leftarrow n_i \\ \leftarrow d_i \end{matrix}$

(c) Let $l_i = \text{lcm}(d_{2i-1}, d_{2i})$ for i = 1,...,t.

From the lemma, if $\bar{j}_{2i-1}, \bar{j}_{2i}$ coprime, then, $l_i = r$.

From KLM Thm 7.1.12, this happens with prob > 0.6.

(d) Output r = max ($l_1, l_2, \ldots, l_t$).

With 2 random samples, prob(get correct r) > 0.6.

Period finding algorithm: "PF1 for the case r|d"

(2) Classical processing: proof of correctness

(b) $\frac{z_i}{d} = \frac{\bar{j}_i}{r} = \frac{\bar{j}_i / \gcd(r, \bar{j}_i)}{r / \gcd(r, \bar{j}_i)}$ $\begin{matrix} \leftarrow n_i \\ \leftarrow d_i \end{matrix}$

(c) Let l_i = lcm (d_{2i-1} , d_{2i}) for i = 1,...,t.

From the lemma, if $\bar{j}_{2i-1}, \bar{j}_{2i}$ coprime, then, $l_i = r$.

From KLM Thm 7.1.12, this happens with prob > 0.6.

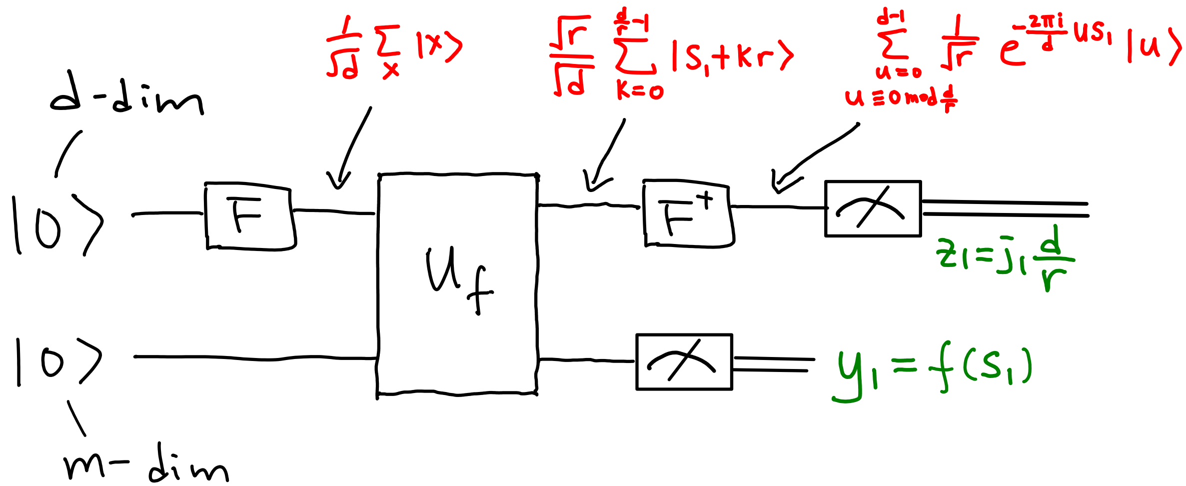
(d) Output r = max ($l_1, l_2, \ldots, l_t$).

With 2 random samples, prob(get correct r) > 0.6.

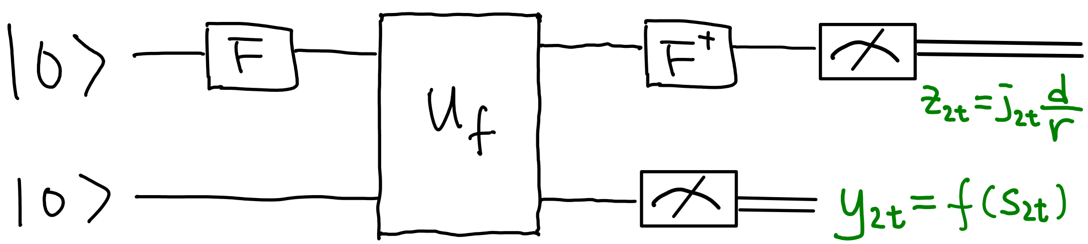
With 2t samples, prob(get correct r) > 1 - 0.4^t

(84%, 93.6% for t=2,3 ...) $\square$

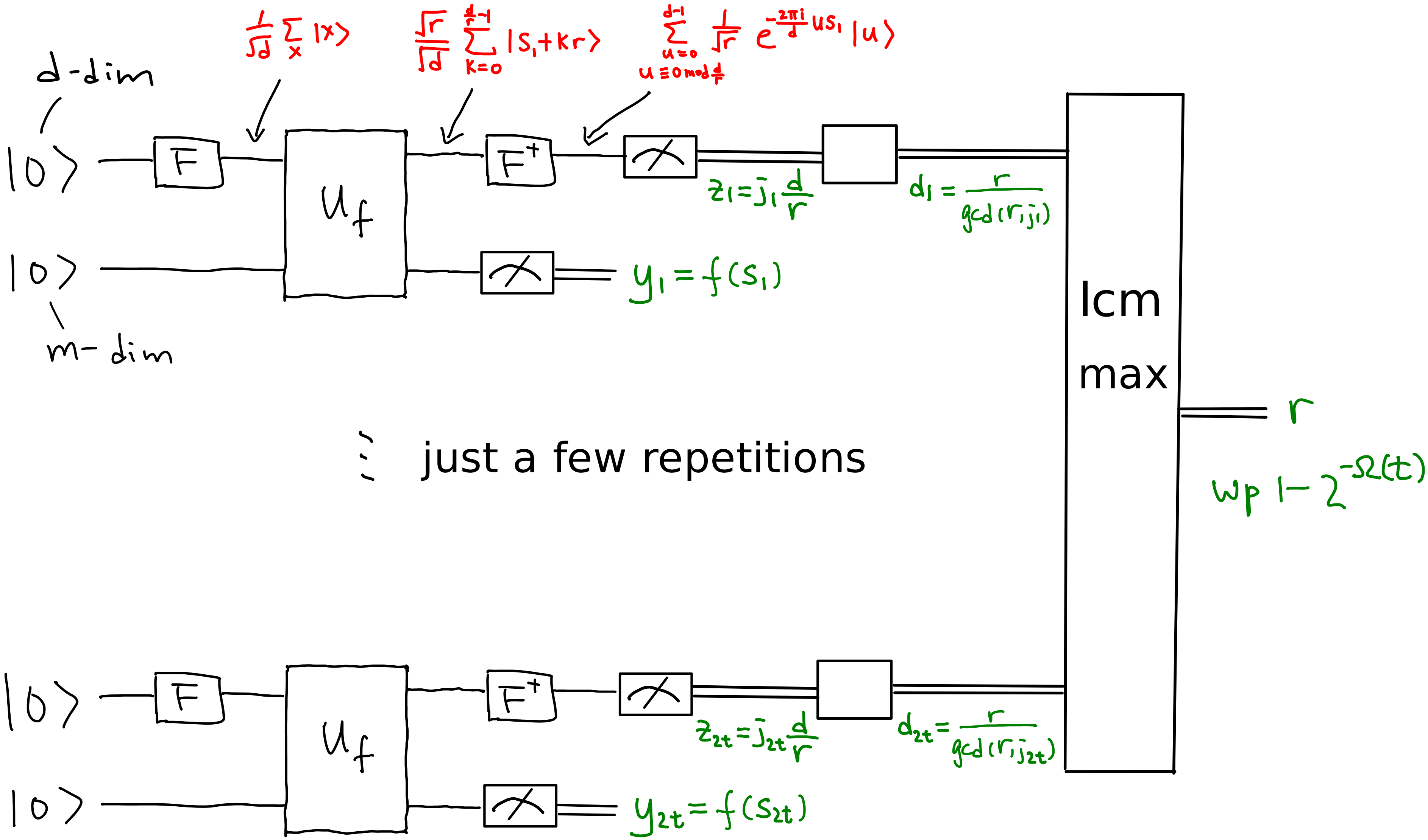
Summary for period finding: "PF1 for the case r|d"



