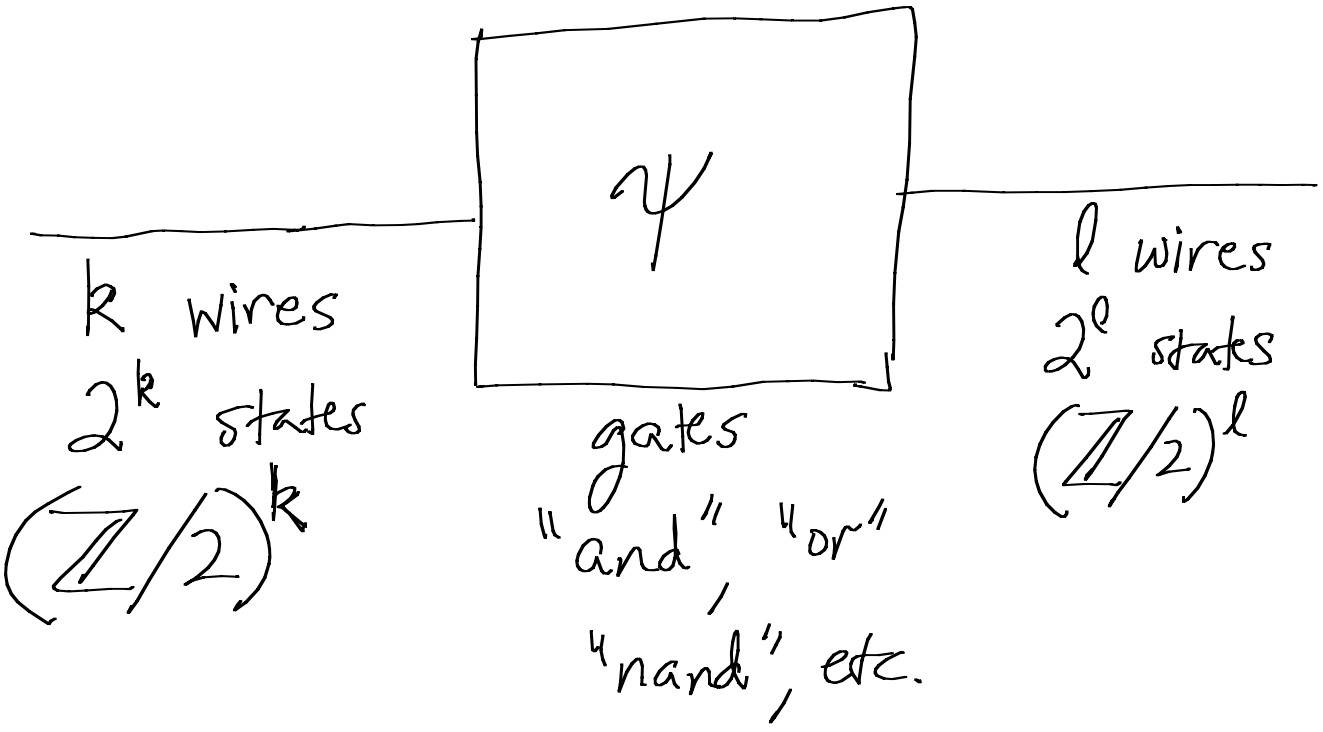
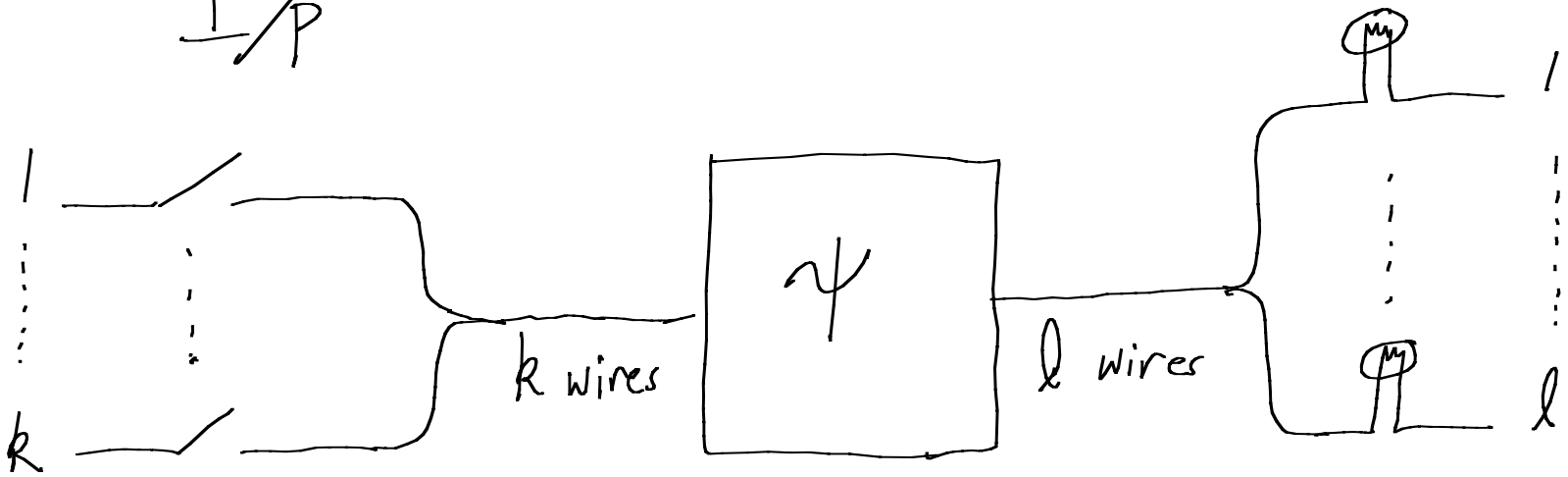
$k, l \geq 1$ integers

