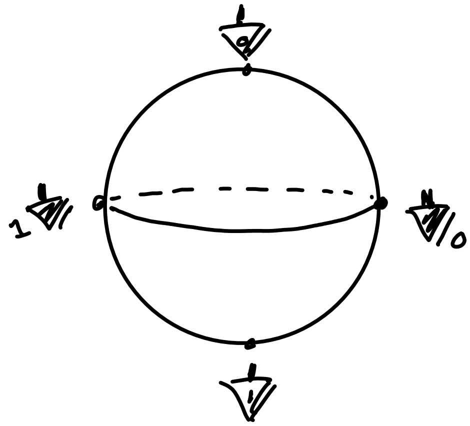
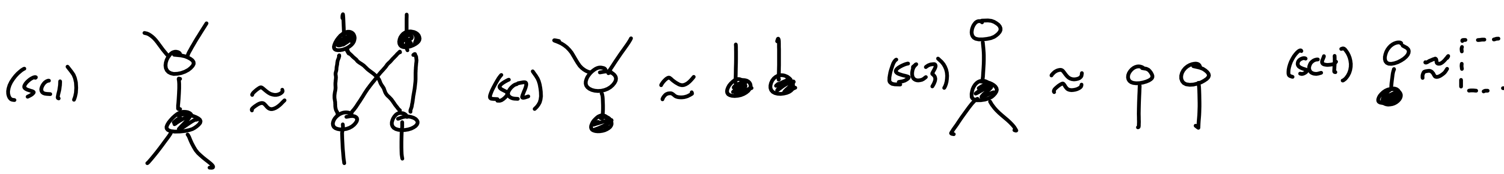
Lecture 18

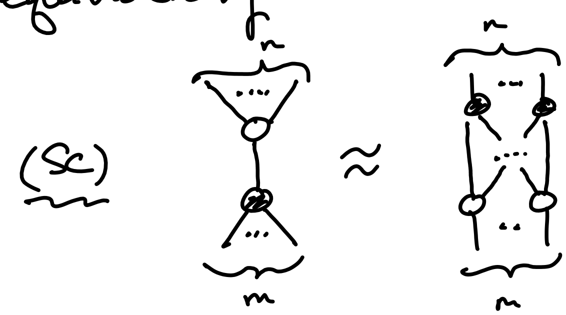


9.3 Strong complementarity.

Def ○ and ● are strongly complementary if:

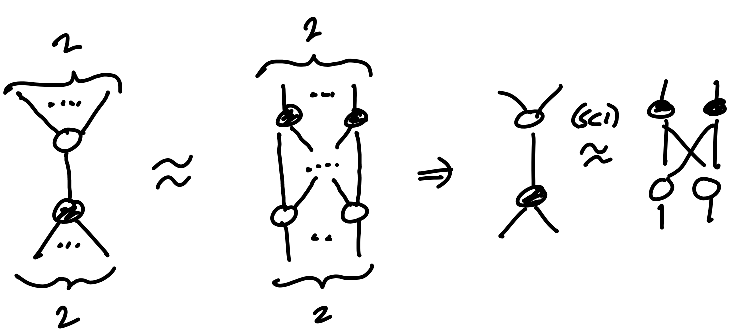


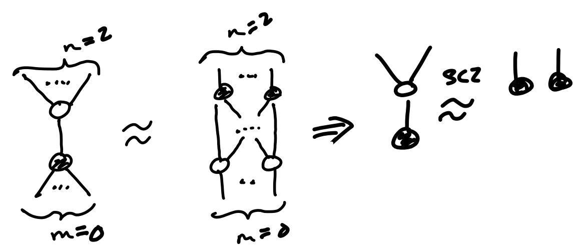
... or equivalently:

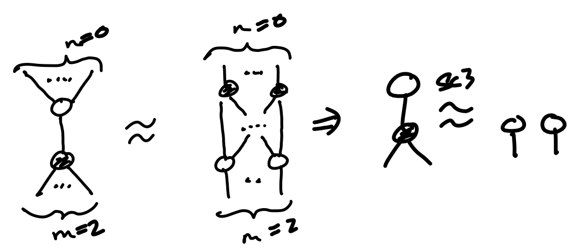


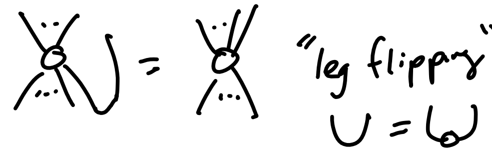
← totally connected
(complete bipartite graph)

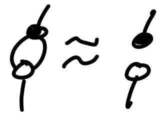
(SC) $\Rightarrow$ (SC1) + (SC2) & (SC3)

