# Lecture 5

(S) <u>States</u> are descr. by vectors* in a Hilbert space

(C) <u>Compound</u> systems are decribed by the tensor product.

(U) Time-evolution is <u>unitary</u>.

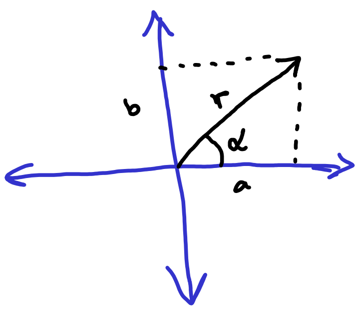
(M) <u>Measurement</u> probabilities come from the Born rule.

(*) Complex numbers can be written in:

<u>Cartesian form</u>: $c = a + ib$, $a \in \mathbb{R}$, $b \in \mathbb{R}$

<u>Polar form</u>: $= re^{i\alpha}$, $r \in \mathbb{R}_{\geq 0}$, $\alpha$: angle

$\left(e^{i\alpha} := \cos\alpha + i\sin\alpha\right)$




Let $|c| := \sqrt{\bar{c} \cdot c}$, the absolute value. $c = re^{i\alpha} \Rightarrow |c| = r$.

When $|c| = 1$, $r = 1$. So $c = e^{i\alpha}$. This number is called a <u>complex phase</u>, or just a <u>phase</u>.

<u>PROPERTIES</u>

1. $e^{i0} = e^{0} = 1$
2. $\overline{e^{i\alpha}} = \cos\alpha - i\sin\alpha = \cos(-\alpha) + i\sin(-\alpha) = e^{-i\alpha}$
3. $e^{i\alpha} \cdot e^{i\beta} = e^{i(\alpha+\beta)}$

# States

**Def** A quantum pure state is a normalised vector $|\psi\rangle \in \mathcal{H}$, upto a global phase: $|\psi\rangle \sim e^{i\alpha} \cdot |\psi\rangle$.

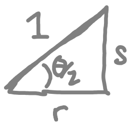
$\langle\psi|\psi\rangle = 1$

We ignore global phases because they don't affect <u>measurement</u> probabilities, as we will see.

— In 2D, this gives a nice way to plot qubit states $|\psi\rangle \in \mathbb{C}^2$.

$$\triangledown_{\psi} = re^{i\beta}\,\triangledown_{0} + se^{i\gamma}\,\triangledown_{1}$$

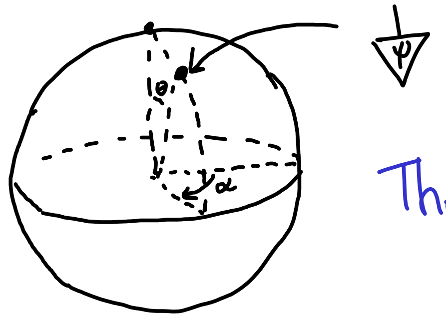
$\psi$ normalised $\iff$ $r^2 + s^2 = 1$ $\iff$ for some $\theta$: $r = \cos\frac{\theta}{2}$ $\quad s = \sin\frac{\theta}{2}$




$$\triangledown_{\psi} = \cos\tfrac{\theta}{2}\, e^{i\beta}\,\triangledown_{0} + \sin\tfrac{\theta}{2}\, e^{i\gamma}\,\triangledown_{1}$$

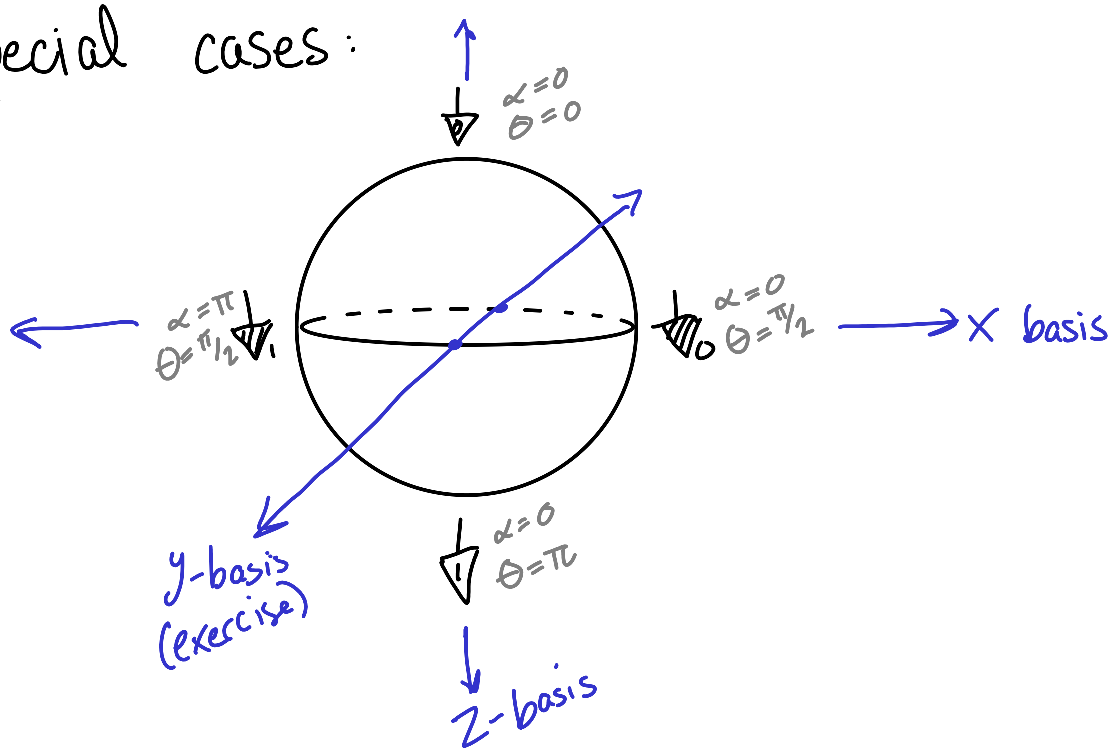
$$\sim e^{-i\beta} \cdot \triangledown_{\psi} = \cos\tfrac{\theta}{2}\,\triangledown_{0} + \sin\tfrac{\theta}{2}\, e^{i\alpha}\,\triangledown_{1} \qquad (\alpha = \gamma - \beta)$$