$\psi : (\mathbb{Z}/2)^k \longrightarrow (\mathbb{Z}/2)^l$



time to build = complexity of ψ
(ttb) = # gates

I/p



Attatch to I/I and voilá

Disadvantage: 1 i/p at a time

VS = complex vector space

F finite set, e.g., $(\mathbb{Z}/2)^k$

$$\boxed{L^2F} := \{\text{functions } F \to \mathbb{C}\}$$

$$\boxed{\langle \sigma, \tau \rangle} = \sum_{f \in F} \boxed{\sigma(f)}\boxed{\overline{\tau(f)}}$$

$$\boxed{\|\sigma\|} := \sqrt{\langle \sigma, \sigma \rangle}$$

$$\boxed{QF} := \{\sigma \in L^2F \ni \|\sigma\| = 1\}$$

"quantum states"

$\forall \sigma \in L^2F \setminus \{0\}, \quad \boxed{\sigma^N} := \sigma / \|\sigma\| \in QF$

$\forall S \subseteq F, \quad \mathbb{1}_S \in L^2F$ defd by

$$\mathbb{1}_S(f) = \begin{cases} 1 & \text{if } f \in S \\ 0 & \text{if } f \in F \setminus S \end{cases}$$

$\forall f \in F, \quad \boxed{\mathbb{1}_f} := \mathbb{1}_{\{f\}} \in QF$ "pure stak"

Sometimes see "$|f\rangle$"

instead of "$\mathbb{1}_f$"

