9.3 Strong complementarity.

Def 0 and 0 are strongly complementary if:

\((sc1) \sim \) \hspace{1cm} \((sc2) \sim \) \hspace{1cm} \((sc3) \sim \) \hspace{1cm} \((sc4) \sim \)

"or equivalently:

\((sc) \sim \)

\(<\sim \) totally connected
\(\langle \) complete bipartite graph \(\rangle\)

\((sc) \Rightarrow (sc1) + (sc2) + (sc3)\)
$Trim \text{ Strong compl. } \Rightarrow \varnothing \simeq \varnothing$.

**Pf**

$\varnothing = \varnothing = \varnothing = \varnothing \approx \varnothing = \varnothing$.

$\approx$

$\approx$

$\approx$

The main use of "\(2\text{r}\)" strong complementarity comes from:

$\sqrt{2} \varnothing = \frac{1}{\sqrt{2}} \varnothing = \frac{1}{\sqrt{2}} \sqrt{2}$

\[\text{xor} \]

\[\text{xor} \]

\[\text{xor} \]

\[\text{xor} \]

\[\text{xor} \]

n.b., for complementarity: \[\frac{1}{\sqrt{2}} \varnothing = \frac{1}{\sqrt{2}} \varnothing \Rightarrow \varnothing = \frac{1}{\sqrt{2}} \varnothing \]
\[ \frac{1}{\sqrt{2}} | \xi \rangle = \frac{1}{\sqrt{2}} \left( | \downarrow \rangle + e^{i\pi} | \downarrow \rangle \right) = | \downarrow \rangle. \]

\[ \frac{1}{\sqrt{2}} | \pi \rangle = \frac{1}{\sqrt{2}} \left( | \downarrow \rangle + e^{i\pi} | \downarrow \rangle \right) = \frac{1}{\sqrt{2}} \left[ | \downarrow \rangle - | \downarrow \rangle \right] = | \uparrow \rangle. \]

\[ \text{xor} \] is the group addition for the group \( \mathbb{Z}_2 \) (integers modulo 2) of order 2, cyclic group of order 2.
Classical subgroup

\[ \mathbb{Z}_2 \]

\[ \{0, 1\} \]

Phase group \( U(1) \)

\[ \{0, 2\pi\} \]

9.76

\[ \mathbb{Z}_2 \times \mathbb{Z}_2 \] and \( \mathbb{Z}_2 \) are strongly complementary iff the classical phases:

\[ \{0, 2\pi\} \] form a subgroup of the phase group.

\[ \mathbb{Z}_2 \times \mathbb{Z}_2 \text{ classical phases } \Rightarrow \text{ classical phase } \]

9.4 \( \mathcal{ZX}\)-calculus := \( SC + (1 \text{ Bloch sphere}) \)

Def The \( \mathcal{ZX}\)-calculus consists of 4 rules:

\[ \alpha_1 \oplus \alpha_2 = \alpha_1 + \alpha_2 \]

\[ \alpha_1 \oplus \alpha_2 = \alpha_1 + \alpha_2 \]

Where

\[ \begin{array}{c}
\text{Hadamard}\\
\text{Euler decr}\end{array} \]

\[ \begin{array}{c}
\text{X}\\
\text{Z}\\
\text{Y}\end{array} \]
ZX-rules are colour-symmetric:

\[
\begin{align*}
\text{ZX-rules } & \rightarrow \quad \equiv \quad \equiv \\
\end{align*}
\]

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

Q: Why?

- Efficient Automation
- Make use of algebraic structures
- Closer to logic

Def 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 \( \approx \) to one of the following states:

\[
\begin{align*}
\begin{array}{c}
\circ & \circ \\
\text{0-basis states} & \text{Z-basis states}
\end{array}
\end{align*}
\]

\[
\begin{align*}
\begin{array}{c}
\circ & \circ \\
\text{0-basis \#'s} & \text{X-basis \#'s}
\end{array}
\end{align*}
\]

\[
\begin{align*}
\begin{array}{c}
\circ & \circ \\
\text{Y-basis \#'s}
\end{array}
\end{align*}
\]