$|\psi\rangle$ (upto phase) is totally described by 2 angles, which we can plot on a sphere:




The Bloch sphere.

Special cases:



# Compound Systems

... are described by the tensor product:

$$\underset{d\text{-dim'l}}{\mathcal{H}}\,,\ \underset{e\text{-dim'l}}{\mathcal{K}} \rightsquigarrow \underset{d\cdot e \text{ dim'l}}{\mathcal{H}\otimes\mathcal{K}}$$

$\{|i\rangle\}_{i=1}^{d}$ ONB

$\{|j\rangle\}_{j=1}^{e}$ ONB

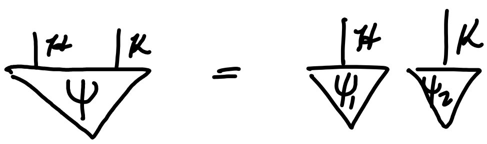
$\{|i,j\rangle := |i\rangle\otimes|j\rangle\}_{i=1,j=1}^{d,e}$ product ONB

$$(\mathbb{C}^2)^{\otimes n} := \underbrace{\mathbb{C}^2\otimes\ldots\otimes\mathbb{C}^2}_{n}$$

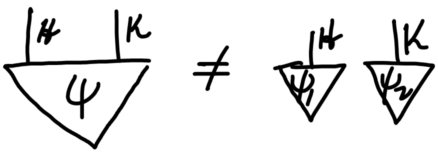
$N = 2^n$-dim'l

$\{|\vec{b}\rangle = |b_1,\ldots,b_n\rangle \mid b_k\in\{0,1\}\}$

bitstring basis




separable

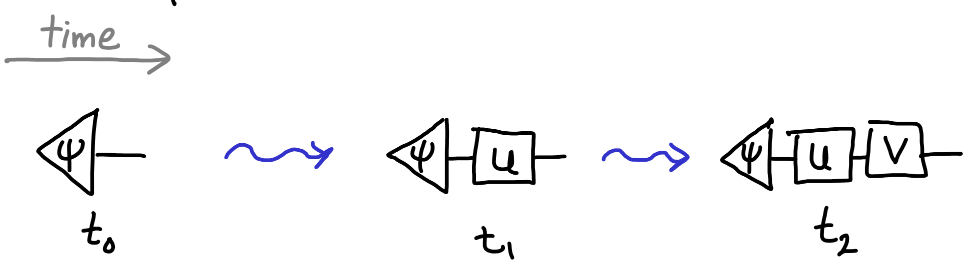



non-separable / entangled

# Unitaries

Time evolution in QT is:

* linear
* preserves normalisation.




the same

<u>Thm</u> A linear map $U : \mathcal{H} \to \mathcal{H}$ preserves normalisation ($\| |\psi\rangle \|^2 = 1 \Rightarrow \| U|\psi\rangle \|^2 = 1$) if and only if it is <u>unitary</u>, i.e.


Time-independent Schrödinger eqn:

$$i\hbar \frac{d}{dt} |\psi_t\rangle = \underbrace{H}_{\substack{\text{Hamiltonian} \\ H = H^\dagger}} |\psi_t\rangle$$

where the physics lives!