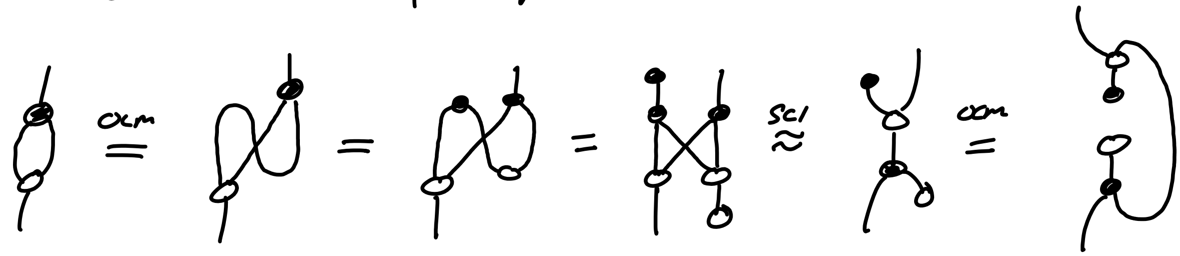


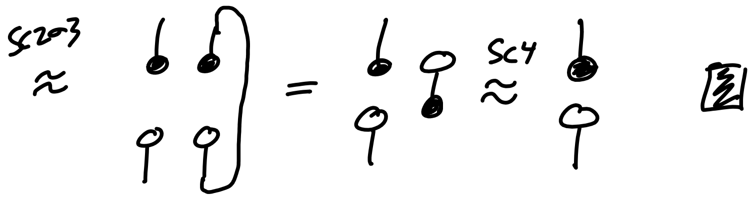




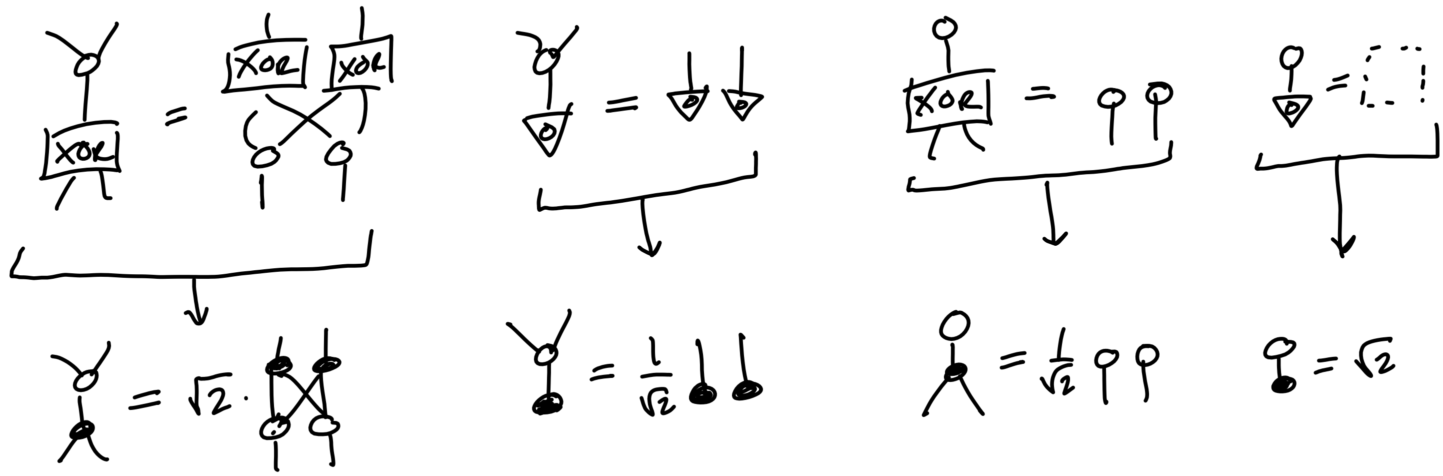


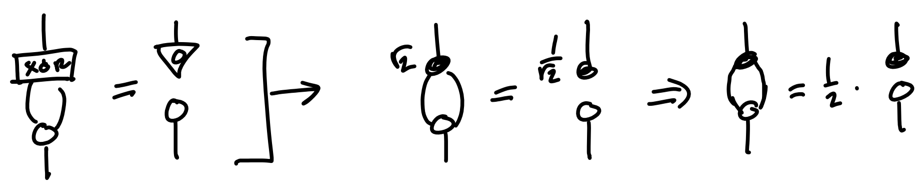
Thm Strong compl. $\Rightarrow$ 

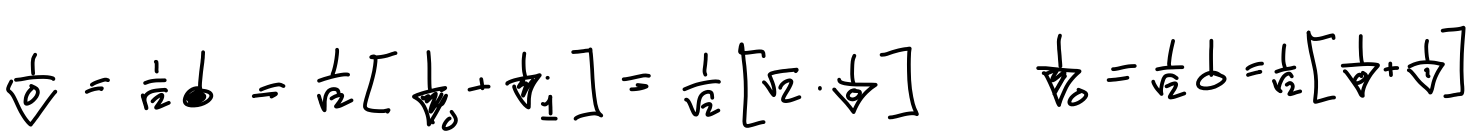
Pf 

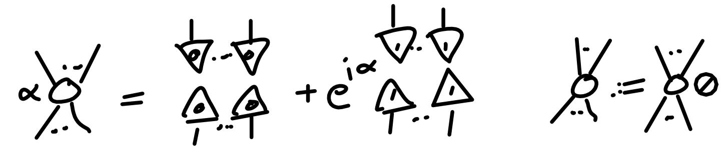


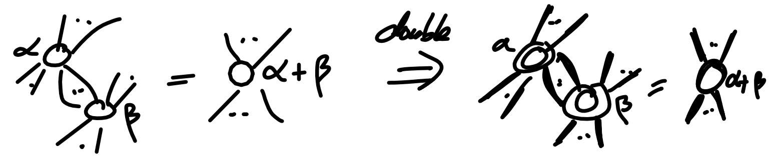
~~The number~~ "ZX" strong complementarity comes from:

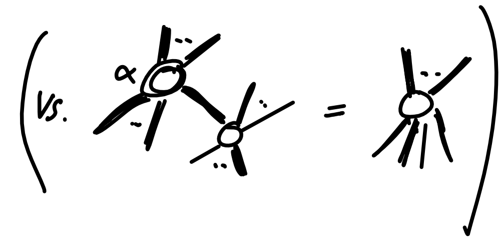


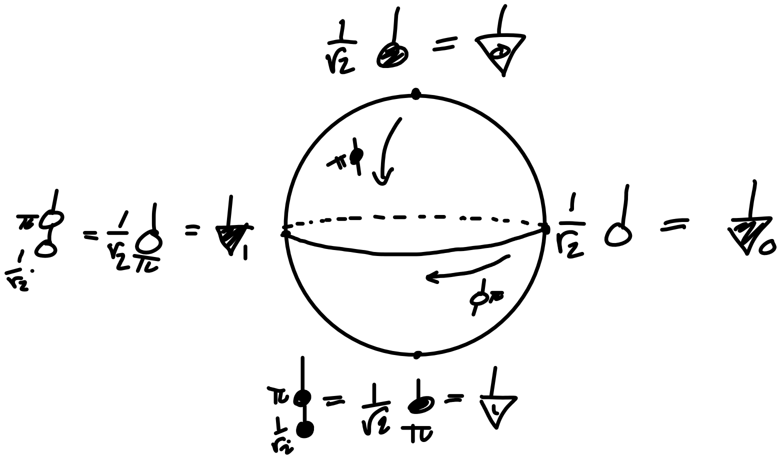
n.b., for complementarity: 

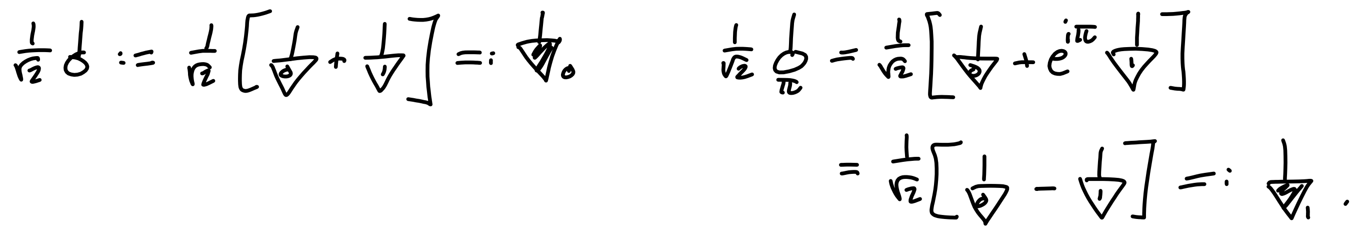


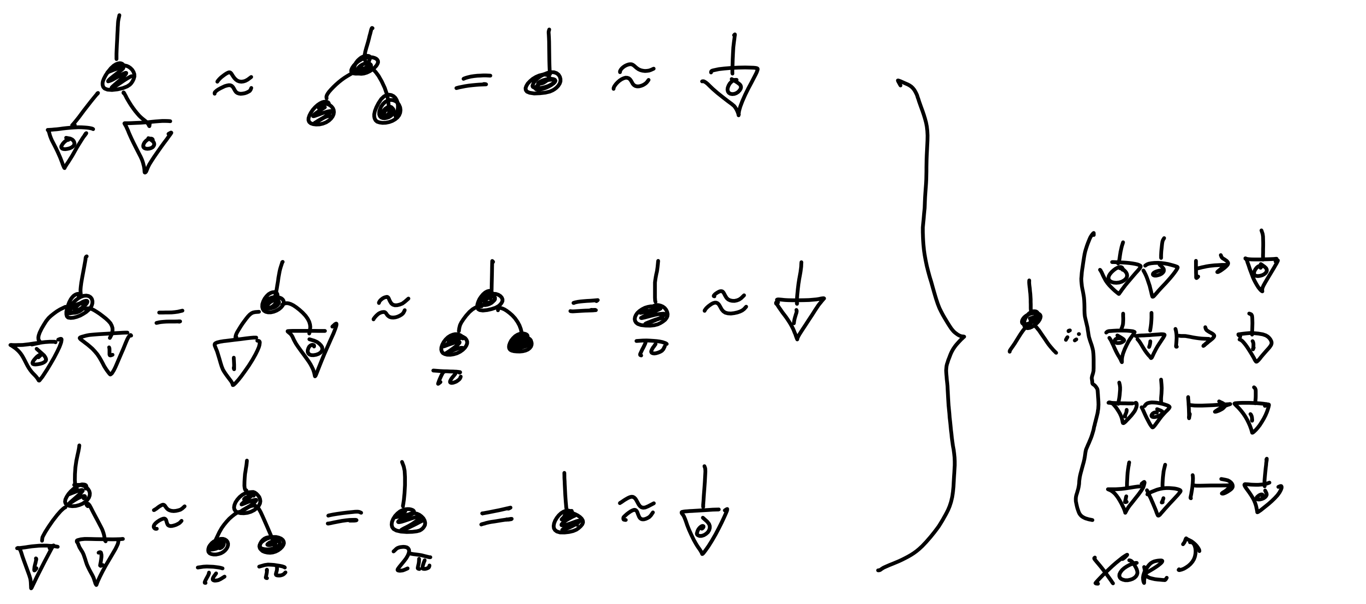






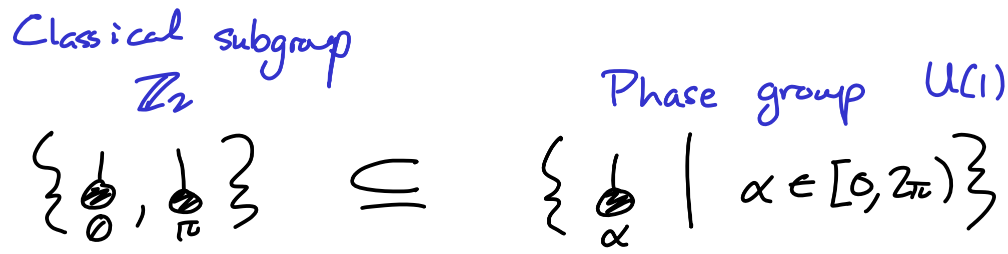




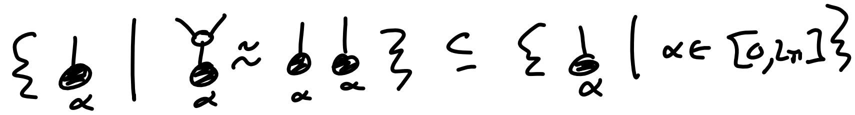


XOR is the group addition for the group $\mathbb{Z}_2$.