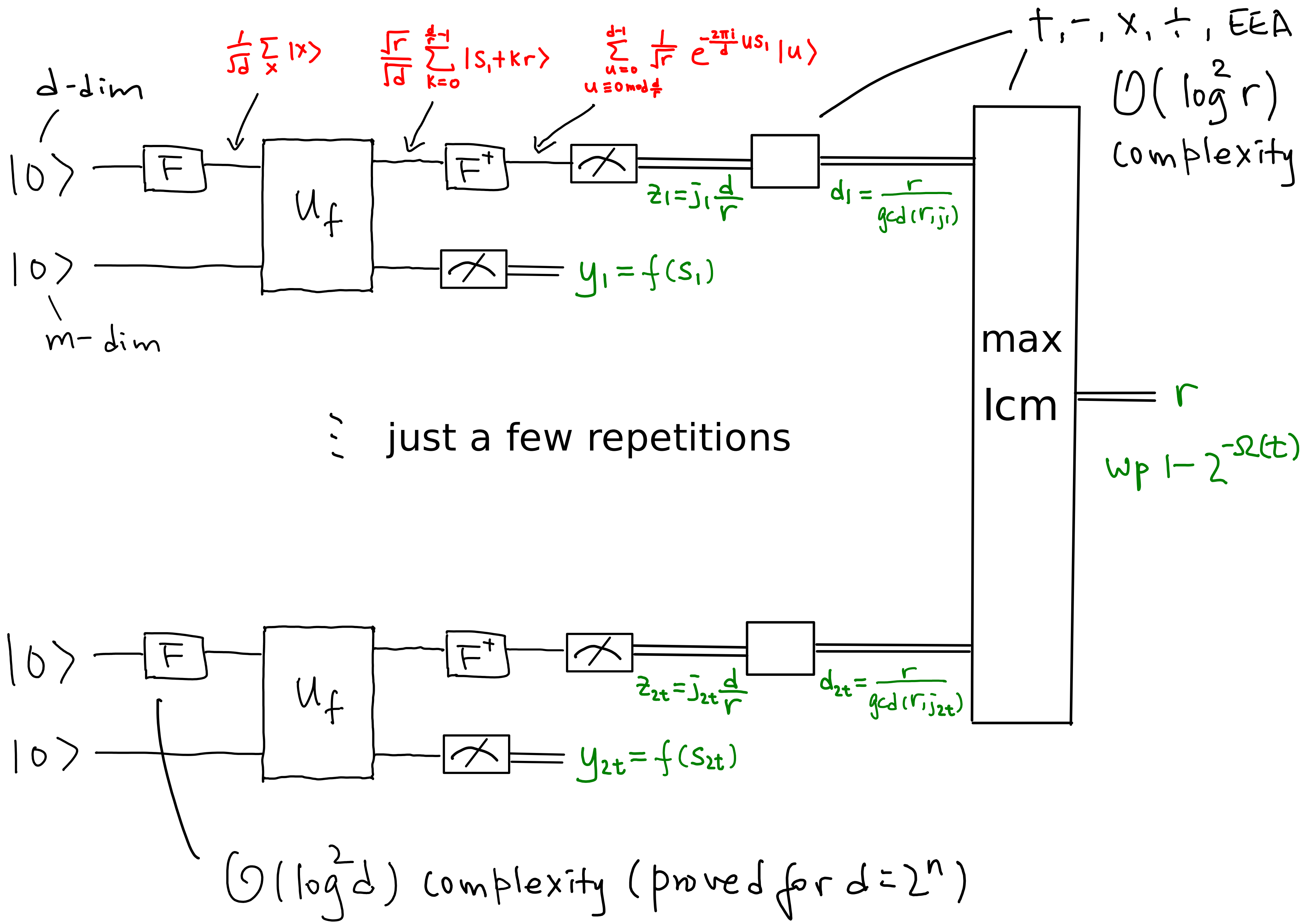
⋮ just a few repetitions



Summary for period finding: "PF1 for the case r|d"



Summary for period finding: "PF1 for the case r|d"



Congrats! We solved the easy case when $r|d$!

Period finding: PF2 real deal

Given: a black box for a function f: $\mathbb{Z} \to \{0,1,..,m-1\}$

Promise: $\exists$ r s.t. f(x) = f(y) iff x $\equiv$ y mod r

Problem: determine r

Period finding: PF2 real deal

Given: a black box for a function f: $\mathbb{Z} \to \{0,1,..,m-1\}$

Promise: $\exists$ r s.t. f(x) = f(y) iff x $\equiv$ y mod r

Problem: determine r

Ideas:

(1) choose d s.t. restricting the domain to {0,..,d-1} preserves desirable features for the r|d case with high accuracy & preserves the complexity.

Period finding: PF2 real deal

Given: a black box for a function f: $\mathbb{Z} \rightarrow \{0,1,..,m-1\}$

Promise: $\exists$ r s.t. f(x) = f(y) iff x $\equiv$ y mod r

Problem: determine r

Ideas:

(1) choose d s.t. restricting the domain to {0,..,d-1} preserves desirable features for the r|d case with high accuracy & preserves the complexity.

(2) additional classical postprocessing to extract r

(3) additional error analysis to ensure correctness

What d makes the function "almost periodic" for all unknown r of interest, when restricting the domain to {0,1,...d-1}?

Intuitively, for d very large compared to any such r. We assume an upper bound on r is known.

What d makes the function "almost periodic" for all unknown r of interest, when restricting the domain to {0,1,...d-1}?

Intuitively, for d very large compared to any such r. We assume an upper bound on r is known.

We choose $d = 2^n$ for an efficient implementation of the QFT over $\mathbb{Z}_d$.

Good values of d will come from the error analysis.

So what goes wrong when $r \nmid d$?

Example: Suppose we know $r \in \{1,2,..7\}$; pick $d = 64$.

$r = 1,2,4$ are special with $r|d$,

$r = 3,5,6,7$ are generic.

So what goes wrong when $r \nmid d$?

Example: Suppose we know $r \in \{1,2,..7\}$; pick $d = 64$.

$r = 1,2,4$ are special with $r|d$,

$r = 3,5,6,7$ are generic.

If $r=5$, possible states after measuring 2nd register:

$$\left(|0\rangle + |5\rangle + |10\rangle + \dots + |55\rangle + |60\rangle\right)\frac{1}{\sqrt{13}}$$

$$\left(|1\rangle + |6\rangle + |11\rangle + \dots + |56\rangle + |61\rangle\right)\frac{1}{\sqrt{13}}$$

$$\vdots$$

$$\left(|3\rangle + |8\rangle + |13\rangle + \dots + |58\rangle + |63\rangle\right)\frac{1}{\sqrt{13}}$$

$$\left(|4\rangle + |9\rangle + |14\rangle + \dots + |59\rangle \qquad \right)\frac{1}{\sqrt{12}}$$

So what goes wrong when $r \nmid d$?