Solutions are always of the form: $|\psi_t\rangle = \underbrace{e^{-i\frac{t}{\hbar}H}}_{\text{matrix exponential}} |\psi_0\rangle$

$$i\hbar \frac{d}{dt}|\psi_t\rangle = i\hbar \frac{d}{dt}\left(e^{-i\frac{t}{\hbar}H}|\psi_0\rangle\right) = \cancel{i\hbar}\cdot\frac{-i}{\cancel{\hbar}} H\left(e^{-i\frac{t}{\hbar}H}|\psi_0\rangle\right) = H|\psi_t\rangle$$

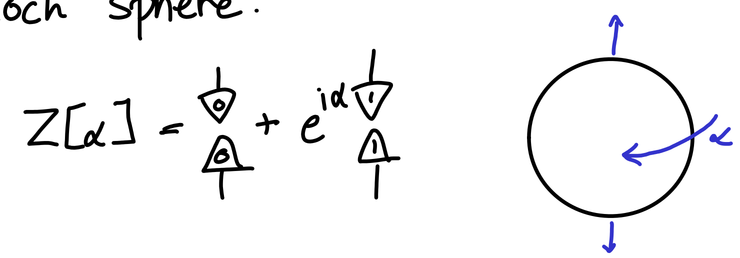
<u>BUT</u> for us the only important thing is:

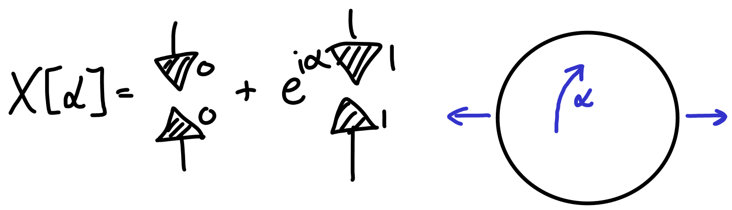
$H$ self-adjoint $\Rightarrow$ $U = e^{-i\frac{t}{\hbar}H}$ unitary.

$U \longleftrightarrow$ "evolving for a fixed amount of time $t$"

For qubits, unitaries $U : \mathbb{C}^2 \to \mathbb{C}^2$ corresp. to <u>rotations</u> of the Bloch sphere.

e.g.



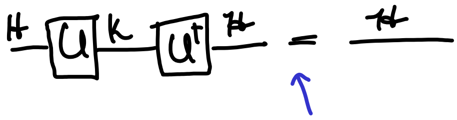




<u>Any</u> unitary can be written:

$$-\boxed{U}- = e^{i\theta}\, -\boxed{Z[\alpha]}-\boxed{X[\beta]}-\boxed{Z[\gamma]}-$$

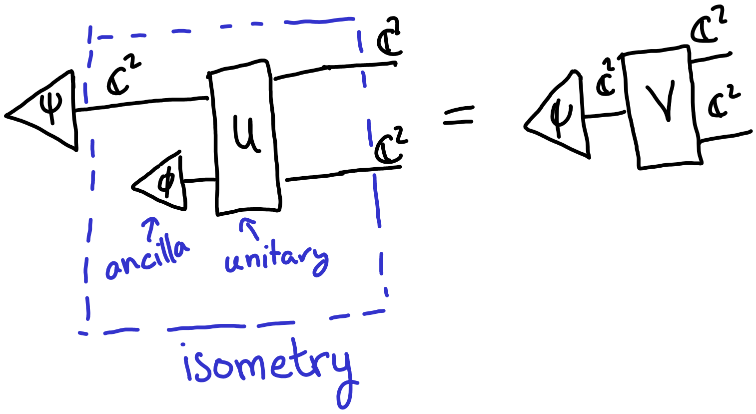
Euler decomposition.

Thm $U : \mathcal{H} \to K$ presv's normalisation if it is an isometry.




adj. is one-sided inverse

Ex unitary + ancilla :



# Lecture 6

## Measurements

- A <u>measurement</u> is the only way to get information out of a quantum system.
- It is non-deterministic, and has an <u>outcome</u> $j \in \{1, \dots, k\}$
- For a state $|\psi\rangle$ & measurement $\mathcal{M}$, quantum theory tells us how to compute:

  1. the probability of outcome $j$
  2. the post-measurement state

<u>Def</u> A linear map $P$ is called a <u>projector</u> if it is: <u>self-adjoint</u> and <u>idempotent</u>.

$P = P^\dagger$ $\qquad$ $PP = P$

A projector spits a space into two orthogonal pieces:

$$\mathrm{im}(P) := \{ |\psi\rangle \mid P|\psi\rangle = |\psi\rangle \}$$

identity matrix

$$\mathrm{im}(P)^\perp = \{ |\psi\rangle \mid P|\psi\rangle = 0 \} = \mathrm{im}(Q) \qquad Q = I - P$$

$$\mathcal{H} = \mathrm{im}(P) \oplus \mathrm{im}(Q) \longleftrightarrow P + Q = I.$$

More generally, $P_1, \dots, P_k$ where $\sum_{j=1}^{k} P_j$ splits into $k$ orthogonal pieces.