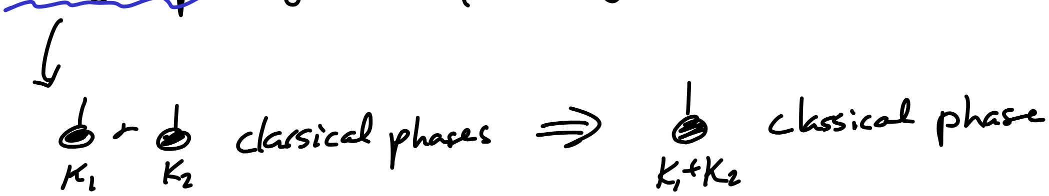
integers modulo 2, "cyclic group" of order 2.



9.76
Thm ○ and ● are strongly complementary iff the classical phases:

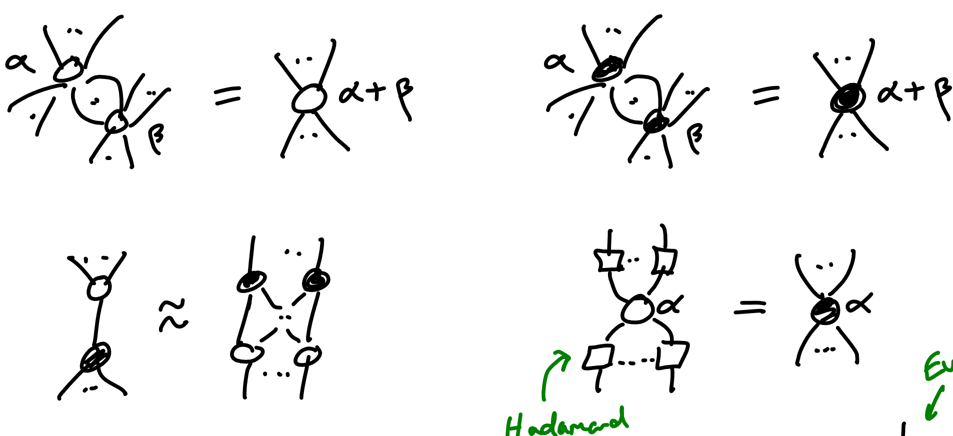


form a subgroup of the phase group.

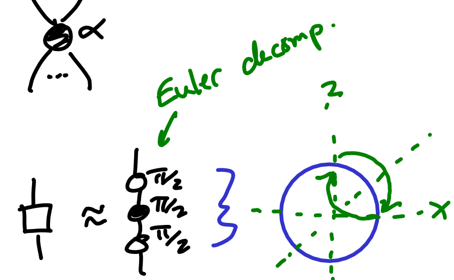


9.4 ZX-calculus := SC + (1 Bloch sphere)

Def The ZX-calculus consists of 4 rules:

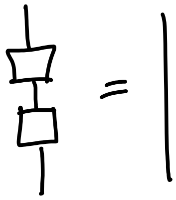


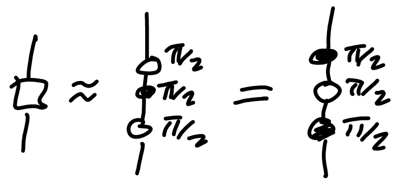
where

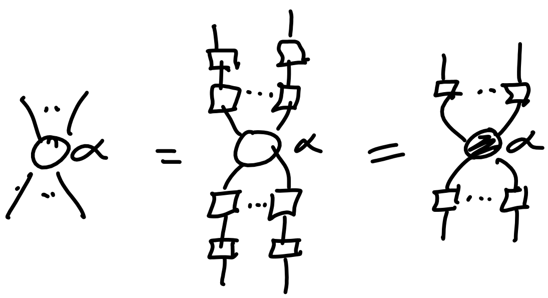


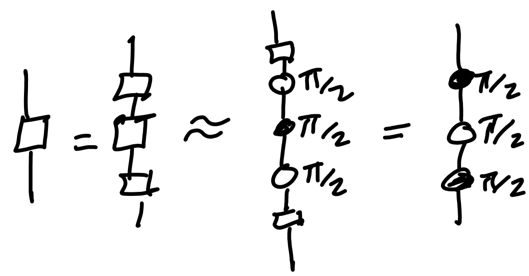
Lecture 19

ZX-rules are colour-symmetric:

ZX-rules ⇒ 

ZX-rules ⇒ 



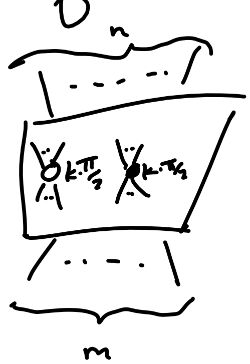


<u>The game</u>: prove as much as possible using just the ZX-rules (and not matrix calculation)

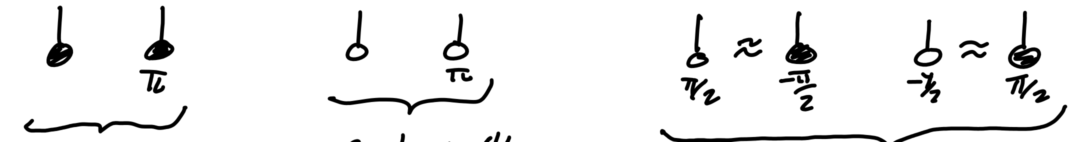
<u>Q</u>: Why? → <u>Efficient</u> Automation
→ Make use of algebraic structures
→ Closer to logic

Stabilizer ZX-diagrams

<u>Def</u> A Clifford ZX-diagram is a ZX-diagram whose phases are integer multiples of $\pi/2$.



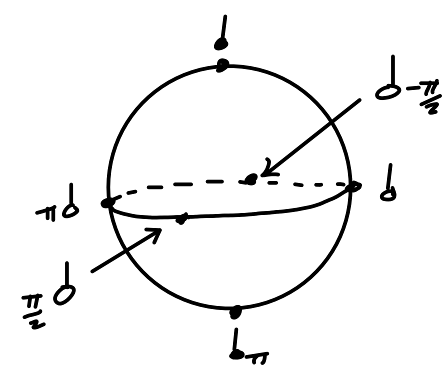
Ex The 1-qubit Clifford ZX-diagrams are all ≈ to one of the following states:



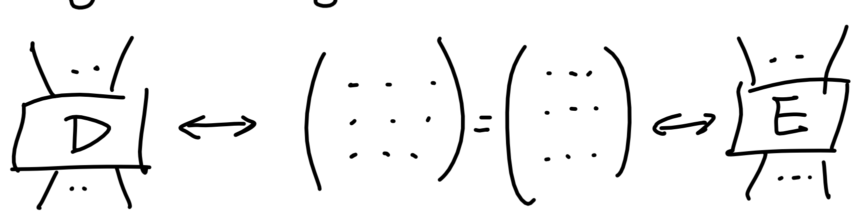
o-basis states
Z-basis states

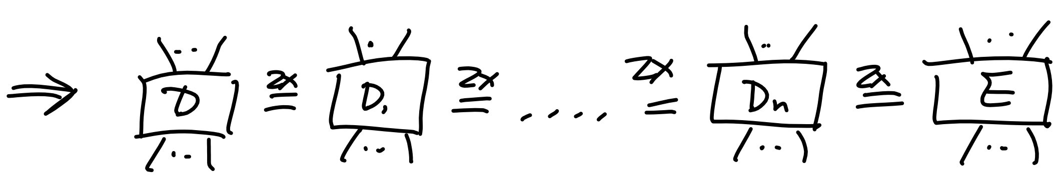
●-basis st's
X-basis st's

Y basis st's



THm The ZX-calculus is complete for Clifford ZX-diagrams, i.e. if two Cl. ZX-diagrams describe the same linear map, we can prove they are equal with the ZX-calculus.