Thm: The \( ZX \)-calculus is complete for Clifford \( ZX \)-diagrams, i.e. if two \( Q \) \( ZX \)-diagrams describe the same linear map, we can prove they are equal with the \( ZX \)-calculus.

\[
\begin{align*}
\begin{array}{c}
\begin{array}{c}
\circ \quad \circ \\
D
\end{array}
\end{array}
\rightleftharpoons \begin{array}{c}
\begin{array}{c}
\circ \quad \circ \\
E
\end{array}
\end{array}
\end{align*}
\]

\[
\Rightarrow \begin{array}{c}
\begin{array}{c}
\circ \quad \circ \\
D
\end{array}
\end{array} \equiv \begin{array}{c}
\begin{array}{c}
\circ \quad \circ \\
D
\end{array}
\end{array} \equiv \ldots \equiv \begin{array}{c}
\begin{array}{c}
\circ \quad \circ \\
D_m
\end{array}
\end{array} \equiv \begin{array}{c}
\begin{array}{c}
\circ \quad \circ \\
E
\end{array}
\end{array}
\end{align*}
\]

and furthermore, this is efficient! (polynomially many steps)
Quantum computations involving only Clifford ZX-diags can be efficiently simulated on a classical computer.

\[ \Rightarrow \text{version of the Gottesman-Knill theorem.} \]

\[ \text{Proc} \]

\[ \text{Clifford ZX-diagram} \]

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)

- Single qubit: $\begin{array}{c}
\text{matrices} \quad \text{Clifford ZX-diagrams} \\
\scriptstyle 2 \times 2 \quad \approx \text{single spider} \in \{0, \frac{\pi}{4}, \frac{\pi}{2}, \frac{3\pi}{4}, \pi\} \\
\text{vector} \quad \approx \mathcal{O}(n^2) \text{ spiders in it.}
\end{array}$

$n=20 \quad \approx 10^6 \text{ dim.'l} \quad \approx 400 \text{ spiders}$

($Q$-calculus $\rightarrow \mathcal{X} \ + \text{ all 1-qubit unitaries given as quaternions}$)

Finite, discrete, classical $\subseteq$ Discrete $\subseteq$ All

- Clifford ZX-diagrams $\subseteq$ Clifford+T ZX-diagrams $\subseteq$ All

- $k\frac{\pi}{4}$, $k\frac{3\pi}{4}$

ZX-diagrams are universal:

- For all $2^n \times 2^m$ matrices, $\exists$ ZX-diagram $D$ s.t.
  $\frac{\vdots}{D} \leftrightarrow M$  \hfill ($\Rightarrow$ any group can be expressed as a ZX-diagram)
Thm. Clifford $+$ T ZX-diagrams are approx. universal.

For any linear map $\begin{array}{c} \psi \end{array}$ and $\epsilon > 0$, there exists a Clifford-$+$T ZX-diagram $\begin{array}{c} \mathcal{D} \end{array}$ such that:

$$\left\| \begin{array}{c} \mathcal{F} \end{array} - \begin{array}{c} \mathcal{D} \end{array} \right\| < \epsilon .$$

[recall: $\left\| \begin{array}{c} \psi \end{array} \right\|^2 = \begin{array}{c} \psi \end{array}$]

n.b. as $\epsilon \to 0$, $\begin{array}{c} \mathcal{D} \end{array} \to \begin{array}{c} \mathcal{F} \end{array}$.

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

Lecture 20

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


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 are complete for all ZX-diagrams. \( \text{arXiv:1812.09114}^* \)

* 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 \[\text{Deutch 1985}\]
  - quantum circuit model \[\text{Deutch 1989}\]
    - measurement-based QC
    - solid state (supercool, ion traps)
    - topological
    - adiabatic QC
      - eg. D-Wave
Computations in the q. circuit model consist of:

1. preparation
2. apply unitary gates
3. measure in Z-basis
4. classical post-processing

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

E.g.:

$\text{CNOT} := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $H := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ $\leftarrow$ Clifford

$\phi$ $\leftarrow$ Clifford + phase

Any unitary can be built from Clifford+phase gates, exactly.
Any unitary can be approximated from Clifford+T gates, for any $\epsilon$.

\[
\begin{array}{c}
\hat{U} \\
\text{circuit A}
\end{array}
\approx
\begin{array}{c}
\text{Clifford+T}
\end{array}
\]

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

A: “What does $\hat{U}$ do to $\varphi$?”