$\underline{\Phi} : L^2F \longrightarrow L^2F$ is **unitary**

if ① $\underline{\Phi}$ is $\mathbb{C}$-linear

and ② $\forall \sigma \in L^2F$,

$$\|\underline{\Phi}(\sigma)\| = \|\sigma\|$$

$\underline{\Phi} : QF \longrightarrow QF$ **quantum**

if $\exists$ unitary $\underline{\hat{\phi}} : L^2F \longrightarrow L^2F$

$\ni$: $\underline{\hat{\phi}} \,|\, QF = \underline{\Phi}$

$\forall$ bijective $\phi : F \longrightarrow F$,

$\boxed{Q\phi} : QF \longrightarrow QF$

defined by $\sigma \longmapsto \sigma \circ \phi^{-1}$

$Q\phi$ quantum

$\forall f \in F, \quad (Q\phi)(\underline{1}_f) = \underline{1}_{\phi(f)}$

$\Phi : QF \longrightarrow QF$ is $\boxed{\text{classical}}$

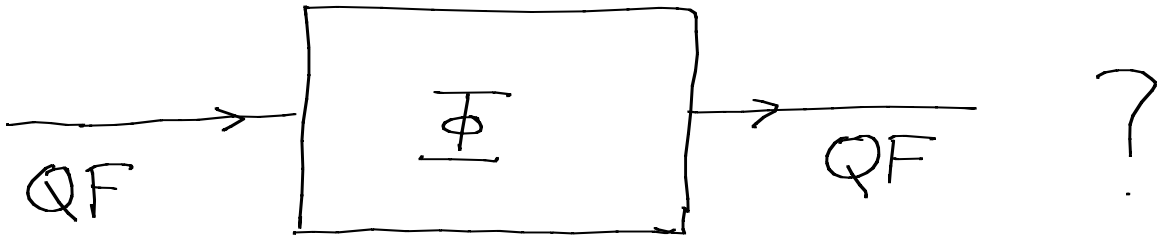
if $\exists$ bijective $\phi : F \longrightarrow F$

$\ni : \Phi = Q\phi$

F finite set, e.g., $(\mathbb{Z}/2)^k$

$\Phi : QF \longrightarrow QF$ quantum

Can we build



Hope: $\forall$ bijective $\phi : F \longrightarrow F$

$\exists$ $\boxed{Q\phi}$ with same ttb as $\boxed{\phi}$

Say we can build $\boxed{Q\phi}$.

Let $f_1, \ldots, f_n$ be the elements of F

Prepare i/p $\left(\mathbb{1}_{f_1} + 2\,\mathbb{1}_{f_2} + \cdots + n\,\mathbb{1}_{f_n}\right)^N \in QF$

o/p : $\left(\mathbb{1}_{\phi(f_1)} + 2\,\mathbb{1}_{\phi(f_2)} + \cdots + n\,\mathbb{1}_{\phi(f_n)}\right)^N$

Note: $Q\phi$ computes $\phi(f_1), \ldots, \phi(f_n)$ simultaneously

e.g. $n = 2^{500}$: Parallel processing on <u>steroids</u>!

Problems : ① Prepare i/p.

② Throughput : design $\boxed{Q\phi}$

③ Read o/p

Note : ③ is intrinsically difficult

Observation of $\sigma \in QF$

results in seeing :

f with probability $|\sigma(f)|^2$

Plan: Explain how to handle non-bijective ϕ

Reduce (1) to "mere" engineering problems

Declare that (2) is a mere engineering problem

Discuss factorization of huge numbers & how to work around (3)