<u>Example</u>: Suppose we know $r \in \{1,2,..7\}$; pick $d = 64$.

$r = 1,2,4$ are special with $r|d$,
$r = 3,5,6,7$ are generic.

If $r=5$, possible states after measuring 2nd register:

$$\left.\begin{matrix}
\left(|0\rangle + |5\rangle + |10\rangle + \dots + |55\rangle + |60\rangle\right)\frac{1}{\sqrt{13}} \\
\left(|1\rangle + |6\rangle + |11\rangle + \dots + |56\rangle + |61\rangle\right)\frac{1}{\sqrt{13}} \\
\vdots \\
\left(|3\rangle + |8\rangle + |13\rangle + \dots + |58\rangle + |63\rangle\right)\frac{1}{\sqrt{13}}
\end{matrix}\right\}$$

meas outcomes are multiples of 13 if we apply QFT for d = 65.

$$\left(|4\rangle + |9\rangle + |14\rangle + \dots + |59\rangle\right)\frac{1}{\sqrt{12}} \; \}$$

meas outcomes are multiples of 12 if we apply QFT for d = 60.

But doing these require knowing
r = 5 and the random shift s!
All we have is d = 64 !

So what goes wrong when $r \nmid d$?

<u>Example</u>: Suppose we know $r \in \{1,2,..7\}$; pick d = 64.

r = 1,2,4 are special with r|d,
r = 3,5,6,7 are generic.

For r=6, possible states after meas 2nd register:

$$\left.\begin{array}{l} \left(|0\rangle + |6\rangle + |12\rangle + \ldots + |54\rangle + |60\rangle\right)\frac{1}{\sqrt{11}} \\ \vdots \\ \left(|3\rangle + |9\rangle + |15\rangle + \ldots + |57\rangle + |63\rangle\right)\frac{1}{\sqrt{11}} \end{array}\right\}$$

wish for QFT for d = 66 here

$$\left.\begin{array}{l} \left(|4\rangle + |10\rangle + |16\rangle + \ldots + |58\rangle\right)\frac{1}{\sqrt{10}} \\ \left(|5\rangle + |11\rangle + |17\rangle + \ldots + |59\rangle\right)\frac{1}{\sqrt{10}} \end{array}\right\}$$

and for d = 60 here

But all we can do is to apply QFT for d=64!
We cannot tailor to r or s that are unknown to us.

Surprise: applying QFT for $d=64$ works well ENOUGH !

In general: after step 3, postmeasurement state is

$$|\psi_{r,s}\rangle = \frac{1}{\sqrt{h}} \sum_{k=0}^{h-1} |s+kr\rangle, \quad h = \left\lfloor \frac{d}{r} \right\rfloor \text{ or } \left\lceil \frac{d}{r} \right\rceil$$ depending on s.

In general: after step 3, postmeasurement state is

$$|\psi_{r,s}\rangle = \frac{1}{\sqrt{h}} \sum_{k=0}^{h-1} |s+kr\rangle, \quad h = \left\lfloor \frac{d}{r} \right\rfloor \text{ or } \left\lceil \frac{d}{r} \right\rceil$$ depending on s.

Inverting the QFT (for the known d):

$$F^{\dagger} |\psi_{r,s}\rangle = \frac{1}{\sqrt{d}} \frac{1}{\sqrt{h}} \sum_{k=0}^{h-1} \sum_{u=0}^{d-1} \sum_{w=0}^{d-1} e^{-\frac{2\pi i}{d} uw} |u\rangle\langle w| s+kr\rangle$$

In general: after step 3, postmeasurement state is

$$|\Psi_{r,s}\rangle = \frac{1}{\sqrt{h}} \sum_{k=0}^{h-1} |s+kr\rangle, \quad h = \left\lfloor \frac{d}{r} \right\rfloor \text{ or } \left\lceil \frac{d}{r} \right\rceil$$ depending on s.

Inverting the QFT (for the known d):

$$F^\dagger |\Psi_{r,s}\rangle = \frac{1}{\sqrt{d}} \frac{1}{\sqrt{h}} \sum_{k=0}^{h-1} \sum_{u=0}^{d-1} \sum_{w=0}^{d-1} e^{-\frac{2\pi i}{d} uw} |u\rangle\langle w | s+kr\rangle$$

$$= \frac{1}{\sqrt{d}} \frac{1}{\sqrt{h}} \sum_{u=0}^{d-1} \sum_{k=0}^{h-1} e^{-\frac{2\pi i}{d} u(s+kr)} |u\rangle$$

$$= \frac{1}{\sqrt{d}} \frac{1}{\sqrt{h}} \sum_{u=0}^{d-1} e^{-\frac{2\pi i}{d} us} \sum_{k=0}^{h-1} \left(e^{-\frac{2\pi i}{d} ur}\right)^k |u\rangle$$

In general: after step 3, postmeasurement state is

$$|\Psi_{r,s}\rangle = \frac{1}{\sqrt{h}} \sum_{k=0}^{h-1} |s+kr\rangle, \quad h = \left\lfloor \frac{d}{r} \right\rfloor \text{ or } \left\lceil \frac{d}{r} \right\rceil$$ depending on s.

Inverting the QFT (for the known d):

$$F^{\dagger}|\Psi_{r,s}\rangle = \frac{1}{\sqrt{d}}\frac{1}{\sqrt{h}} \sum_{k=0}^{h-1} \sum_{u=0}^{d-1} \sum_{w=0}^{d-1} e^{-\frac{2\pi i}{d} uw} |u\rangle\langle w| s+kr\rangle$$

$$= \frac{1}{\sqrt{d}}\frac{1}{\sqrt{h}} \sum_{u=0}^{d-1} \sum_{k=0}^{h-1} e^{-\frac{2\pi i}{d} u(s+kr)} |u\rangle$$

$$= \frac{1}{\sqrt{d}}\frac{1}{\sqrt{h}} \sum_{u=0}^{d-1} e^{-\frac{2\pi i}{d} us} \sum_{k=0}^{h-1} \left(e^{-\frac{2\pi i}{d} ur}\right)^{k} |u\rangle$$

But:

$$\sum_{k=0}^{h-1} \left(e^{-\frac{2\pi i}{d} ur}\right)^{k} = \frac{e^{-2\pi i \frac{ur}{d} h} - 1}{e^{-2\pi i \frac{ur}{d}} - 1} \neq \begin{cases} \frac{d}{r} & \text{if } u = j\frac{d}{r} \\ 0 & \text{otherwise} \end{cases}$$

Instead,

$$\Pr(u) = \frac{1}{dh}\left|\frac{e^{-2\pi i \frac{ur}{d} h}-1}{e^{-2\pi i \frac{ur}{d}}-1}\right|^2$$

for the state after step 4:

$$F^{\dagger}|\Psi_{r,s}\rangle = \frac{1}{\sqrt{d}}\frac{1}{\sqrt{h}}\sum_{u=0}^{d-1} e^{-\frac{2\pi i}{d} us} \sum_{k=0}^{h-1}\left(e^{-\frac{2\pi i}{d} ur}\right)^k |u\rangle$$

$$= \frac{1}{\sqrt{d}}\frac{1}{\sqrt{h}}\sum_{u=0}^{d-1} e^{-\frac{2\pi i}{d} us} \frac{e^{-2\pi i \frac{ur}{d} h}-1}{e^{-2\pi i \frac{ur}{d}}-1} |u\rangle$$