Def A quantum (von Neumann) measurement is a set of projectors:

$$\mathcal{M} = \{M_1, \dots, M_k\} \quad \text{where} \quad \sum_j M_j = I.$$

1. When we measure $|\psi\rangle$ with $\mathcal{M}$, prob. of outcome $j$ is:

$$\mathrm{Prob}(i \,|\, |\psi\rangle) := \langle\psi| M_i |\psi\rangle$$

( The Born rule. )

Back to global phases: $|\psi\rangle \sim |\phi\rangle \left(= e^{i\alpha}|\psi\rangle\right)$

$$\mathrm{Prob}(j \,|\, |\phi\rangle) = \mathrm{Prob}(j \,|\, e^{i\alpha}|\psi\rangle) = \left(e^{-i\alpha}\langle\psi|\right) M_j \left(e^{i\alpha}|\psi\rangle\right)$$

$$= \cancel{e^{-i\alpha} e^{i\alpha}} \cdot \langle\psi| M_j |\psi\rangle = \mathrm{Prob}(j \,|\, |\psi\rangle)$$

Ex: ONB measurements:

$$\mathrm{ONB} = \{ |i\rangle \}_i$$

$$\Downarrow$$

$$\text{Projectors} := \{ M_i = |i\rangle\langle i| \}_i \quad \text{and} \quad \sum_i |i\rangle\langle i| = I$$

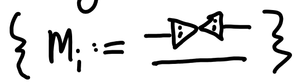
$$M_i^2 = M_i M_i = |i\rangle \underbrace{\langle i|i\rangle}_{1} \langle i| = |i\rangle\langle i| = M_i = M_i^\dagger$$

$$\mathrm{Prob}(j \,|\, |\psi\rangle) = \langle\psi| m_j |\psi\rangle = \langle\psi| \overbrace{|j\rangle\langle j|}^{m_j} |\psi\rangle$$

$$= \overline{\langle j|\psi\rangle} \cdot \langle j|\psi\rangle$$

$$= \| \langle j|\psi\rangle \|^2$$

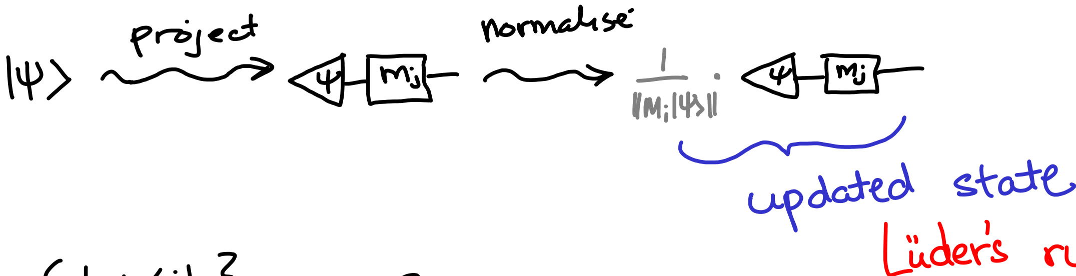
Ex: Measuring 1 system:



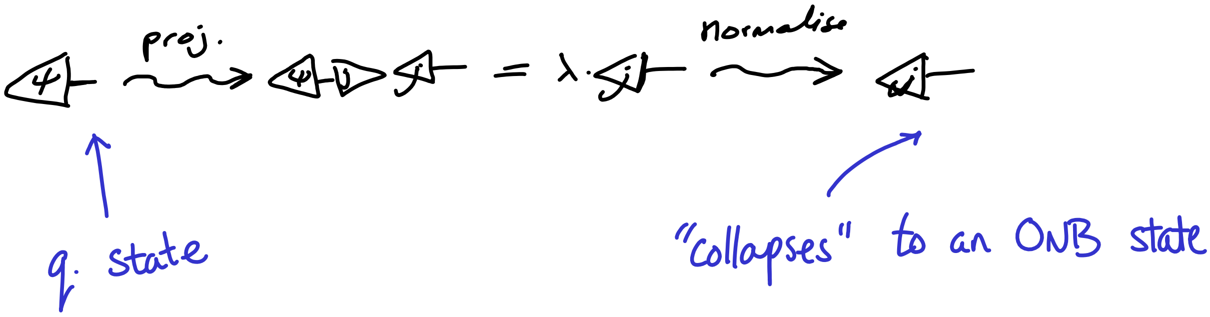

Ex: Distinguishing subspaces: $\mathrm{Span}\{|0\rangle, |1\rangle\} \leq \mathbb{C}^3$ vs. $\mathrm{Span}\{|2\rangle\} \leq \mathbb{C}^3$

$$\mathcal{M} = \{ M_1 = |0\rangle\langle 0| + |1\rangle\langle 1| ,\ M_2 = |2\rangle\langle 2| \}$$