A, B finite sets

$F = A \times B$

$\forall \alpha \in L^2 A, \quad \forall \beta \in L^2 B$

$\boxed{\alpha \otimes \beta} \in L^2 F$ defined by

$$(\alpha \otimes \beta)(a, b) = [\alpha(a)][\beta(b)]$$

$$\|\alpha \otimes \beta\| = \|\alpha\| \cdot \|\beta\|$$

Warning: $\{\alpha \otimes \beta\} \subsetneq L^2 F$

but: $\operatorname{span}\{\alpha \otimes \beta\} = L^2 F$

Fact: $\forall$ quantum

$A : QA \longrightarrow QA$ and

$B : QB \longrightarrow QB$,

$\exists!$ quantum $A \otimes B : QF \longrightarrow QF$

$\ni : (A \otimes B)(\alpha \otimes \beta) =$

$(A\alpha) \otimes (B\beta)$

Hope: $\mathrm{ttb}\,\boxed{A \otimes B} \leq$

$\mathrm{ttb}\,\boxed{A} + \mathrm{ttb}\,\boxed{B}$

$\boxed{\mathcal{H}} : Q(\mathbb{Z}/2) \longrightarrow Q(\mathbb{Z}/2)$

defd by $\underline{1}_0 \longmapsto (\underline{1}_0 + \underline{1}_1)^N$

$\underline{1}_1 \longmapsto (\underline{1}_0 - \underline{1}_1)^N$

nonclassical

Hope: $\mathrm{ttb}\,\boxed{\mathcal{H}} \leq 1$

$\forall$ finite F, $\quad i_F : F \to F$ identity

$$ttb\ \boxed{i_F} = 0$$

$$\partial_F := Q i_F : QF \to QF \quad \text{identity}$$

$$ttb\ \boxed{\partial_F} = 0$$

Hope: $\boxed{O^k}$ — no i/p

o/p = $1_{(0,\ldots,0)} \in Q((\mathbb{Z}/2)^k)$

$ttb \leq k$

Hope = mere engineering problem!

$A := (\mathbb{Z}/2)^k$, $B := (\mathbb{Z}/2)^l$

$\phi : A \longrightarrow B$ not necessarily bijective

---

ttb $\boxed{\phi}$ reasonable

$F := A \times B$

$\psi : F \longrightarrow F$ defd by

$(a, b) \longmapsto (a, (\phi(a)) + b)$

ψ bijective

ttb $\boxed{\psi}$ reasonable

$$\Psi := Q\Psi : QF \longrightarrow QF$$

ttb $\boxed{\Psi}$ reasonable

$$\mathcal{H} : Q(\mathbb{Z}/2) \longrightarrow Q(\mathbb{Z}/2)$$

$$\boxed{\mathcal{H}^k} := \mathcal{H} \otimes \cdots \otimes \mathcal{H} : QA \longrightarrow QA$$

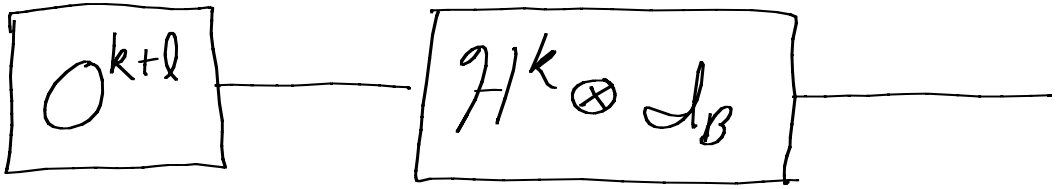
$$\mathcal{I}_B : QB \longrightarrow QB$$

$$\mathcal{H}^k \otimes \mathcal{I}_B : QF \longrightarrow QF$$

---

ttb $\boxed{\mathcal{H}^k \otimes \mathcal{I}_B} \leq k$

Exercise: o/p of



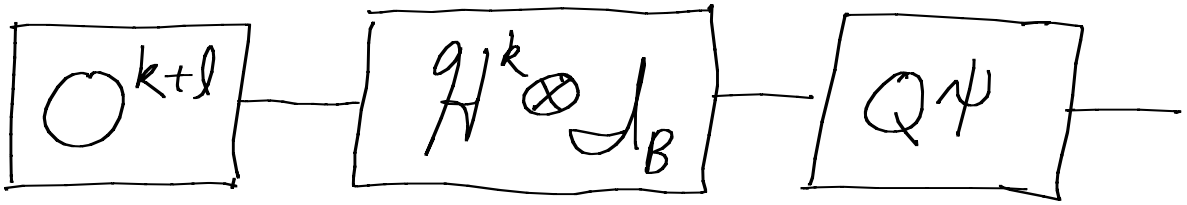
is $\left[\sum_{a \in A} \mathbb{1}_{(a,0)}\right]^N =: \chi$

$$\psi(a,b) = (a, \ (\phi(a)) + b)$$

$$\psi(a,0) = (a, \ \phi(a))$$

$$\therefore (Q\psi)(\chi) = \left[\sum_{a \in A} \mathbb{1}_{(a, \phi(a))}\right]^N$$