Instead,

$$\Pr(u) = \frac{1}{dh}\left|\frac{e^{-2\pi i \frac{ur}{d}h} - 1}{e^{-2\pi i \frac{ur}{d}} - 1}\right|^2$$

$$= \frac{1}{dh}\left|\frac{e^{-\pi i \frac{ur}{d}h} - e^{+\pi i \frac{ur}{d}h}}{e^{-\pi i \frac{ur}{d}} - e^{+\pi i \frac{ur}{d}}}\right|^2$$

Instead,

$$\Pr(u) = \frac{1}{dh}\left|\frac{e^{-2\pi i \frac{ur}{d}h} - 1}{e^{-2\pi i \frac{ur}{d}} - 1}\right|^2$$

$$= \frac{1}{dh}\left|\frac{e^{-\pi i \frac{ur}{d}h} - e^{+\pi i \frac{ur}{d}h}}{e^{-\pi i \frac{ur}{d}} - e^{+\pi i \frac{ur}{d}}}\right|^2$$

$$= \frac{1}{dh}\,\frac{\sin^2 \pi \frac{ur}{d}h}{\sin^2 \pi \frac{ur}{d}}$$

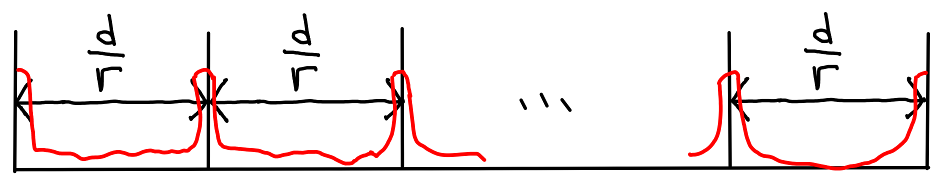
Instead,

$$\Pr(u) = \frac{1}{dh}\left|\frac{e^{-2\pi i \frac{ur}{d}h}-1}{e^{-2\pi i \frac{ur}{d}}-1}\right|^2$$

$$= \frac{1}{dh}\left|\frac{e^{-\pi i \frac{ur}{d}h}-e^{+\pi i \frac{ur}{d}h}}{e^{-\pi i \frac{ur}{d}}-e^{+\pi i \frac{ur}{d}}}\right|^2$$

$$= \frac{1}{dh}\,\frac{\sin^2 \pi \frac{ur}{d}h}{\sin^2 \pi \frac{ur}{d}}$$

tightly peaked at $\frac{jd}{r}$ if $r \ll d$.



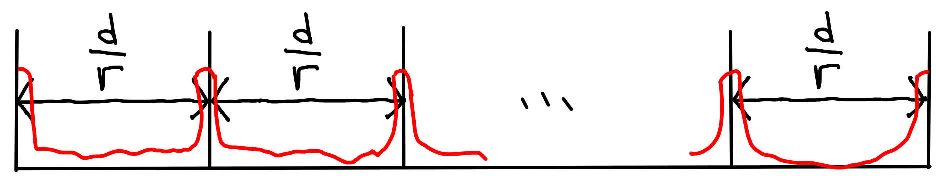
Instead,

$$\Pr(u) = \frac{1}{dh} \left| \frac{e^{-2\pi i \frac{ur}{d} h} - 1}{e^{-2\pi i \frac{ur}{d}} - 1} \right|^2$$

$$= \frac{1}{dh} \left| \frac{e^{-\pi i \frac{ur}{d} h} - e^{+\pi i \frac{ur}{d} h}}{e^{-\pi i \frac{ur}{d}} - e^{+\pi i \frac{ur}{d}}} \right|^2$$

$$= \frac{1}{dh} \frac{\sin^2 \pi \frac{ur}{d} h}{\sin^2 \pi \frac{ur}{d}}$$

tightly peaked at $\frac{jd}{r}$ if $r \ll d$.



Theorem: if an integer u is within 1/2 from $j\frac{d}{r}$

then pr(u) $\geq \frac{4}{\pi^2} \frac{1}{r}$

$\approx$ 0.4, loss relative to r|d case

Theorem: if an integer u is within 1/2 from $j\frac{d}{r}$

then pr(u) $\geq \frac{4}{\pi^2}\frac{1}{r}$

Proof:

Theorem: if an integer u is within 1/2 from $j\frac{d}{r}$

then pr(u) $\geq \frac{4}{\pi^2}\frac{1}{r}$

Proof: if $u = j\frac{d}{r} + \delta$ with $|\delta| \leq \frac{1}{2}$

Theorem: if an integer u is within 1/2 from $\bar{j}\frac{d}{r}$

then pr(u) $\geq \frac{4}{\pi^2}\frac{1}{r}$

Proof: if $u = \bar{j}\frac{d}{r} + \delta$ with $|\delta| \leq \frac{1}{2}$

$$Pr(u) = \frac{1}{dh}\frac{\sin^2 \pi \frac{ur}{d} h}{\sin^2 \pi \frac{ur}{d}} = \frac{1}{dh}\frac{\sin^2 \pi \frac{\delta r}{d} h}{\sin^2 \pi \frac{\delta r}{d}}$$

($\because \pi \bar{j}\frac{d}{r}$ drops out)

Theorem: if an integer u is within 1/2 from $j\frac{d}{r}$

then pr(u) $\geq \frac{4}{\pi^2}\frac{1}{r}$

Proof: if $u = j\frac{d}{r} + \delta$ with $|\delta| \leq \frac{1}{2}$

$$\Pr(u) = \frac{1}{dh}\frac{\sin^2 \pi \frac{ur}{d} h}{\sin^2 \pi \frac{ur}{d}} = \frac{1}{dh}\frac{\sin^2 \pi \frac{\delta r}{d} h}{\sin^2 \pi \frac{\delta r}{d}} \quad (\because \pi j \tfrac{d}{r} \text{ drops out})$$

$$\approx \frac{1}{dh}\frac{\sin^2 \pi \frac{\delta r}{d} h}{(\pi \frac{\delta r}{d})^2} \quad (\because \pi \tfrac{r}{d}\delta \text{ small} \because d \gg r)$$

Theorem: if an integer u is within 1/2 from $j\frac{d}{r}$

then $pr(u) \geq \frac{4}{\pi^2}\frac{1}{r}$

Proof: if $u = j\frac{d}{r} + \delta$ with $|\delta| \leq \frac{1}{2}$

$$Pr(u) = \frac{1}{dh}\frac{\sin^2 \pi \frac{ur}{d} h}{\sin^2 \pi \frac{ur}{d}} = \frac{1}{dh}\frac{\sin^2 \pi \frac{\delta r}{d} h}{\sin^2 \pi \frac{\delta r}{d}}$$ ($\because \pi j \frac{d}{r}$ drops out)

$$\approx \frac{1}{dh}\frac{\sin^2 \pi \frac{\delta r}{d} h}{\left(\pi \frac{\delta r}{d}\right)^2}$$ ($\because \pi \frac{r}{d}\delta$ small $\because d \gg r$)

$$\approx \frac{1}{dh}\frac{\sin^2 \pi \delta}{\left(\pi \frac{\delta r}{d}\right)^2}$$ ($\frac{r}{d}h \approx 1$ if $d \gg r$)