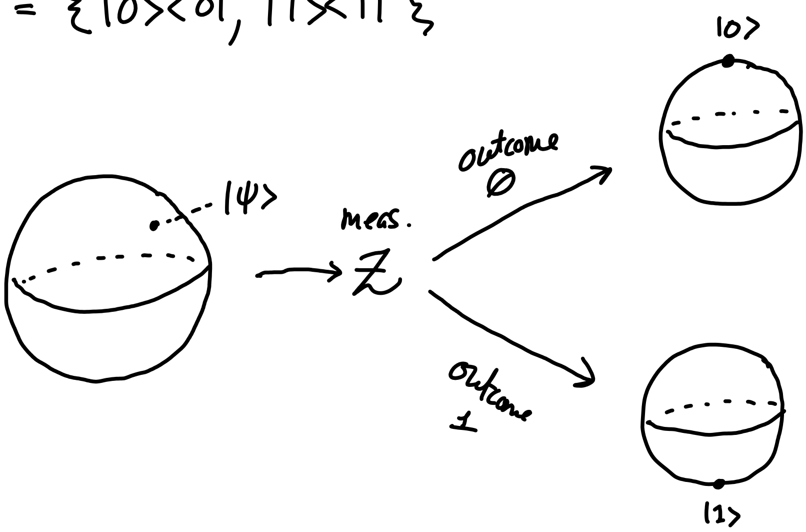
## 2. Post-measurement state:




If $\mathcal{M} = \{ |j\rangle\langle j| \}_j$ ONB meas:



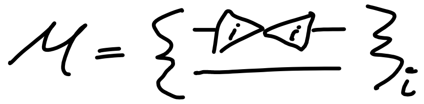

Ex $\quad \mathcal{Z} = \{ |0\rangle\langle 0|, |1\rangle\langle 1| \}$

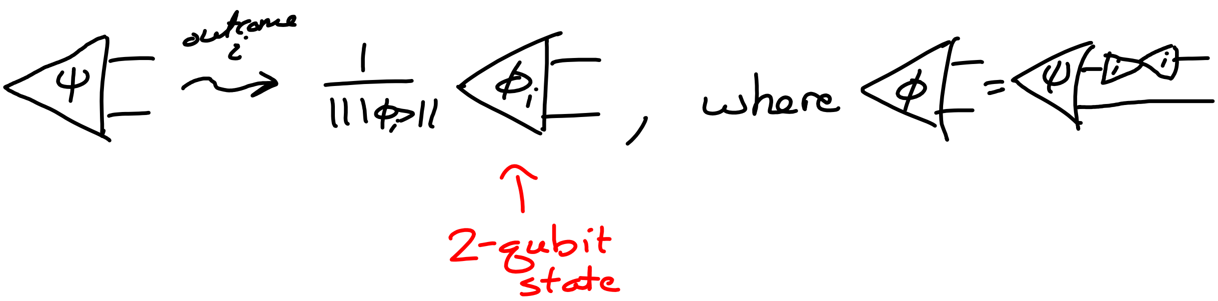



$$\mathrm{Prob}(0 \,|\, |\psi\rangle) = \langle \psi | 0\rangle\langle 0 | \psi\rangle = \| \langle 0 | \psi\rangle \|^2$$

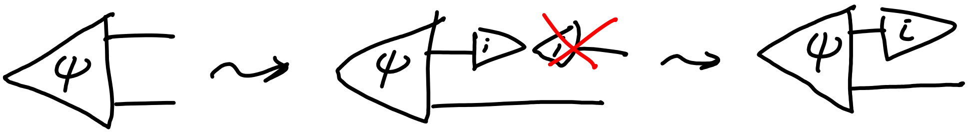
$$\mathrm{Prob}(1 \,|\, |\psi\rangle) = \| \langle 1 | \psi\rangle \|^2$$

**Ex** Measuring a subsystem, e.g.



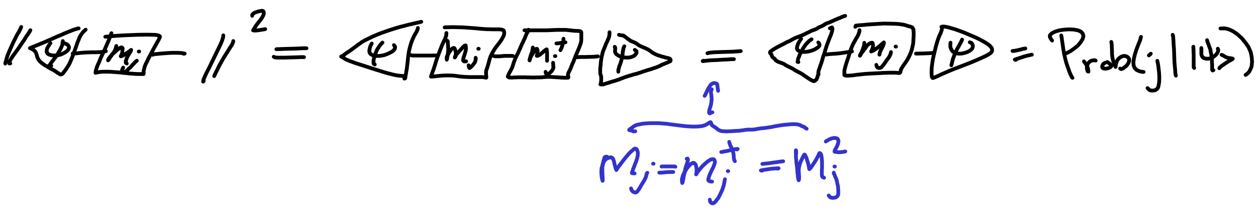

The first qubit is not entangled, so we can ignore it and write the state of the 2nd qubit:



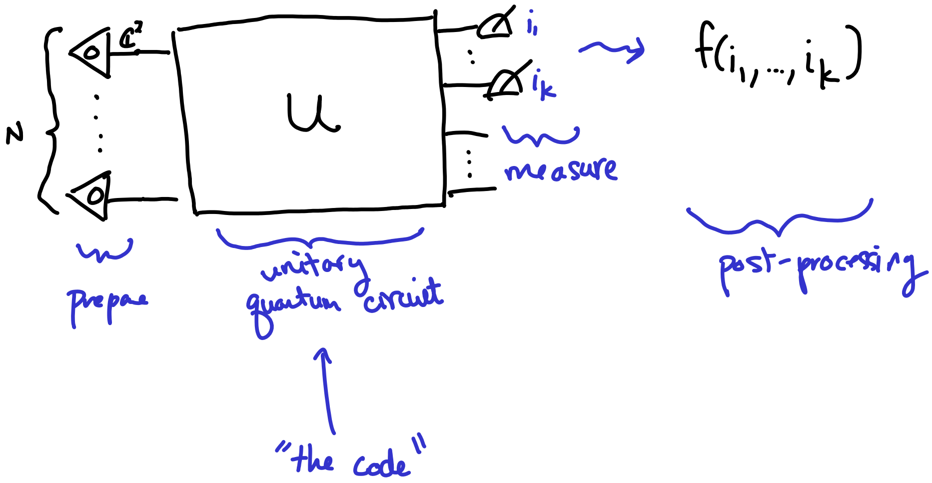

* n.b. this is only allowed because the qubits are not entangled. If they are entangled, this results in a mixed state, cf. Section 2.7.1 of the Crow book.

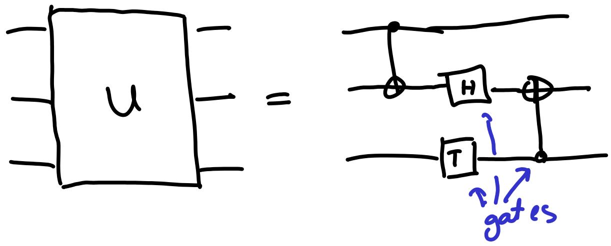
**Remark** Sometimes we don't normalise , because it's norm$^2$ contains some useful info: the Born rule probability!





# The Quantum Circuit Model.




CNOT (0,1)
H(1)
T(2)
CNOT (2,1)
...

Q: Where do they come from?

(I) classical computations:

$$\underbrace{\pi : \mathbb{B}^n \to \mathbb{B}^n}_{\text{reversible fn (aka permutation)}} \rightsquigarrow \underbrace{U_\pi :: |\vec{x}\rangle \mapsto |\pi(\vec{x})\rangle}_{\text{unitary}}$$

$\underline{\text{Ex}}$ $\quad \text{NOT} : \mathbb{B} \to \mathbb{B} \rightsquigarrow X :: \begin{array}{l} |0\rangle \mapsto |1\rangle \\ |1\rangle \mapsto |0\rangle \end{array}$

$$\text{CNOT} : \mathbb{B}^2 \to \mathbb{B}^2 \rightsquigarrow \text{CNOT} :: |x, y\rangle \mapsto |x, x \oplus y\rangle$$

$$f : \mathbb{B}^n \to \mathbb{B} \quad \rightsquigarrow \quad U_f : (\mathbb{C}^2)^{\otimes n+1} \to (\mathbb{C}^2)^{\otimes n+1}$$

any function

$$U_f :: |\vec{x}, y\rangle \mapsto |\vec{x}, f(\vec{x}) \oplus y\rangle$$

unitary ("Bennett trick")

**Thm** For any $f$, $U_f$ is unitary.

**Pf** First, note $\pi(\vec{x}, y) := (\vec{x}, f(\vec{x}) \oplus y)$ is a permutation, because $\pi^{-1} = \pi$ :

$$\pi(\pi(\vec{x}, y)) = \pi(\vec{x}, f(\vec{x}) \oplus y)$$
$$= (\vec{x}, f(\vec{x}) \oplus f(\vec{x}) \oplus y)$$
$$= (\vec{x}, y).$$

Then $U_f :: |\vec{x}, y\rangle \mapsto |\pi(\vec{x}, y)\rangle$ is unitary. $\boxtimes$

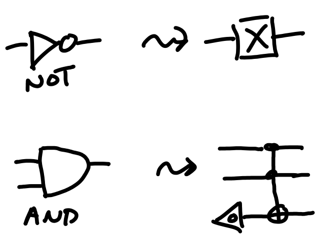
Ex: $\mathrm{AND} : \mathbb{B}^2 \to \mathbb{B}$
$\mathrm{AND}(x, y) := xy$
$\rightsquigarrow$ $\mathrm{TOF} :: |x, y, z\rangle \mapsto |x, y, (xy) \oplus z\rangle$

Toffoli / CCNOT

* classical (reversible) circuits $\quad C \rightsquigarrow C' \rightsquigarrow U$

$C$: AND + NOT

$C'$: Toffoli + NOT + ancillas




*

# Lecture 7

## (II) "quantum tricks"

### (a) change of basis:

$-\boxed{H}- \; := \; \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

Hadamard

$H|0\rangle = |+\rangle := \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
$H|1\rangle = |-\rangle := \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