$\therefore$ O/p of



is $\left[\sum_{a \in A} \mathbb{1}_{(a, \phi(a))} \right]^N$

Application: Factor huge numbers

$M \geq 1$ integer

$F := \mathbb{Z}/M$

$j \longmapsto \boxed{[j]} : \mathbb{Z} \longrightarrow \mathbb{Z}/M$ canonical

---

$\forall a \in \mathbb{Z}$ $\quad e_{[a]} : F \longrightarrow \mathbb{C}$

defd by $\quad [j] \longmapsto e^{2\pi i j a/M}$

$i = \sqrt{-1}$

$\forall \sigma \in L^2F$, $\boxed{\hat{\sigma}} \in L^2F$ defd by

$$\hat{\sigma}(f) = \langle \sigma, e_f \rangle$$

Fact: $\|\hat{\sigma}\| = \|\sigma\|$

$\sigma \longmapsto \hat{\sigma} : QF \longrightarrow QF$ quantum

---

Fact: $M = qr$, $q, r \geq 1$ ints.

σ is q-periodic $\Longleftrightarrow$ $\hat{\sigma} = 0$ off $[r], [2r], \ldots$

$k \geq 1$ int.

$F := (\mathbb{Z}/2)^k$ $\qquad$ $\tilde{F} := \mathbb{Z}/2^k$

$\alpha : F \longrightarrow \tilde{F}$ defd by

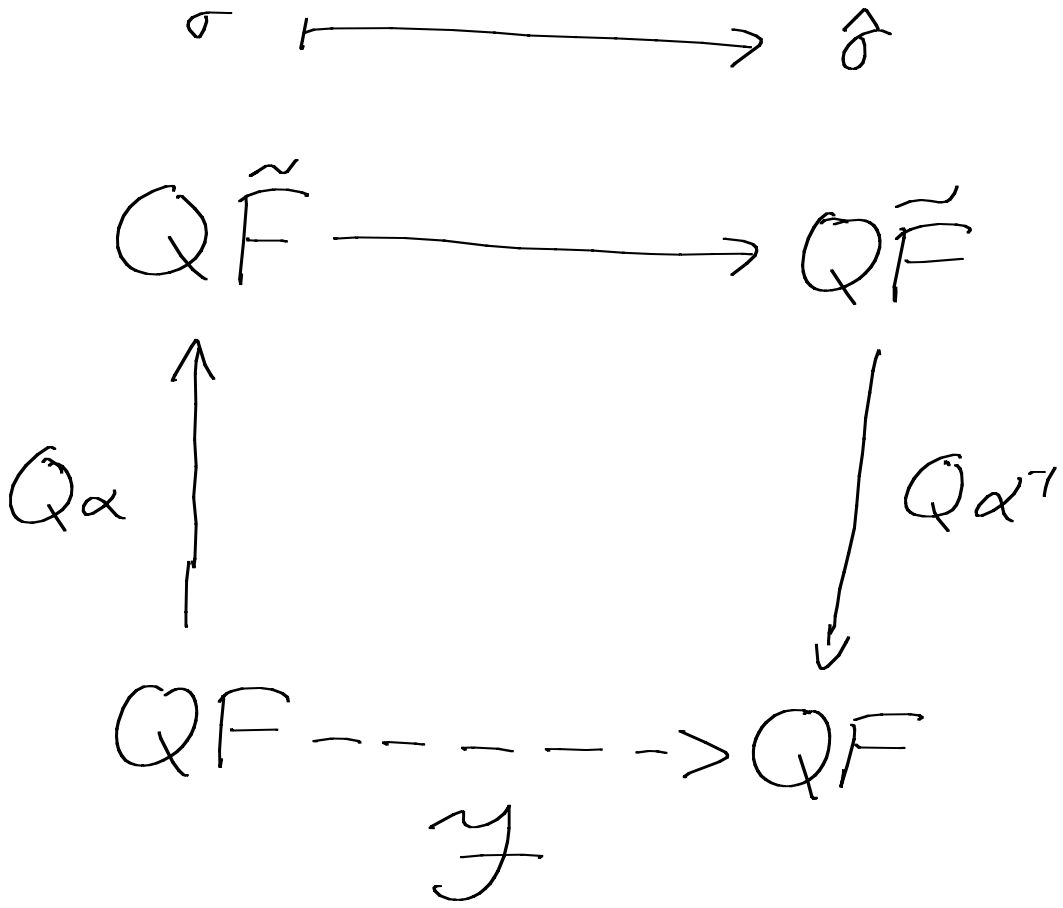
$(b_{k-1}, \dots, b_0) \longmapsto [2^{k-1} b_{k-1} + \cdots + 2b_1 + b_0]$