Theorem: if an integer u is within 1/2 from $j\frac{d}{r}$

then pr(u) $\geq \frac{4}{\pi^2}\frac{1}{r}$

Proof: if $u = j\frac{d}{r} + \delta$ with $|\delta| \leq \frac{1}{2}$

$$Pr(u) = \frac{1}{dh}\frac{\sin^2 \pi \frac{ur}{d} h}{\sin^2 \pi \frac{ur}{d}} = \frac{1}{dh}\frac{\sin^2 \pi \frac{\delta r}{d} h}{\sin^2 \pi \frac{\delta r}{d}} \quad (\because \pi j \tfrac{d}{r} \text{ drops out})$$

$$\approx \frac{1}{dh}\frac{\sin^2 \pi \frac{\delta r}{d} h}{(\pi \frac{\delta r}{d})^2} \quad (\because \pi \tfrac{r}{d}\delta \text{ small} \because d \gg r)$$

$$\approx \frac{1}{dh}\frac{\sin^2 \pi \delta}{(\pi \frac{\delta r}{d})^2} \quad (\tfrac{r}{d}h \approx 1 \text{ if } d \gg r)$$

$$\geq \frac{1}{dh}\frac{4\delta^2}{(\pi \frac{r}{d}\delta)^2} \quad \left(\sin\theta \geq \frac{\theta}{\frac{\pi}{2}} \text{ if } 0 \leq \theta \leq \frac{\pi}{2}\right)$$

Theorem: if an integer u is within 1/2 from $j\frac{d}{r}$

then pr(u) $\geq \frac{4}{\pi^2}\frac{1}{r}$

Proof: if $u = j\frac{d}{r} + \delta$ with $|\delta| \leq \frac{1}{2}$

$$\Pr(u) = \frac{1}{dh}\frac{\sin^2 \pi \frac{ur}{d} h}{\sin^2 \pi \frac{ur}{d}} = \frac{1}{dh}\frac{\sin^2 \pi \frac{\delta r}{d} h}{\sin^2 \pi \frac{\delta r}{d}} \quad (\because \pi j \tfrac{d}{r} \text{ drops out})$$

$$\approx \frac{1}{dh}\frac{\sin^2 \pi \frac{\delta r}{d} h}{(\pi \frac{\delta r}{d})^2} \quad (\because \pi \tfrac{r}{d}\delta \text{ small } \because d \gg r)$$

$$\approx \frac{1}{dh}\frac{\sin^2 \pi \delta}{(\pi \frac{\delta r}{d})^2} \quad (\tfrac{r}{d}h \approx 1 \text{ if } d \gg r)$$

$$\geq \frac{1}{dh}\frac{4\delta^2}{(\pi \frac{r}{d}\delta)^2} \quad \left(\sin\theta \geq \frac{\theta}{\frac{\pi}{2}} \text{ if } 0 \leq \theta \leq \frac{\pi}{2}\right)$$

$$= \frac{1}{dh}\frac{d^2}{r}\frac{4}{\pi^2 r} \approx 0.4\frac{1}{r} \quad \left(\because \frac{1}{dh}\frac{d^2}{r} \approx 1\right)$$

If in step 5, measurement outcome z is at most 1/2 from jd/r, how to obtain r?

Divide by d (as in the r|d case): $\left| \frac{z}{d} - \frac{j}{r} \right| \leqslant \frac{1}{2d}$

If in step 5, measurement outcome z is at most 1/2 from jd/r, how to obtain r?

Divide by d (as in the r|d case): $\left| \frac{z}{d} - \frac{j}{r} \right| \leq \frac{1}{2d}$

Claim: If we know $r < N$ and we choose $d \geq N^2$

then $\exists! \frac{j}{r}$ within $\frac{1}{2d}$ from $\frac{z}{d}$

If in step 5, measurement outcome z is at most 1/2 from jd/r, how to obtain r?

Divide by d (as in the r|d case): $\left| \frac{z}{d} - \frac{j}{r} \right| \leqslant \frac{1}{2d}$

Claim: If we know $r < N$ and we choose $d \geqslant N^2$

then $\exists ! \frac{j}{r}$ within $\frac{1}{2d}$ from $\frac{z}{d}$

Proof: for any r, r' < N, any j, j' : $\frac{j}{r} - \frac{j'}{r'} = \frac{r'j - rj'}{rr'}$

If in step 5, measurement outcome z is at most 1/2 from jd/r, how to obtain r?

Divide by d (as in the r|d case): $\left| \frac{z}{d} - \frac{j}{r} \right| \leq \frac{1}{2d}$

Claim: If we know $r < N$ and we choose $d \geq N^2$

then $\exists! \frac{j}{r}$ within $\frac{1}{2d}$ from $\frac{z}{d}$

Proof: for any r, r' < N, any j, j' : $\frac{j}{r} - \frac{j'}{r'} = \frac{r'j - rj'}{rr'}$

$$\left| \frac{j}{r} - \frac{j'}{r'} \right| = \left| \frac{r'j - rj'}{rr'} \right| \geq \left| \frac{1}{rr'} \right| \geq \frac{1}{N^2} \geq \frac{1}{d}$$

Note we only use r, r' < N and no other info on r, r'.

If $\left| \frac{z}{d} - \frac{j}{r} \right| \leqslant \frac{1}{2d}$,

algorithmically, we can obtain j/r from z/d by the continued fraction expansion (CFE):

If $\left| \frac{z}{d} - \frac{j}{r} \right| \leqslant \frac{1}{2d}$,

algorithmically, we can obtain j/r from z/d by the continued fraction expansion (CFE):

If 0<b<1:

$$b = \cfrac{1}{a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots}}}$$

$$\left(\begin{array}{ll} a_0 = \lfloor \frac{1}{b} \rfloor, & b_1 = \frac{1}{b} - a_0 \\ a_1 = \lfloor \frac{1}{b_1} \rfloor, & b_2 = \frac{1}{b_1} - a_1 \\ \vdots & \end{array} \right)$$

If $\left| \frac{z}{d} - \frac{j}{r} \right| \leqslant \frac{1}{2d}$,

algorithmically, we can obtain j/r from z/d by the continued fraction expansion (CFE):

If 0<b<1:

$$b = \cfrac{1}{a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots}}} \qquad \left[\begin{array}{ll} a_0 = \lfloor \frac{1}{b} \rfloor, & b_1 = \frac{1}{b} - a_0 \\ a_1 = \lfloor \frac{1}{b_1} \rfloor, & b_2 = \frac{1}{b_1} - a_1 \\ \vdots & \end{array}\right]$$

To find $\frac{j}{r}$ within $\frac{1}{2d}$ from $\frac{z}{d}$, we can stop the expansion once the approx is within $\frac{1}{2d}$.

Period finding algorithm (PF2),

for unknown r upper bounded by N:

a. Choose $d = 2^n \geqslant N^2$.

Period finding algorithm (PF2),
for unknown r upper bounded by N:

a. Choose $d = 2^n \geqslant N^2$.

b. Repeat quantum subroutine 2t times to get

$z_1, z_2, \ldots, z_{2t}$

From Theorem, an integer u within 1/2 from $j\frac{d}{r}$
has prob > 0.4 / r to be each of the above outcomes.

Period finding algorithm (PF2),
for unknown r upper bounded by N:

a. Choose $d = 2^n \geqslant N^2$.

b. Repeat quantum subroutine 2t times to get

$z_1, z_2, \ldots, z_{2t}$

From Theorem, an integer u within 1/2 from $j\frac{d}{r}$
has prob > 0.4 / r to be each of the above outcomes.

c. For each i, apply CFE to $\frac{z_i}{d}$

Stop when the fraction approx is within 1/2d.

Period finding algorithm (PF2),
for unknown r upper bounded by N:

a. Choose $d = 2^n \geqslant N^2$.

b. Repeat quantum subroutine 2t times to get

$z_1, z_2, \ldots, z_{2t}$

From Theorem, an integer u within 1/2 from $\frac{jd}{r}$
has prob > 0.4 / r to be each of the above outcomes.

c. For each i, apply CFE to $\frac{z_i}{d}$

Stop when the fraction approx is within 1/2d.
Bring fraction to lowest order, call denominator d_i.
Reject suspicious, spurious d_i's from the 2t values.