- Exponentially big

Applications: Simulating physical q. processes.
- Condensed matter
- Quantum chemistry

Q: Can it solve classical problems faster?

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

\[ F : \{0,1\}^N \rightarrow \{0,1\}^3 \]

e.g. **Problem**: SAT

given $F$ as a logical formula, does there exist any bitstring $s$ s.t. $F(s) = 1$?
Step 1: Define a quantum oracle.

\[ \text{function } F \rightarrow \text{ linear map } f \rightarrow \text{ unitary } U_f \]

always unitary.

\[ U_f \text{ is unitary for a classical } f = f. \]

**Pf**

\[ \begin{align*}
    & \begin{array}{c}
        \text{Classical } f
    \end{array} \\
    & \begin{array}{c}
        \text{complementary } f
    \end{array}
\end{align*} \]

\[ = \begin{align*}
    & \begin{array}{c}
        \text{causality } f
    \end{array} \\
    & \begin{array}{c}
        \text{is similar...}
    \end{array}
\end{align*} \]
Q: What can I do with $\hat{U}_f$?

A1: We can:

\[ \hat{U}_f = \downarrow = \downarrow = \downarrow \]

A2: More interesting:

\[ \hat{U}_f = \downarrow = \downarrow \]

double (8)

\[ \leadsto \text{8 state that "knows everything" about } f. \]

(\[ \equiv \text{to } f \text{ under map-state duality}. \]

The catch: to get info, we need to measure.

e.g. a bad choice of measurement:

\[ \hat{f} \]

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

\[ \text{...equivalently, we could pick } i \text{ at random and compute } F(i). \]

\[ \Rightarrow \text{we should choose measurements carefully}. \]
Problem: Deutsch-Jozsa problem:

Given a function $F$ which is either constant or balanced:

$F: \mathbb{Z}_2^n \to \{0,1\}$

Decide: Is $F$ constant or balanced?

Classically:

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

A: $\frac{2^n}{2} + 1 \leftarrow$ more than half of $\mathbb{Z}_2^n$ in the worst case.

Quantumly:

A: 1 (!)

Algorithm:

\[ \hat{U}_F \]

\[ \hat{U}_I \]

Output part gives outcome:

- $\downarrow_0$ if $F$ is constant
- $\downarrow_i > 0$ if $F$ is balanced.

i.e.

$\text{Prob}(0) = 1$ if $F$ const.

$\text{Prob}(0) = 0$ if $F$ balanced.
Proof (Correctness of D-J alg.)

$F$ is constant $\Rightarrow \exists i \in \{0,1\} \quad f = \begin{array}{c}
\text{output } i \\
\text{ignore input}
\end{array}
$

$F$ is balanced

$\Rightarrow \quad f = \sum_i q_i \frac{\eta^n}{\eta^i} = \sum_{i, F(i) = 0} q_i \frac{\eta^n}{\eta^i} + \sum_{i, F(i) = 1} q_i \frac{\eta^n}{\eta^i}
$

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

Proof:

$\hat{U}_f = \begin{array}{c}
\text{output } i \\
\text{ignore input}
\end{array}
$

$\sim f = \begin{array}{c}
\text{output } i \\
\text{ignore input}
\end{array}
$

$\sim f = \begin{array}{c}
\text{output } i \\
\text{ignore input}
\end{array}
$

$\sim \frac{\eta^n}{\eta^0} \sim 0$ and $\frac{\eta^n}{\eta^0} \sim 0$.
**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, I would expect to run $F \approx 4$ times to find $i$.

**Algorithm**

(where $\mathcal{U}_F$ is unitary)

$(4)$ returns $\frac{1}{\sqrt{4}}$ st. $F(i) = 1$.

Proof (Correctness) PQ8 pp. 773-776.

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

**Problem Grover Search.**

Given: $F : \mathbb{2}^n \rightarrow \mathbb{2}^n$ s.t. for 1 input $i$, $F(i) = 1$.

Find: $i$.