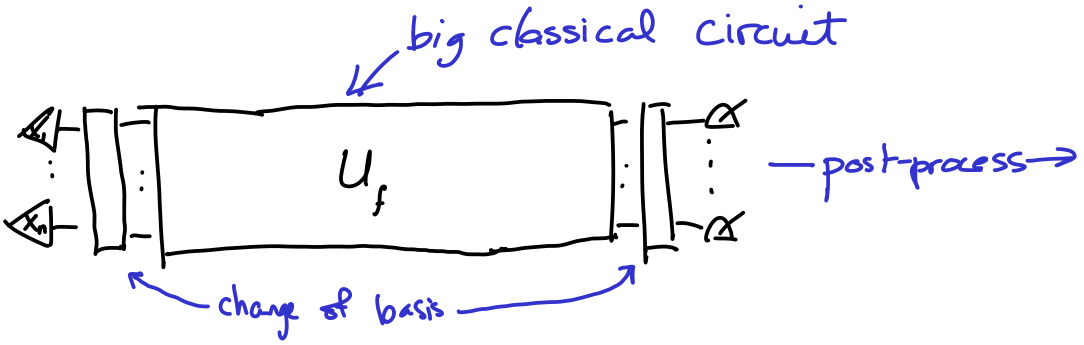
OR MORE GENERALLY: $\mathbb{C}^N - \boxed{F} - \mathbb{C}^N$ where $F_j^k = \frac{1}{\sqrt{N}}\,\omega^{j\cdot k}$, $\omega := e^{2\pi i/N}$

Fourier xform

$\left(\text{n.b.} \quad H_j^k = \frac{1}{\sqrt{2}}(-1)^{j\cdot k}, \quad \omega = e^{2\pi i/2} = e^{\pi i} = -1\right)$

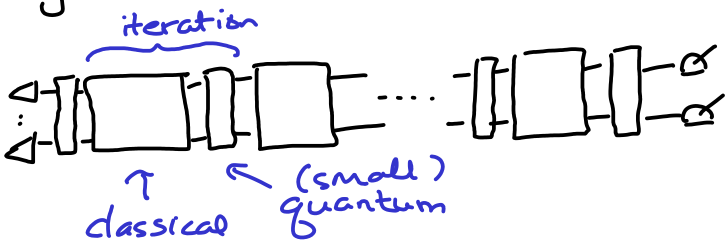
- Most quantum algorithms fall into a handful of forms:

• "Oracle style" algorithms:




- Proof of concept: Deutsch-Jozsa, Simons
- Factoring (to factor N, we use $f(a) = x^a \bmod N$ + q. period finding)
- Hidden subgroup (for any $G \xrightarrow{\boxed{f}} X = G \xrightarrow{\boxed{f}} G/H \xrightarrow{\boxed{i}} X$, where $G, H$ Abelian groups, $i$ injective, we can find $H$.)

- Grover-style:

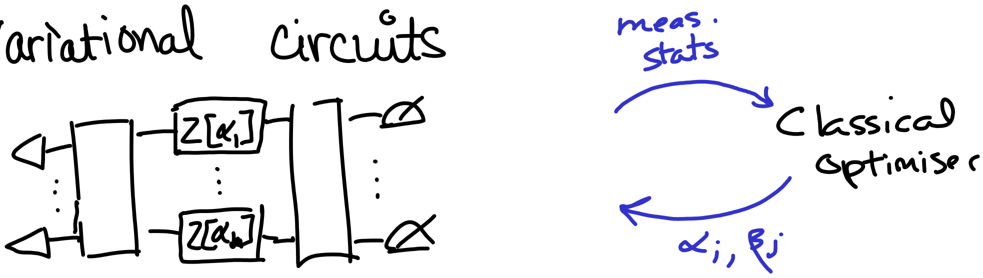



  - * Grover search
  - * amplitude amplification
  - * quantum walks

- Hamiltonian simulation (wk 7)

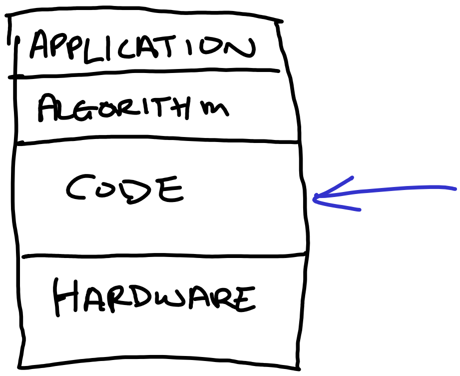
- Hybrid / quantum ML

Variational circuits




$$Z[\alpha] :: \begin{array}{l} |0\rangle \mapsto |0\rangle \\ |1\rangle \mapsto e^{i\alpha}|1\rangle \end{array}$$

"Stack"



# Quantum circuit problems

**Problem:** (synthesis) Given a (high-level) description of a computation/unitary $U$, build a circuit that does $U$.

**Problem** (optimisation) given a circuit $C$ that does $U$, find a smaller $C'$ that also does $U$.

**Problem** (classical simulation) given $C$ that does $U$, and an input $|\psi\rangle$ either:

Strong simulation $\rightarrow$ * compute measurement probabilities for $U|\psi\rangle$, or

weak simulation $\rightarrow$ * Sample measurement outcomes for $U|\psi\rangle$

# ZX-diagrams

- are a tool for reasoning about circuits (and more!)