Period finding algorithm (PF2),

for unknown r upper bounded by N:

a. Choose $d = 2^n \geqslant N^2$.

b. Repeat quantum subroutine 2t times to get

$z_1, z_2, \ldots, z_{2t}$

From Theorem, an integer u within 1/2 from $j\frac{d}{r}$ has prob > 0.4 / r to be each of the above outcomes.

c. For each i, apply CFE to $\frac{z_i}{d}$

Stop when the fraction approx is within 1/2d.

Bring fraction to lowest order, call denominator d_i.

Reject suspicious, spurious d_i's from the 2t values.

d. Let $l_i = \mathrm{lcm}(d_{2i-1}, d_{2i})$ if neither d_{2i-1}, d_{2i} rejected.

Period finding algorithm (PF2),
for unknown r upper bounded by N:

a. Choose $d = 2^n \geqslant N^2$.

b. Repeat quantum subroutine 2t times to get

$$z_1, z_2, \ldots, z_{2t}$$

From Theorem, an integer u within 1/2 from $j\frac{d}{r}$
has prob > 0.4 / r to be each of the above outcomes.

c. For each i, apply CFE to $\frac{z_i}{d}$

Stop when the fraction approx is within 1/2d.
Bring fraction to lowest order, call denominator d_i.
Reject suspicious, spurious d_i's from the 2t values.

d. Let $l_i = \mathrm{lcm}(d_{2i-1}, d_{2i})$ if neither d_{2i-1}, d_{2i} rejected.

e. Output r = max ($l_1, l_2, \ldots, l_t$).

Correctness "proof":

1. 40% of the time, step b gives an outcome z $\bar{c}$ within 1/2 from some jd/r.

Correctness "proof":

1. 40% of the time, step b gives an outcome $\tilde{z}_i$ within 1/2 from some jd/r.

2. with prob > 0.4 * 0.4 * 0.6, both $\tilde{z}_{2i-1}, \tilde{z}_{2i}$ are within 1/2 from some $\tilde{j}_{2i-1} \frac{d}{r}, \tilde{j}_{2i} \frac{d}{r}$ and gcd $(\tilde{j}_{2i-1}, \tilde{j}_{2i})$ = 1.

   If so, lcm $(d_{2i-1}, d_{2i}) = r$.

Correctness "proof":

1. 40% of the time, step b gives an outcome z_i within 1/2 from some jd/r.

2. with prob > 0.4 * 0.4 * 0.6, both z_{2i-1}, z_{2i} are within 1/2 from some $j_{2i-1} \frac{d}{r}, j_{2i} \frac{d}{r}$ and gcd(j_{2i-1}, j_{2i}) = 1.

   If so, lcm$(d_{2i-1}, d_{2i}) = r.$

3. with small constant t, enough of the lcm's will be equal to r (and the spurious cases rejected).

Correctness "proof":

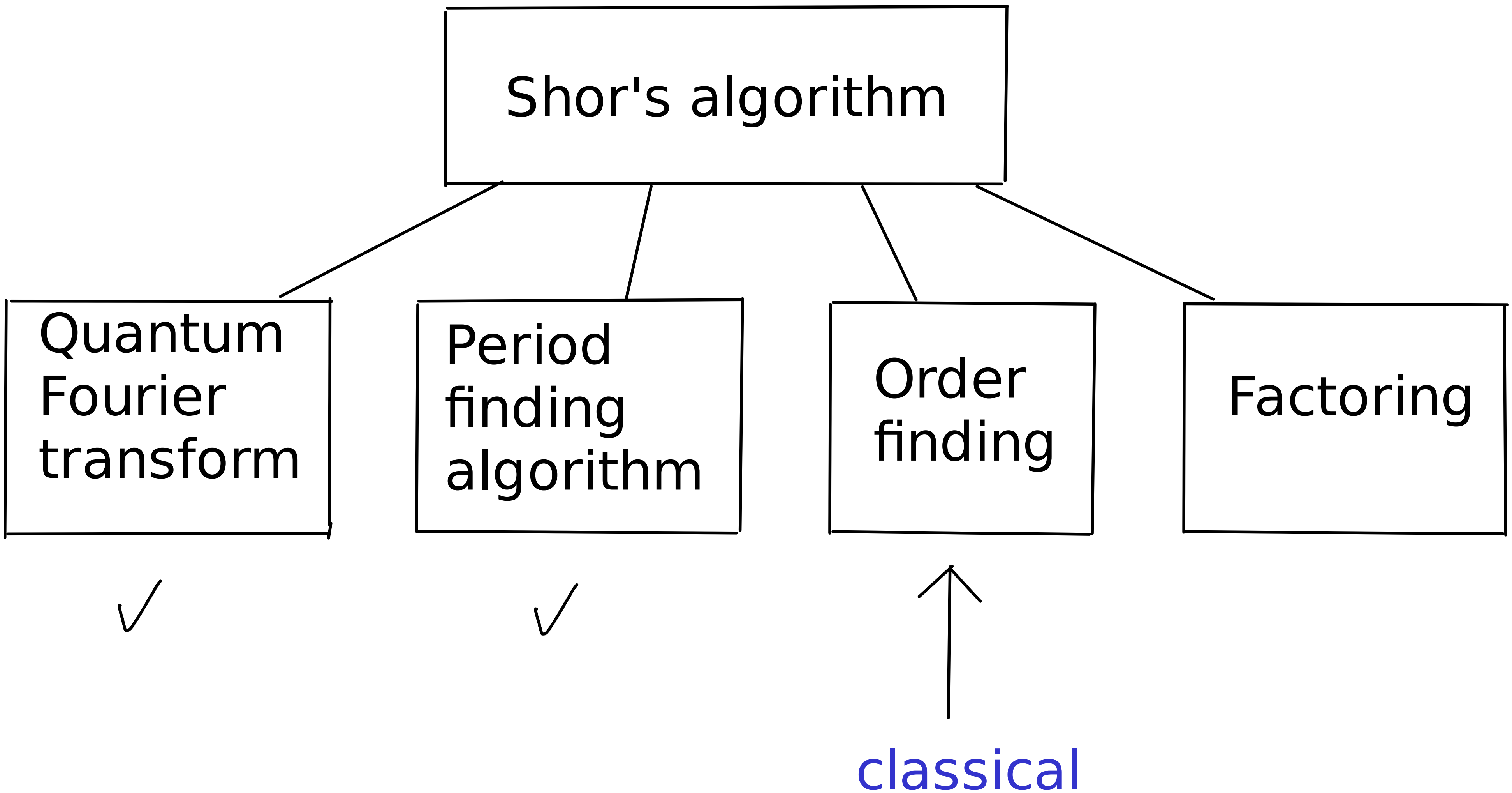
1. 40% of the time, step b gives an outcome z_i within 1/2 from some jd/r.

2. with prob > 0.4 * 0.4 * 0.6, both z_{2i-1}, z_{2i} are within 1/2 from some $\bar{j}_{2i-1}\frac{d}{r}, \bar{j}_{2i}\frac{d}{r}$ and gcd $(\bar{j}_{2i-1}, \bar{j}_{2i})$ = 1.

   If so, lcm $(d_{2i-1}, d_{2i}) = r.$

3. with small constant t, enough of the lcm's will be equal to r (and the spurious cases rejected).