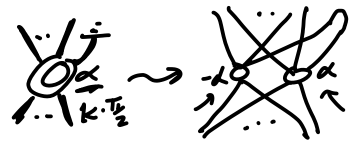




and furthermore, this is efficient! (polynomially many steps)

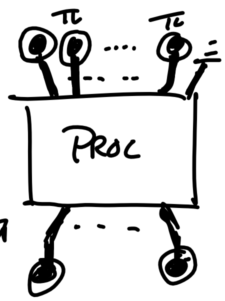
COR Quantum computations involving only Clifford ZX-diags can be efficiently simulated on a classical computer.

...version of the Gottesman-Knill theorem.

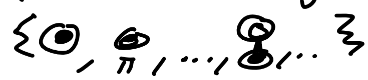


Pf (sketch)

Prob(0101101) :=



= ..... = BASIC ZX-diagram



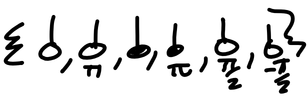
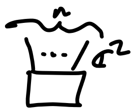
∎

Clifford ZX-diagram

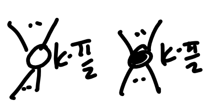
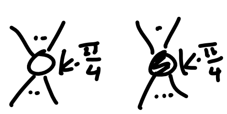
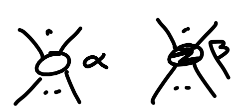
Consequence: Clifford ZX-diagrams are not interesting for q. computation! But! They are still interesting because:

* most q. crypto uses Cliffords
* most q. non-locality experiments use Cliffords
* most q. error correction uses Cliffords
* ,....

Scale (Clifford ZX-diagrams vs. their matrices)

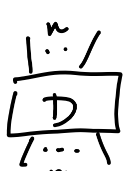
	MATRICES	Clifford ZX-diagrams
SINGLE QUBIT : 	2D	$\approx$ single spider $\in$ 
N QUBITS ; 	2^nD vector	$\approx O(n^2)$ spiders in it.
$n=20$	$\sim 10^6$ dim'l	~ 400 spiders

(Q-calculus $\rightarrow$  + all 1-qubit unitaries, given as quaternions)

finite, discrete, classical		discrete		
{Clifford ZX-diagrams}	$\subseteq$	{Clifford+T ZX-diagrams}	$\subseteq$	{all ZX-diagrams}
				 $\alpha, \beta \in [0, 2\pi)$

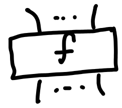
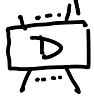
THM ZX-diagrams are universal:

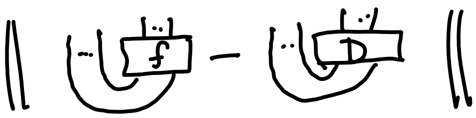
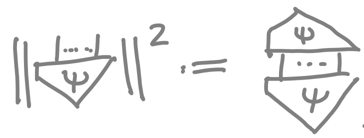
$\forall M$ $2^n \times 2^m$ matrices. $\exists$ ZX-diagram D s.t.

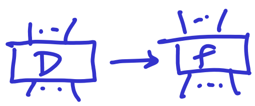
 $\longleftrightarrow M$

($\Rightarrow$ any q.map can be expressed as a ZX-diagram)

Thm Clifford + T ZX-diagrams are approx. universal.

For any linear map  and $\varepsilon > 0$, there exists a Clifford+T ZX-diagram  such that:

 $< \varepsilon$. [recall: ]

n.b. as $\varepsilon \to 0$,  .

$\Rightarrow$ Clifford + T diagrams can approximate any linear map (and hence any quantum map) to any precision we like.

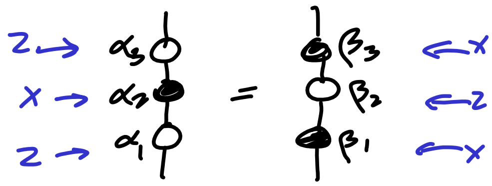
Lecture 20

After PQP was published, 2 stronger completeness theorems were shown for extensions of the ZX-calculus.

Thm (JPV 2017) The extended ZX-calculus is complete for Clifford + T diagams. arXiv: 1705.11151 *

Thm (Wang, Ng) The universal ZX-calculus is complete for all ZX-diagrams. arXiv: 1706.09877 *

Vilmart [2018] showed that the 4 basic ZX-rules +



$\beta_i = f_i(\alpha_1, \alpha_2, \alpha_3)$ ← big trig function

are complete for all ZX-diagrams. arXiv: 1812.09114*

* Google these arXiv numbers if you want to see the original papers with the rules.

Quantum computation

(covered in lecture: 12.1 intro, 12.1.1, 12.2 intro, & 12.2.1)

Models →
- quantum Turing machines [Deutch 1985]
- quantum circuit model [Deutch 1989]
  ← solid state (supercond, ion traps)
- measurement-based QC
  ← photonics
- topological
- adiabatic QC*
  e.g. D-Wave

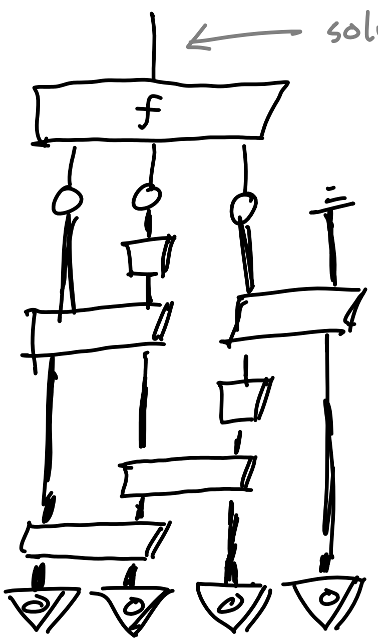
Computations in the q. circuit model consist of:

4. classical post-processing →

3. measure in Z-basis →

2. apply unitary gates →

1. preparation →



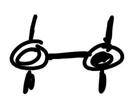
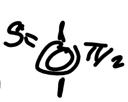
← solution.

OUTCOMES encode solution

CIRCUIT encodes the problem

The set of gates $\mathcal{G}$ is fixed in advance (e.g. by the hardware.)

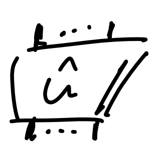
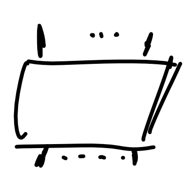
e.g.

{ CNOT := , H := , S =  } ← Clifford

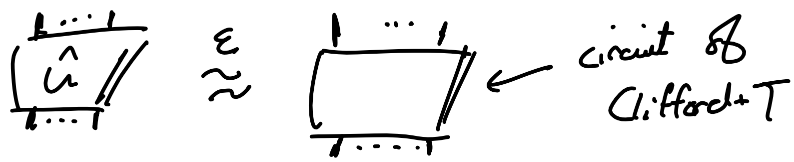
{ " , " , T =  } ← Clifford+T

{ " , " ,  } ← Clifford+phase

Thm Any unitary can be built from Clifford+phase gates, exactly.

 =  ← circuit of Clifford+phase.

Thm Any unitary can be approx'd from Clifford+T gates, for any ε.



Q: What kinds of problems can we solve w/ Q.C.?

(obvious) A: "What does $\hat{U}$ do to $\hat{\psi}$?"

exponentially big.