$\|$

$(b_{k-1} \cdots b_0)_{\text{base two}}$

"bits" 0 or 1

α is bijective



quantum

nonclassical

Coppersmith :

$\exists$ quantum nonclassical

$$R : Q((\mathbb{Z}/2)^2) \longrightarrow Q((\mathbb{Z}/2)^2)$$

$\exists$: if ttb $\boxed{R} \leq 1$

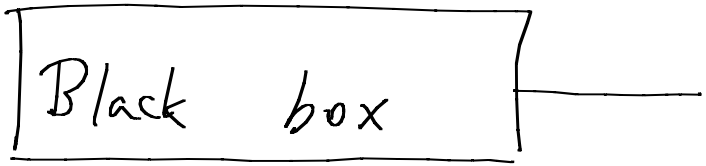
then ttb $\boxed{\mathcal{F}} \leq k^2$

Calculation of period

$$F = (\mathbb{Z}/2)^k$$

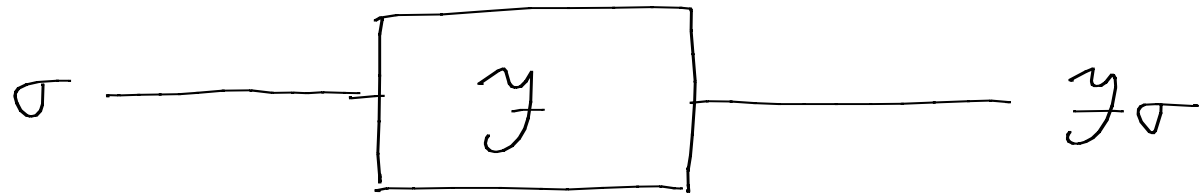
$$M = \#F = 2^k$$

Say we've prepared $\sigma \in QF$



Want: Period q of σ

Want: $r := M/q$



---

y_σ is 0 off $[r], [2r], \ldots, [qr]$ $=$ $[0]$

Fact $|y_\sigma|^2$ const. on $[r], [2r], \ldots, [qr]$

---

100 Observations: $[u_1 r], [u_2 r], \ldots, [u_{100} r]$

$u_1, \ldots, u_{100} \in \{1, \ldots, q\}$ random iid

With very high probability,

$$\gcd(u_1 r, u_2 r, \ldots, u_{100} r) = r$$

Shor's factorization algorithm

$M > 1$ nonprime integer

$M < 10^{500}$

Want: A factor of M in $\{2, \ldots, M-1\}$

Pick $a \in \{2, \ldots, M-1\}$ at random

$\gcd(a, M) \neq 1 \Longrightarrow$ o/p gcd & stop

$[a] \in (\mathbb{Z}/M)^*$:= {multiplicatively invertible elts of $\mathbb{Z}/M$}

---

order of $[a]$ in $(\mathbb{Z}/M)^*$ is

period of $[1], [a], [a^2], \ldots$

which can be computed

---

odd order $\Longrightarrow$ start over

order $= 2v$

$$(a^v+1)(a^v-1) = a^{2v}-1 \equiv 0 \pmod{M}$$

$$M \mid (a^v-1)(a^v+1)$$

$$\gcd(a^v+1, M) \neq 1 \quad \text{or}$$

$$\gcd(a^v-1, M) \neq 1$$

If one of these gcds is in

$$\{2, \ldots, M-1\}$$

o/p it; o.w. start over

Prob of start over $< \frac{1}{2}$.