Cost: O(n^2) for QFT, O(n^2) for EEA, O(n^3) for CFE
O(1) queries.



Shor's algorithm
Quantum Fourier transform
Period finding algorithm
Order finding
Factoring
classical

Order finding:

called the order of a (mod N)

Given: a, N $\in \mathbb{N}$.

Problem: determine the smallest r $\in \mathbb{N}$ such that

$$a^r \equiv 1 \mod N$$

Order finding:

Given: a, N $\in \mathbb{N}$.

called the order of a (mod N)

Problem: determine the smallest r $\in \mathbb{N}$ such that

$$a^r \equiv 1 \mod N$$

Note:

(1) This is NOT a black box problem !

(2) No solution unless gcd(N,a)=1.

(Checkable with the EEA in polylog(N) time.)

For example, if a=0 mod N, no solution.

Order finding:

Given: a, N $\in \mathbb{N}$.

Problem: determine the smallest r $\in \mathbb{N}$ such that

$$a^r \equiv 1 \mod N$$

Algorithm:

Let $f(x) = a^x \mod N$.

Order finding:

Given: a, N $\in \mathbb{N}$.

Problem: determine the smallest r $\in \mathbb{N}$ such that

$$a^r \equiv 1 \mod N$$

Algorithm:

Let $f(x) = a^x \mod N$.

f is periodic with period r:

- $f(x+r) = a^{x+r} \mod N = a^x \cdot a^r \mod N = a^x \mod N = f(x)$
- $f(x) = f(y) \Rightarrow a^{x-y} \equiv 1 \mod N \quad \therefore r \mid x-y$

Order finding:

Given: a, N $\in \mathbb{N}$.

Problem: determine the smallest r $\in \mathbb{N}$ such that

$$a^r \equiv 1 \mod N$$

Algorithm:

Let $f(x) = a^x \mod N$.

f is periodic with period r:

- $f(x+r) = a^{x+r} \mod N = a^x \cdot a^r \mod N = a^x \mod N = f(x)$
- $f(x) = f(y) \Rightarrow a^{x-y} \equiv 1 \mod N \quad \therefore r \mid x-y$

We know $r \leq N$.

Apply period finding algorithm PF2 with $d = 2^n \gtrsim N^2$.

One "small" detail:

We have to make our own "blackbox" for the function, and it has to preserve superposition.

One "small" detail:

We have to make our own "blackbox" for the function, and it has to preserve superposition.

The square-and-multiply method gives a fast way to calculate f(x) classically (Math 135):

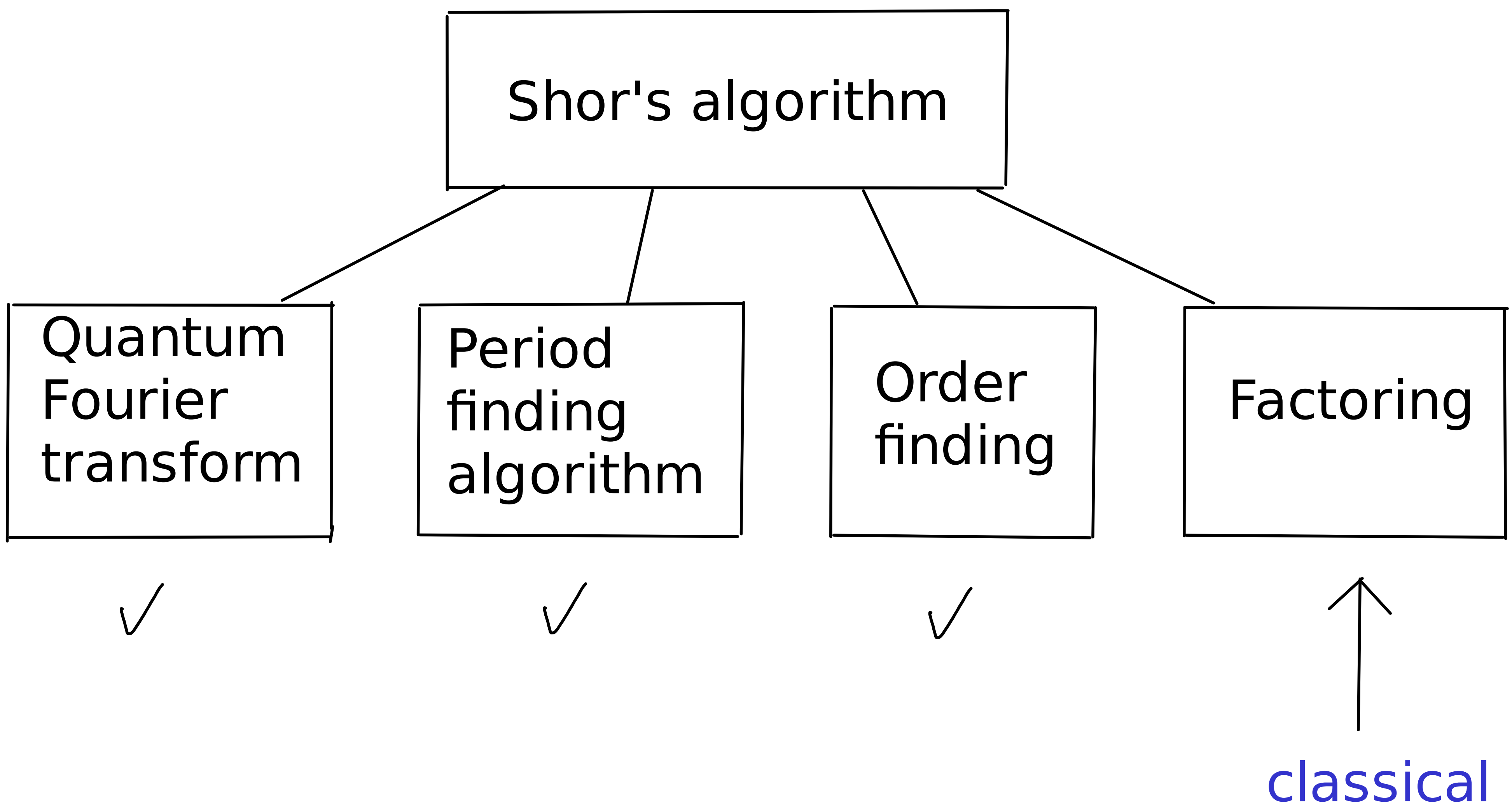
Let $x = x_{n-1} 2^{n-1} + x_{n-2} 2^{n-2} + \cdots + x_1 2 + x_0$

Find

$$a \bmod N \equiv a^{2^0} \bmod N$$
$$a^2 \bmod N \equiv a^{2^1} \bmod N$$
$$a^4 \bmod N \equiv a^{2^2} \bmod N$$
$$\vdots \qquad \vdots$$
$$a^{2^j} \bmod N$$ up to j = n-1

$$a^x \equiv \prod_{j : x_j = 1} a^{2^j} \bmod N$$

Cost : poly(n). Turn reversible & quantum.


Shor's algorithm
Quantum Fourier transform
Period finding algorithm
Order finding
Factoring
classical

Factoring:

Given: $N \in \mathbb{N}$

Problem: find $e_i \in \mathbb{N}$, primes p_i, s.t. $N = \prod_i p_i^{e_i}$.

Factoring:

Given: $N \in \mathbb{N}$

Problem: find $e_i \in \mathbb{N}$, primes p_i, s.t. $N = \prod_i p_i^{e_i}$.