Applications: simulating physical q. processes.

condensed matter

quantum chemistry

Q: Can it solve <u>classical</u> problems faster?

Suppose I want to know some global property about a classical function:

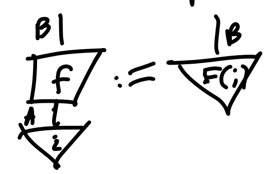
$$F : \{0,1\}^N \to \{0,1\}$$

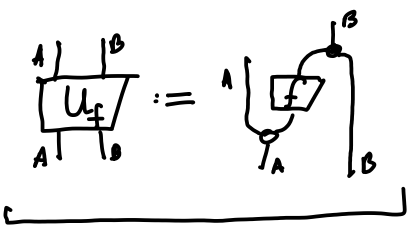
e.g. <u>PROBLEM</u> SAT

given F as a logical formula, does there exist <u>any</u> bitstring s.t. $F(\vec{b}) = 1$?

Step 1: Define a quantum oracle.

function F ⇝ linear map f ⟶ unitary U_f (q. oracle)

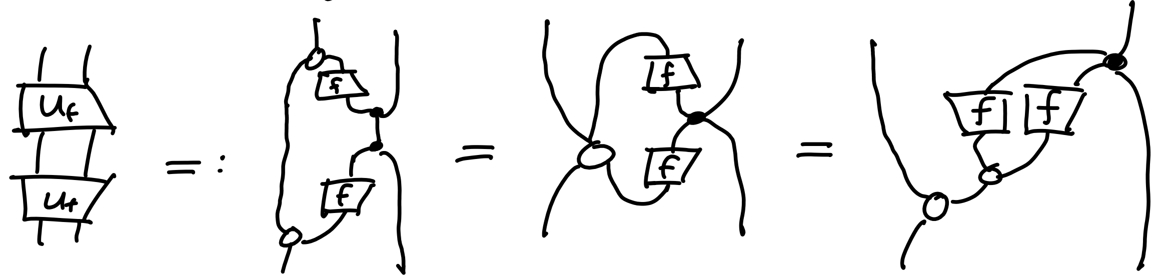


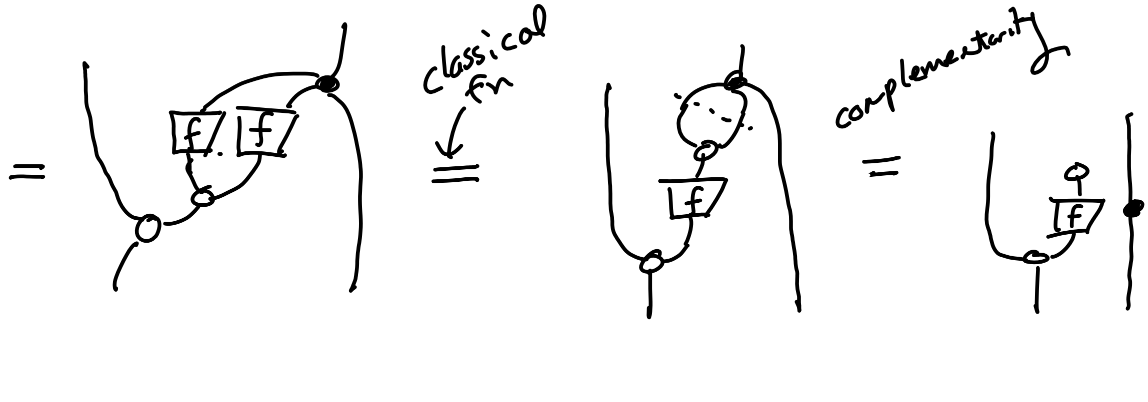


always unitary.

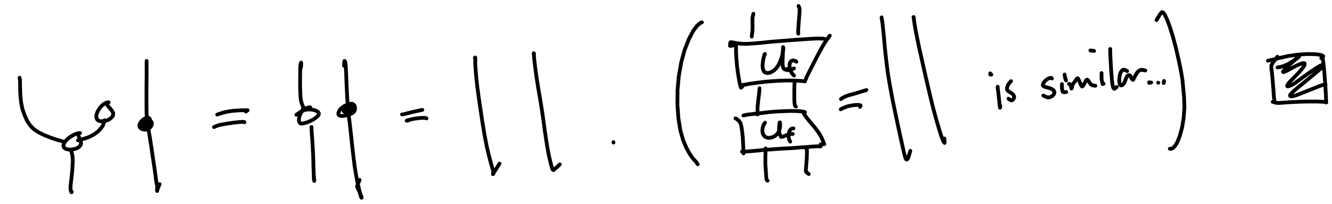
Thm U_f is unitary for a classical fn f.

Pf



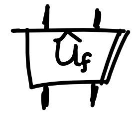


causality f =

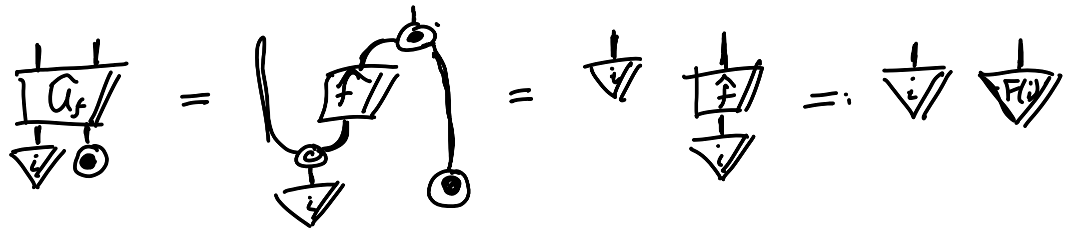


∎

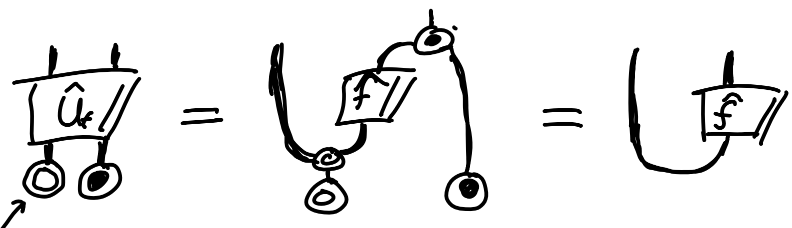
Lecture 21

Q: What can I do with  ?

A1: We can:



A2: More interesting:



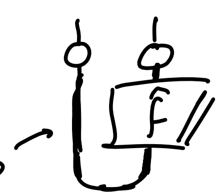
double($\sum_i$ i)

q. state that "knows everything" about f.

($\cong$ to f under map-state duality).

THE CATCH: to get info, we need to measure.

e.g. a bad choice of measurement:



D

gives outcome $(i, F(i))$ with prob: $\frac{1}{D}$.

... equivalently, we could pick i at random and compute $F(i)$.

$\Rightarrow$ we should choose measurements carefully.

~~$\forall i.\ (F(i)=0$ or $F(i)=1)$~~

PROBLEM: Deutsch-Jozsa problem:

Given a function F which is either
- constant → $(\forall i.\ F(i)=0)$ or $(\forall i.\ F(i)=1)$

) OR

- balanced → $\#\{i \mid F(i)=0\} = \#\{i \mid F(i)=1\}$

$F: \underbrace{\{0,1\}^N}_{2^N \text{ elems.}} \to \{0,1\}$

Decide: Is F constant or balanced?

Classically:

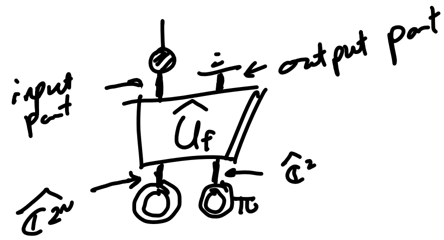
Q: How many times do I need to run F to solve D-J?

A: $\frac{2^N}{2}+1$ ← more than half of $\{0,1\}^N$ in the worst case.

Quantumly:

A: 1 (!)