**Algorithm**

$\sqrt{N}$ times

& gives $\frac{1}{\sqrt{4}}$ with prob $\rightarrow 1$ as $N \rightarrow \infty$. 

$\sqrt{2^2} = 2^2 = 4^\frac{1}{2}$
The Hidden Subgroup Problem
(and factoring!)

Recall: * every family of spiders has an associated phase group: \( G \)

* for complementary spiders \( \mathcal{O}/\mathcal{O} \), the \( \mathcal{O} \)-basis states form a subset of the phase group:

\[
\mathcal{O}_{k_i} \approx \bigvee_{i} \mathcal{O}_{k_i} = \bigvee \mathcal{O}_{a \cdot k_i}
\]

Theorem: For strongly complementary \( \mathcal{O}/\mathcal{O} \), \( \mathcal{O} \)-basis states form a subgroup of the phase group.

Proof (Recall \( \mathcal{O}_k \) classical \( \Rightarrow \mathcal{O}_k \approx \mathcal{O}_k \mathcal{O}_k \))

Suppose \( \mathcal{O}/\mathcal{O} \) are strongly complementary, let \( \mathcal{O}_k, \mathcal{O}_{k'} \) be classical, then:

\[
\mathcal{O}_{k+k'} = \mathcal{O}_k \mathcal{O}_{k'} \approx \mathcal{O}_{k} \mathcal{O}_{k'} =: \mathcal{O}_{k+k'}
\]

\( \Rightarrow \mathcal{O}_{k+k'} \) classical.
Consequence: if we fix $\hat{a}$, then choosing a commutative group $G$ totally fixes $\hat{a}$.

Then from $\hat{a} \neq \hat{b}$, we have $\hat{Y} = (\hat{a})^+ \circ \hat{q} = (\hat{b})^+$, so we have all $\hat{a}$ spiders.

For any $\hat{Y}$ where $\dim(H) = D$, there exists exactly 1 strongly comple supplement for every commutative group of order $D$.

\[ i.e. \ s.c. \ 0/0 \ are \ classified \ by \ finite \ commutative \ groups. \]

\[ e.g. \ * \ In \ \dim = 2, \ there \ is \ a \ unique \ s.c. \ \hat{a}, \ where \ G = \mathbb{Z}_2 \]

\[ * \ In \ \dim = 4, \ there \ are \ 2 \ s.c. \ spiders: \]

\[ G = \mathbb{Z}_4 \ \triangleright \ (0,1,2,3) \ \ x+y = (x+y) \ mod \ 4 \]

\[ G = \mathbb{Z}_2 \times \mathbb{Z}_2 \ \triangleright \ (0,0), (0,1), (1,0), (1,1) \]

\[ (x,y) + (x',y') = (x+x', y+y') \]
Hidden Subgroup problem

For a commutative group $G$, fix $0/\circ$ s.c. such that:

$$\exists \frac{[K_h]}{K_h} \mid g \in G \exists \frac{[\mathbb{Q}]}{\mathbb{Q}}$$

is the classical subgroup of $\frac{[\mathbb{Q}]}{\mathbb{Q}}$.

For a subgroup $H \leq G$, fix another s.c. pair $0/\circ$ on $H$:

$$\exists \frac{[K_h]}{K_h} \mid h \in H \exists \frac{[\mathbb{Q}]}{\mathbb{Q}}$$

are the classical subgroup of $\frac{[\mathbb{Q}]}{\mathbb{Q}}$.

Q: how are the systems $H_G$ and $H_H$ related?

A: let $\frac{[H_G]}{K_h}$ be defined by $\frac{[H_G]}{K_h} := \frac{[K_h]}{K_h}$

RhS makes sense because $H \leq G$, $0 \to h \in H$ (\[
\text{Thm: } \frac{[H_H]}{K_h} \text{ is a group homomorphism: }
\]
\[
\text{Pf follows from } H \leq G \]

$i(h + h') = i(h) + i(h')$
For $G$ and $H \leq G$, we can make a third group:

$$G/H := \{ [g] \mid g \in G \}$$

Quotient group

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

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

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


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

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

A: We have a map $\varphi : \mathcal{H}_G \to \mathcal{H}_{G/H}$ called the quotient map

where:

$$\varphi : \mathcal{H}_G / [g] := [g] \to \mathcal{H}_{G/H} / [g] \subseteq [g].$$
Problem Hidden subgroup:

Given: \( f: G \rightarrow \{0,1\}^n \) such that \( \exists \) subgroup \( H \leq G \) where:

\[
\begin{align*}
T_{G/H}^{f_{0,13^n}} &= f \\
T_{G/H}^{f_{13^n}} &= f
\end{align*}
\]

\( f \) is injective \( f^{-1} \) “hides \( H \)”

Find: \( H \).