Classical algorithm using order-finding as subroutine:

Preamble:

1. Every time we find a divisor b of N, reduce the problem to factoring N/b.

Factoring:

Given: $N \in \mathbb{N}$

Problem: find $e_i \in \mathbb{N}$, primes p_i, s.t. $N = \prod_i p_i^{e_i}$.

Classical algorithm using order-finding as subroutine:

Preamble:

1. Every time we find a divisor b of N, reduce the problem to factoring N/b.

2. Find all even divisors and reduce to odd N.

Factoring:

Given: N $\in \mathbb{N}$

Problem: find $e_i \in \mathbb{N}$, primes p_i, s.t. $N = \prod_i p_i^{e_i}$.

Classical algorithm using order-finding as subroutine:

Preamble:

1. Every time we find a divisor b of N, reduce the problem to factoring N/b.
2. Find all even divisors and reduce to odd N.
3. Check if N is a prime power.
   (NC Ex 5.17 gives a $\log^3(N)$-sized algorithm.)

Factoring:

Given: $N \in \mathbb{N}$

Problem: find $e_i \in \mathbb{N}$, primes p_i, s.t. $N = \prod_i p_i^{e_i}$.

Classical algorithm using order-finding as subroutine:

Preamble:

1. Every time we find a divisor b of N, reduce the problem to factoring N/b.

2. Find all even divisors and reduce to odd N.

3. Check if N is a prime power.
   (NC Ex 5.17 gives a $\log^3(N)$-sized algorithm.)

4. WLOG, N is odd, with at least 2 prime factors.

Reduction to order finding (Miller 1976):

1. Choose a randomly from {2,3,...,N-2}.

Reduction to order finding (Miller 1976):

1. Choose a randomly from {2,3,...,N-2}.
2. If a, N not coprime, gcd(a,N) is a divisor. Reduce N.

Reduction to order finding (Miller 1976):

1. Choose a randomly from {2,3,...,N-2}.
2. If a, N not coprime, gcd(a,N) is a divisor. Reduce N.
3. WLOG, gcd(a,N)=1. Find the order of a (mod N):

$$a^r \equiv 1 \mod N.$$

$$a^r - 1 \equiv 0 \mod N$$

Reduction to order finding (Miller 1976):

1. Choose a randomly from {2,3,...,N-2}.
2. If a, N not coprime, gcd(a,N) is a divisor. Reduce N.
3. WLOG, gcd(a,N)=1. Find the order of a (mod N):

$$a^r \equiv 1 \mod N.$$
$$a^r - 1 \equiv 0 \mod N$$

4. If r is odd, r is not good, so we return to step 1.

   If r is even, $\left(a^{\frac{r}{2}} - 1\right)\left(a^{\frac{r}{2}} + 1\right) \equiv 0 \mod N$

Reduction to order finding (Miller 1976):

1. Choose a randomly from {2,3,...,N-2}.

2. If a, N not coprime, gcd(a,N) is a divisor. Reduce N.

3. WLOG, gcd(a,N)=1. Find the order of a (mod N):

$$a^r \equiv 1 \mod N.$$

$$a^r - 1 \equiv 0 \mod N$$

4. If r is odd, r is not good, so we return to step 1.

If r is even, $\left(a^{\frac{r}{2}} - 1\right)\left(a^{\frac{r}{2}} + 1\right) \equiv 0 \mod N$

5. Note $a^{\frac{r}{2}} - 1 \not\equiv 0 \mod N$ else r is not the order of a.

Reduction to order finding (Miller 1976):

1. Choose a randomly from {2,3,...,N-2}.
2. If a, N not coprime, gcd(a,N) is a divisor. Reduce N.
3. WLOG, gcd(a,N)=1. Find the order of a (mod N):

$$a^r \equiv 1 \mod N.$$

$$a^r - 1 \equiv 0 \mod N$$

4. If r is odd, r is not good, so we return to step 1.

   If r is even, $(a^{\frac{r}{2}} - 1)(a^{\frac{r}{2}} + 1) \equiv 0 \mod N$

5. Note $a^{\frac{r}{2}} - 1 \not\equiv 0 \mod N$ else r is not the order of a.

   If $a^{\frac{r}{2}} + 1 \equiv 0 \mod N$ a is not good; return to step 1.

6. From 4, $\exists\, b \in \mathbb{N}$ s.t $(a^{\frac{r}{2}} - 1)(a^{\frac{r}{2}} + 1) = bN$

If r is even, $(a^{\frac{r}{2}} - 1)(a^{\frac{r}{2}} + 1) \equiv 0 \mod N$

6. From 4, $\exists\, b \in \mathbb{N}$ s.t. $(a^{\frac{r}{2}}-1)(a^{\frac{r}{2}}+1) = bN$

From 5, neither $a^{\frac{r}{2}}-1$ or $a^{\frac{r}{2}}+1$ is a multiple of N.

Note $a^{\frac{r}{2}}-1 \not\equiv 0 \mod N$ else r is not the order of a.

If $a^{\frac{r}{2}}+1 \equiv 0 \mod N$ a is not good; return to step 1.

6. From 4, $\exists\, b \in \mathbb{N}$ s.t $(a^{\frac{r}{2}}-1)(a^{\frac{r}{2}}+1) = bN$

From 5, neither $a^{\frac{r}{2}}-1$ or $a^{\frac{r}{2}}+1$ is a multiple of N.

Each prime factor in N either divides $a^{\frac{r}{2}}-1$ or $a^{\frac{r}{2}}+1$.

So, one of $\gcd(a^{\frac{r}{2}}-1, N)$, $\gcd(a^{\frac{r}{2}}+1, N)$

is a nontrivial factor of N.

6. From 4, $\exists\, b \in \mathbb{N}$ s.t. $(a^{\frac{r}{2}}-1)(a^{\frac{r}{2}}+1) = bN$

From 5, neither $a^{\frac{r}{2}}-1$ or $a^{\frac{r}{2}}+1$ is a multiple of N.

Each prime factor in N either divides $a^{\frac{r}{2}}-1$ or $a^{\frac{r}{2}}+1$.

So, one of $\gcd(a^{\frac{r}{2}}-1, N)$, $\gcd(a^{\frac{r}{2}}+1, N)$

is a nontrivial factor of N.

It remains to upper bound the probability of failure in steps 4 and 5. It is derived in detail in NC Appendix A4.3, Thm A.4.13. If N has m distinct prime factors, the prob of failure is $\frac{1}{2^m}$.

Cost:

Steps 1-6 give one factor with high probability,
so, O(1) repetitions are sufficient to give a factor.

N has O(log N) factors.
Steps 1-6 are repeated O(log N) times.

Cost:

Steps 1-6 give one factor with high probability,
so, O(1) repetitions are sufficient to give a factor.

N has O(log N) factors.
Steps 1-6 are repeated O(log N) times.

Each repetition requires polylog(N) ($O(\log^3(N))$)
classical pre/post-processing, and one period finding

Cost:

Steps 1-6 give one factor with high probability,
so, O(1) repetitions are sufficient to give a factor.

N has O(log N) factors.
Steps 1-6 are repeated O(log N) times.

Each repetition requires polylog(N) ($O(\log^3(N))$)
classical pre/post-processing, and one period finding
(with similar complexity for the classical computations),
and $O(\log^2(N))$ quantum gates for the QFT.

Not covered in the lectures:

Phase estimation and algorithms based on it.
These are discussed in Chapter 7 of KLM (reading assignment).

Hidden subgroup framework.

Remaining discussions in the lectures:

Cryptographic consequences of quantum algorithms (postponed until after covering search algorithms).