Algorithm:

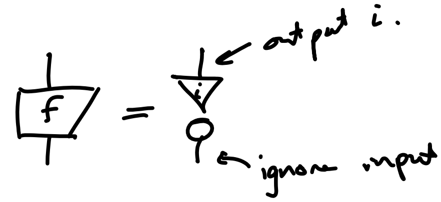


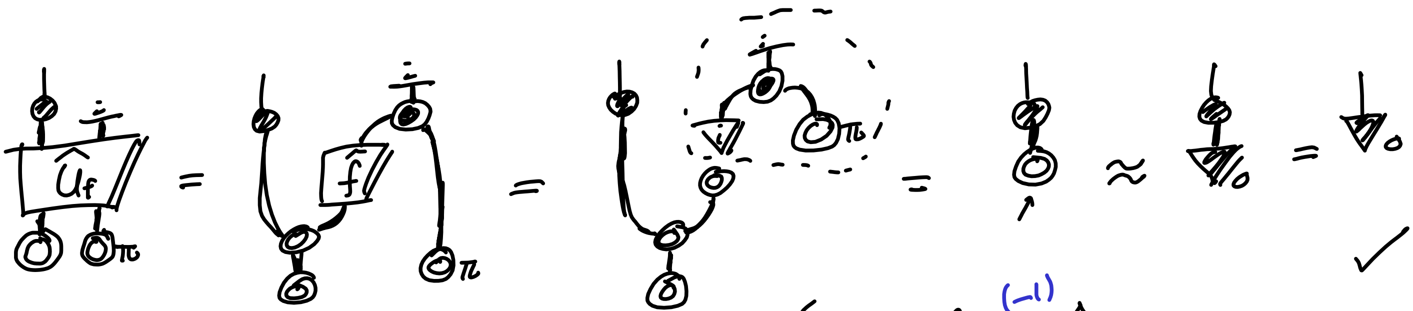
gives outcome $\begin{cases} 0 & \text{if } F \text{ is constant} \\ i>0 & \text{if } F \text{ is balanced.} \end{cases}$

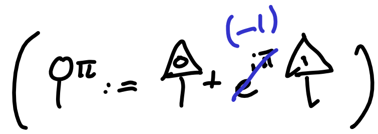
i.e. $\mathrm{Prob}(0) = 1$ if F const.
$\mathrm{Prob}(0) = \emptyset$ if F balanced.

Proof (Correctness of D-J alg.)

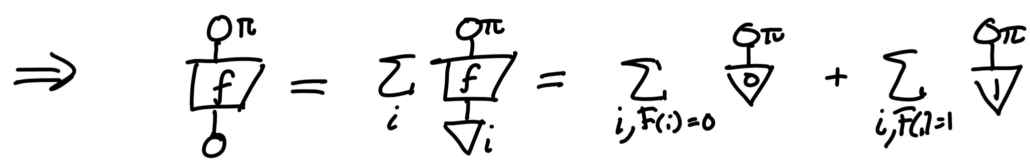
F is constant $\Rightarrow \exists\, i \in \{0,1\}$.



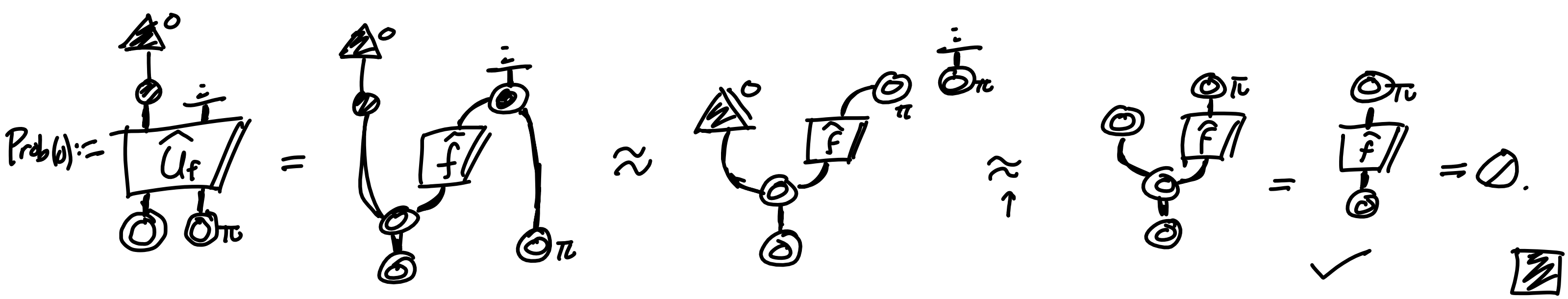




F is balanced



$$= \sum_{i,F(i)=0} 1 + \sum_{i,F(i)=1} (-1) = 0.$$



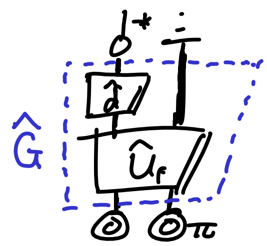
PROBLEM (SIMPLIFIED) GROVER SEARCH.

GIVEN: F s.t. for 1 in 4 inputs i: $F(i) = 1$.

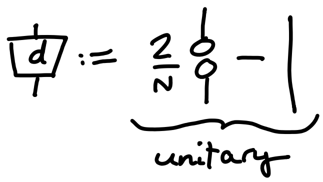
FIND: any i where $F(i) = 1$.

Classically, probabilistically I would expect to run $F \approx 4$ times to find i.

Algorithm



(*) returns ∇_i st. $F(i) = 1$.

where 

Proof (correctness) PQP pp. 773–776.

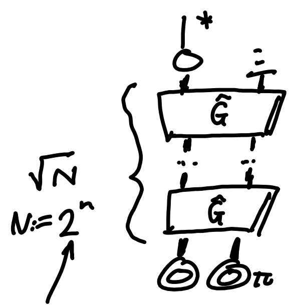
$\Rightarrow$ Quantumly, I need 1 query to F.

PROBLEM Grover search.

GIVEN: $F : \{0,1\}^n \to \{0,1\}$ s.t. for 1 input i, $F(i) = 1$

FIND: i.

Algorithm



* gives ∇_i with prob $\to 1$ as $N \to \infty$.

$\sqrt{2^n} = 2^{\frac{n}{2}} = \sqrt{2}^{\,n}$

Lecture 22

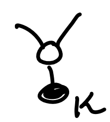
The Hidden Subgroup Problem (and factoring!)

Recall: * every family $\bullet$ of spiders has an associated phase group. $\{\bullet_\alpha\}_\alpha$

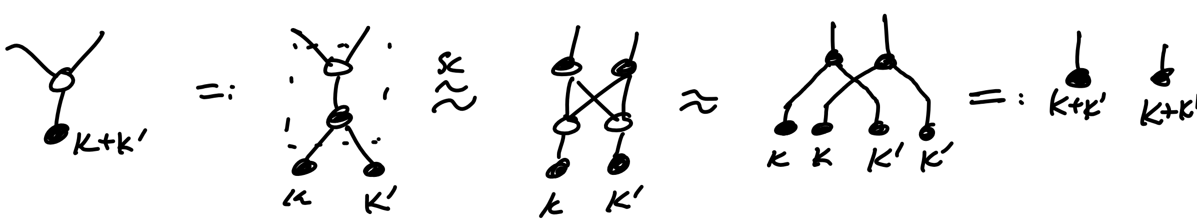
* for complementary spiders $\circ/\bullet$, the $\circ$-basis states form a subset of the phase group.

$$\{\bullet_{k_i} \approx \triangledown_i\}_i \subseteq \{\bullet_\alpha\}_\alpha$$

Thm For strongly compl. $\circ/\bullet$, $\circ$-basis states form a subgroup of the phase group.