Algorithm: gets outcomes \( \{ \hat{v}_g \approx b_{kg} \} \)
Q: Which outcomes $b_{kg}$ do we get?

A: Using:

\[
\text{LEM(12.1)} \quad \frac{L}{G} = \frac{G}{G/H}
\]

(Pf using $\frac{L}{G} = \frac{G}{G/H}$)

\[
\text{Prob}(b) := \frac{k_g}{f} \quad \frac{G}{G/H} = \frac{G}{G/H}
\]

\[
\begin{align*}
\text{LEM} & : \quad \frac{L}{G} = \frac{G}{G/H} \\
\text{LEM} & : \quad \frac{L}{G} = \frac{G}{G/H} \\
\text{LEM} & : \quad \frac{L}{G} = \frac{G}{G/H}
\end{align*}
\]
\[
\begin{align*}
\mathcal{U}_f = \mathcal{U}_g &= \mathcal{U}_i \cup \mathcal{U}_f \\
\text{Either} &
\begin{cases}
\text{(i) } \mathcal{U} = \mathcal{V} \\
\text{(ii) } \mathcal{U} = \emptyset
\end{cases}
\Rightarrow \mathcal{U}_g \cup \mathcal{U}_f = \emptyset
\end{align*}
\]

NEVER SEE OUTCOMES
FOR CASE (ii).

\[\Rightarrow \text{ gets outcomes } \{ \psi_g \sim \phi_{K_0} \} \]

SUCH THAT:
\[
\begin{align*}
\mathcal{U}_f &\subseteq \mathcal{U}_g \\
\mathcal{U}_f &\subseteq \mathcal{U}_g
\end{align*}
\]

i.e. \( \phi_{K_0} \) "acts like deleting on the elements of H".

\[
\begin{align*}
\mathcal{E} \mathcal{H} &\subseteq \mathcal{G} \\
\mathcal{E} \mathcal{H} &\subseteq \mathcal{G}
\end{align*}
\]

\[
\begin{align*}
\mathcal{E} \mathcal{G} &\subseteq \mathcal{G} \\
\mathcal{E} \mathcal{G} &\subseteq \mathcal{G}
\end{align*}
\]

THM (classical graph theory) FOR any \( H \leq G \), \( H' \leq G' \) and \( (H')' = H' \) efficiently.
Summary: To solve HSP:

1. Do \( R \) gets outcomes \( \{ y \approx b \} \)

\[ O(\log |H|) \]

2. Repeat until we have enough \( Q^{k_B} \) to generate \( H' \) then compute \( H'' = H \) classically from \( H' \).

Q: What does HSP have to do with factoring?

Problem: Given \( f: \mathbb{Z} \to \{0,1\}^N \) such that:

\[ \exists r. \forall x. f(x+r) = f(x) \]

Find: \( r \in \mathbb{Z} \).

\[ \iff \]

Problem: Given \( f \) such that:

\[ \frac{1_{\mathbb{Z}_{k_B,13}^*}}{1_{\mathbb{Z}_k}} = \frac{1_{\mathbb{Z}_k^*}}{1_{\mathbb{Z}_{k^*}}}, \quad \text{where} \quad H = \exists k \exists z. k \in \mathbb{Z} \]

Find: \( H \).
Q: What does period finding have to do with factoring?

Thm Let \( f(x) = a^x \mod D \). If \( \forall x \cdot f(x) = f(x+r) \) and \( r \) is even, then either \( a^{\frac{r}{2}} + 1 \) or \( a^{\frac{r}{2}} - 1 \) is a factor of \( D \!

Pf (modular arithmetic, find it in PQP.)