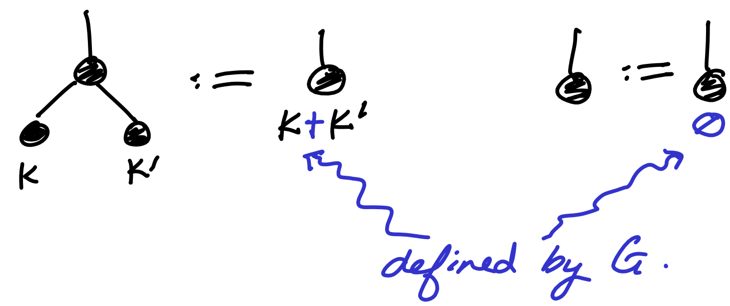
Pf (Recall $\bullet_k$ classical $\iff$  $\approx \bullet_k \bullet_k$)

Spse $\circ/\bullet$ are strongly comp. Let $\bullet_k, \bullet_{k'}$ be classical, then:

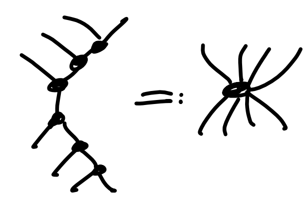


$\Rightarrow \bullet_{k+k'}$ classical. $\square$

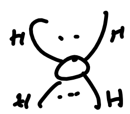
Consequence: if we fix ○, then choosing a finite commutative group G totally fixes ●.



Then from [spider] & [spider], we have $= (\ )^\dagger$ & $= (\ )^\dagger$, so we have all ● spiders.



<u>Thm</u> For any



where $\dim(H) =: D$, there exists <u>exactly</u> <u>1</u> strongly compl. ● for every commutative group of order D.

⇝ i.e. s.c. ○/● are classified by finite comm. groups.

<u>e.g.</u> : * In dim$^{\underline{n}}$ 2, there is a unique s.c. ●, where $G := \mathbb{Z}_2$

* In dim$^{\underline{n}}$ 4, there are 2 s.c. spiders:

$G := \mathbb{Z}_4 \quad \{0,1,2,3\} \quad x \underline{+} y := (x+y) \bmod 4$

$G := \mathbb{Z}_2 \times \mathbb{Z}_2 \quad \{(0,0),(0,1),(1,0),(1,1)\} \quad (x_1,y_1)+(x_2,y_2) := (x_1 \oplus x_2, y_1 \oplus y_2)$

Hidden subgroup problem

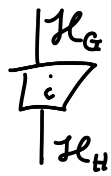
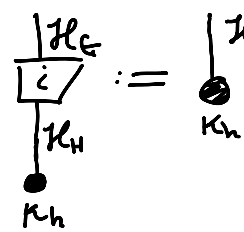
For a commutative group G, fix $\circ/\bullet$ s.c. such that:

$\{ \bullet_{K_g}^{\mathcal{H}_G} \mid g \in G \}$ is the classical subgroup of $\{ \bullet_\alpha \}_\alpha$.

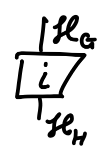
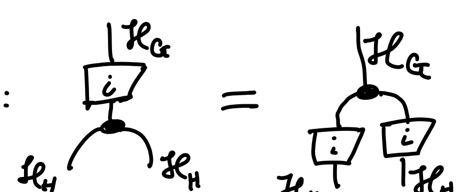
For a subgroup $H \leq G$, fix another s.c. pair $\circ/\bullet$ on $\mathcal{H}_H$

s.t. $\{ \bullet_{K_h}^{\mathcal{H}_H} \mid h \in H \}$ are the cl. subgroup of $\{ \bullet_\alpha^{\mathcal{H}_H} \}_\alpha$.

Q: how are the systems $\mathcal{H}_G$ and $\mathcal{H}_H$ related?

A: let  be defined by 

(RHS makes sense because $H \leq G$, so $h \in H \Rightarrow h \in G$)

Thm  is a group homomorphism:  .

$i(h+h') = i(h) + i(h')$

Pf follows from $H \leq G$ $\blacksquare$

For G and $H \leq G$, we can make a third group:

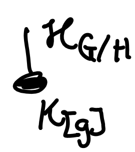
$$\underset{\text{quotient group}}{G/H} := \{ [g] \mid g \in G \}$$

$$[g] := \{ g+h \mid h \in H \} \subseteq G.$$

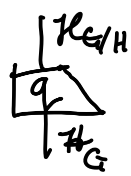
$$[g] + [g'] := [g+g']$$

e.g. $\mathbb{Z}_4 := \{0,1,2,3\}$ $\quad H := \{0,2\} \leq \mathbb{Z}_4$

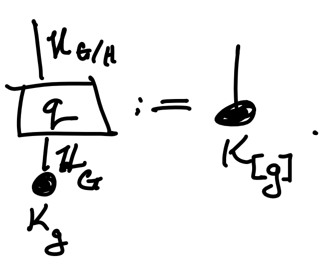
then $\mathbb{Z}_4/H := \{ [0] := \{0,2\}, [1] := \{1,3\}, \cancel{[2] := \{2,0\}}, \cancel{[3] := \{3,1\}} \}$

Make a third s.c. $\overset{o/o}{\text{pair}}$ where $\{$  $\mid [g] \in G/H \}$.

Q: How are the systems $\mathcal{H}_G$ and $\mathcal{H}_{G/H}$ related?

A: We have a map  called the quotient map

where:

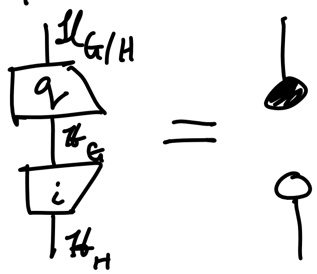


$$h \in H \xmapsto{\ i\ } h \in G \xmapsto{\ q\ } [h] \in G/H$$

$$[h] = [0]$$

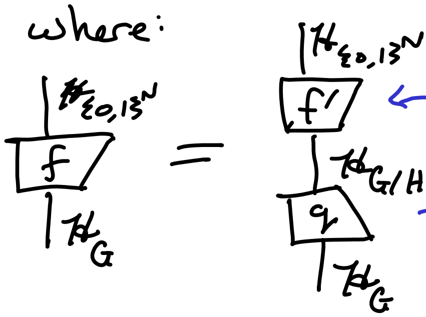
$$[h] = \{h + h' \mid h' \in H\} = \{0 + h' \mid h' \in H\}$$

or as a picture:



<u>Problem</u> Hidden subgroup:

GIVEN: $f : G \to \{0,1\}^N$ such that $\exists$ subgroup $H \leq G$ where:



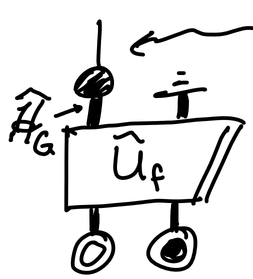
injective f^n

"hides H"

"f is constant on the cosets of $\underline{H}$"

FIND: H.

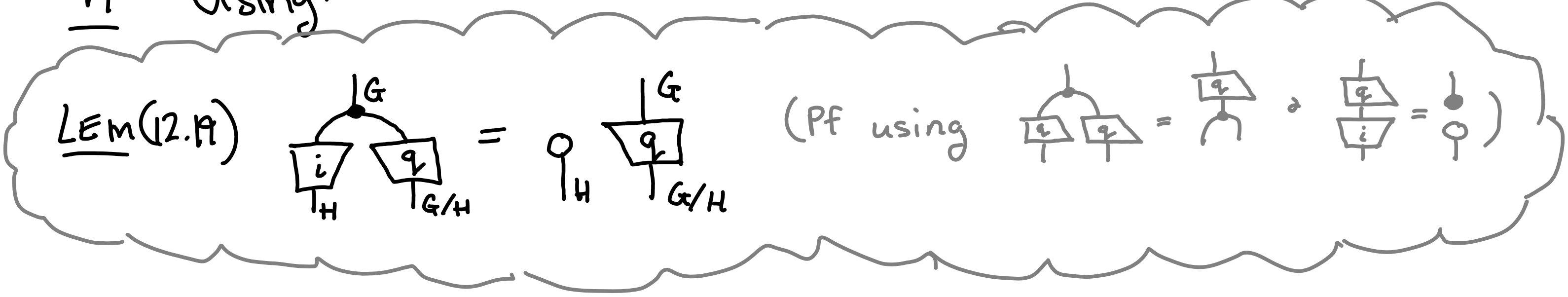
ALGORITHM:

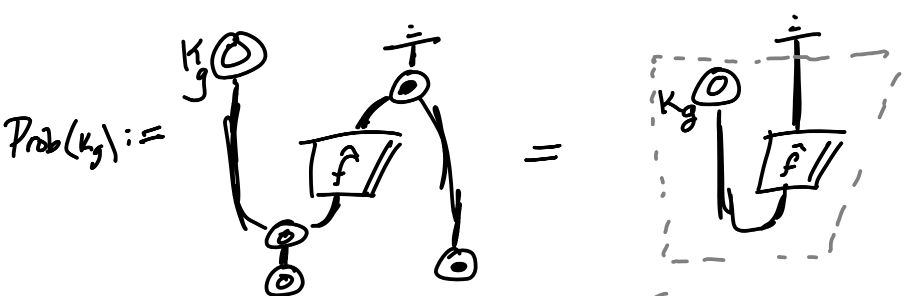


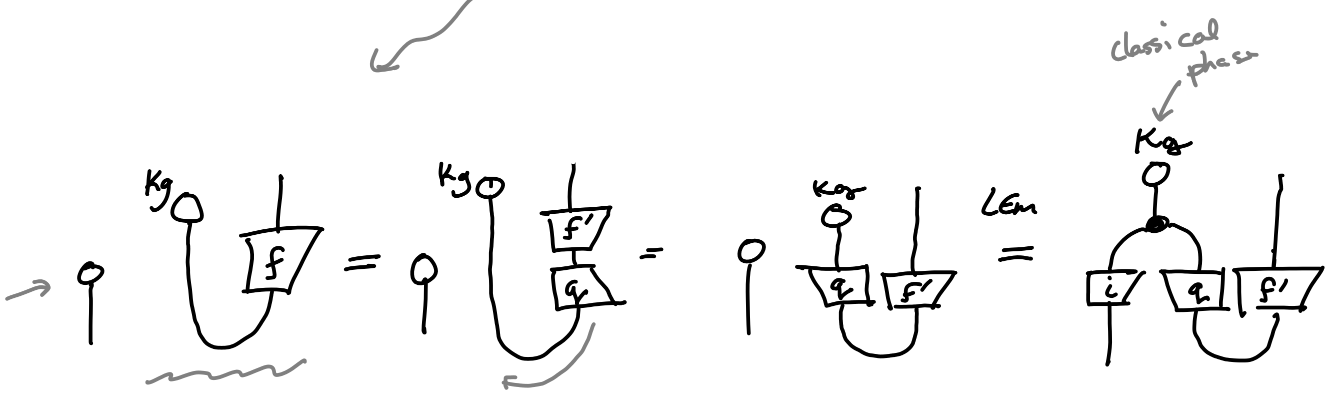
gets outcomes $\{\hat{\phi}_g \approx \delta_{K_g}\}$

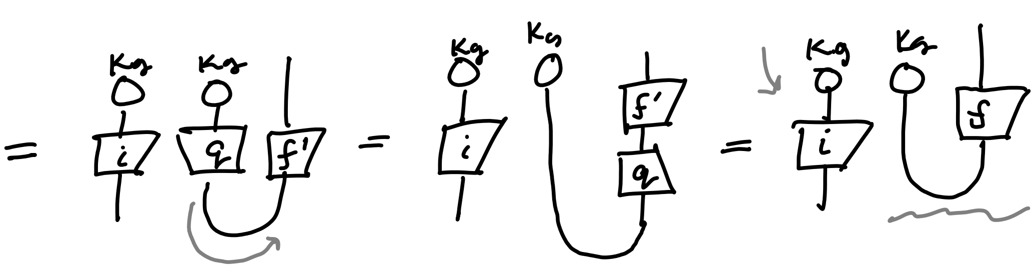
Q: Which outcomes δ_{K_g} do we get?

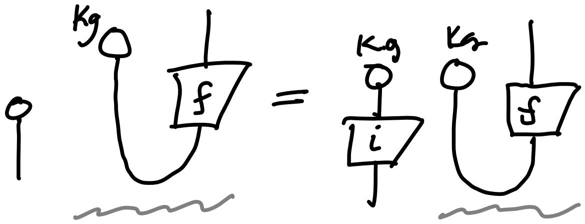
A: Using:



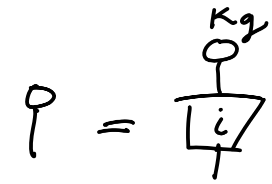


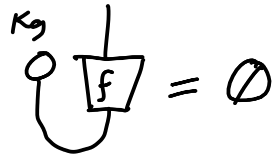


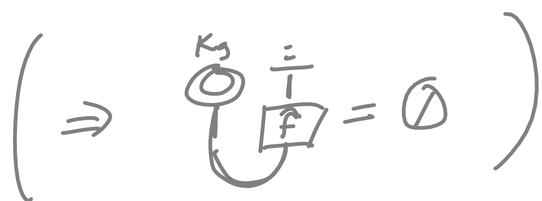




EITHER

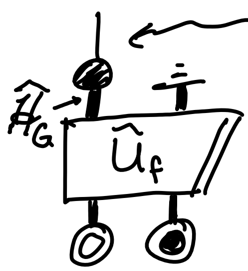
(i) 

(ii) 

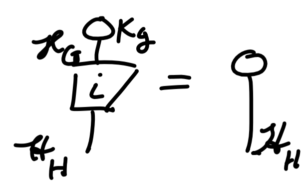


NEVER SEE OUTCOMES FOR CASE (ii).

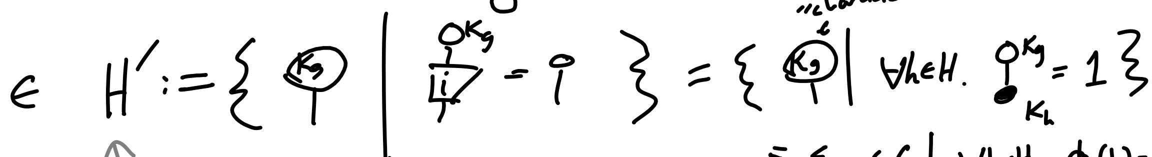
$\Longrightarrow$



gets outcomes $\{ \psi_g \approx K_g \}$

SUCH THAT: 

i.e.  "acts like deleting on the elements of H".



$= \{ g \in G \mid \forall h \in H.\ \phi_g(h) = 1 \}$

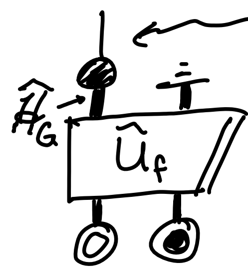
annihilator of H.

THM (classical gp theory) For any $H \leq G$, $H' \leq G$ and $(H')' = H$.

efficiently

SUMMARY: To SOLVE HSP:

1. Do



gets outcomes $\{ \phi_g \approx \delta_{K_g} \}$

2. Repeat until we have enough δ^{K_g} to generate H', then compute $H'' = H$ classically from H'.

$O(\log|H|)$

<u>Q</u>: What does HSP have to do with ~~factoring~~? period finding.

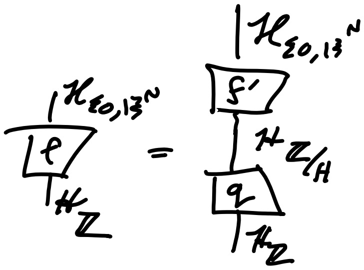
<u>PROBLEM</u>: Given $f : \mathbb{Z} \to \{0,1\}^N$ such that:

$$\exists r . \forall x . \ f(x+r) = f(x)$$

<u>FIND</u>: $r \in \mathbb{Z}$.

$$\Longleftrightarrow$$

<u>PROBLEM</u> Given f such that:



where $H := \{rk\}_{k \in \mathbb{Z}}$

<u>FIND</u>: H.

Q: What does period finding have to do with factoring?

THM Let $f(x) = a^x \bmod D$. If $\forall x.\ f(x) = f(x+r)$ and r is even, then either $\underbrace{a^{r/2}+1}$ or $\underbrace{a^{r/2}-1}$ is a factor of D.

I want to factor

non-trivial factor of D!

Pf (modular arithmetic, find it in PQP.)