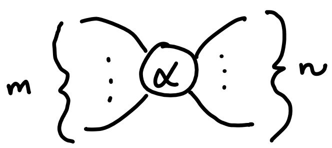
**Perspective 1:** ZX-diagrams are "circuits" made of spiders.

$$Z[\alpha]_m^n : \underbrace{(\mathbb{C}^2)^{\otimes m}}_{\mathbb{C}^{2^m}} \rightarrow \underbrace{(\mathbb{C}^2)^{\otimes n}}_{\mathbb{C}^{2^n}}$$

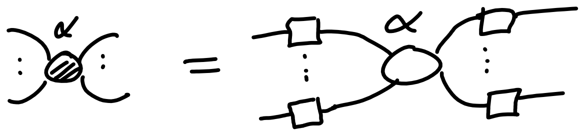
$$Z[\alpha]_m^n = |00..0\rangle\langle 00..0| + e^{i\alpha}|11..1\rangle\langle 11...1| \longleftrightarrow \begin{pmatrix} 1 & & & 0 \\ & 0 & & \\ & & \ddots & \\ 0 & & 0 & e^{i\alpha} \end{pmatrix}$$

ie. $\begin{cases} |00\ldots0\rangle \longmapsto |00\ldots0\rangle \\ |11\ldots1\rangle \longmapsto e^{i\alpha}|11\ldots1\rangle \end{cases}$

rank 2
(usually not unitary!)

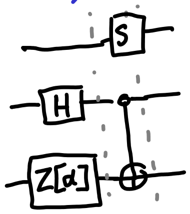


$$X[\alpha]_m^n = |{+}{+}\ldots{+}\rangle\langle{+}{+}\ldots{+}| + e^{i\alpha}|{-}{-}\ldots{-}\rangle\langle{-}{-}\ldots{-}|$$



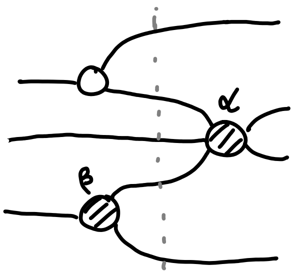
where $\square = \boxed{H} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$

For circuits, we can compute the linear map as:



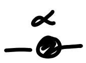
$$(S \otimes CNOT)(I \otimes H \otimes Z[\alpha])$$

Similarly for ZX-diagrams:

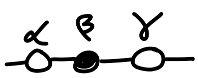


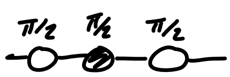
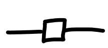
$$(I \otimes X[\alpha]_3^2 \otimes I)(Z[0]_1^2 \otimes I \otimes X[\beta]_1^2)$$

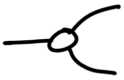
 $= Z[\alpha] = \begin{pmatrix}1 & 0\\ 0 & e^{i\alpha}\end{pmatrix} \leftarrow$ Z phase gate.

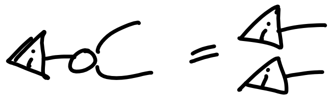
 $= X[\alpha] \leftarrow$ X phase gate

<u>Thm</u> (Euler decomposition) For any single-qubit unitary $U$, $\exists$ angles $\alpha, \beta, \gamma, \theta$ s.t.:

$U = e^{i\theta} \cdot$ 

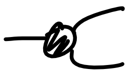
<u>Ex</u> $\boxed{H} = e^{-i\pi/4}$  $=:$ 

 $= |00\rangle\langle 0| + |11\rangle\langle 1|$

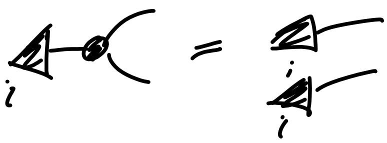
"copies Z-basis" 

 $= \langle 0| + \langle 1|$

"deletes Z-basis"  $= 1$

 $= |++\rangle\langle +| + |--\rangle\langle -|$

 $= |+\rangle + |-\rangle$

  $= 1$

(nb. $\{|x_0\rangle, |x_1\rangle\} = \{|+\rangle, |-\rangle\} = \{$  $\}$)

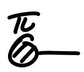
X-basis

# Basis states in ZX:

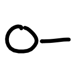
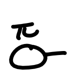
 $= |+\rangle + |-\rangle = \frac{1}{\sqrt{2}}\left[|0\rangle + |1\rangle + |0\rangle - |1\rangle\right]$

$= \frac{2}{\sqrt{2}}|0\rangle = \sqrt{2}\cdot|0\rangle$

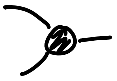
Z basis states

 $= |+\rangle + e^{i\pi}|-\rangle = \frac{1}{\sqrt{2}}\left[|0\rangle + |1\rangle - |0\rangle + |1\rangle\right]$

$= \sqrt{2}\cdot|1\rangle$

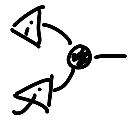
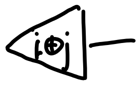
Similarly:  $= \sqrt{2}\cdot|+\rangle$,  $= \sqrt{2}\cdot|-\rangle$

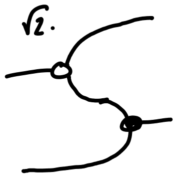
X-basis states

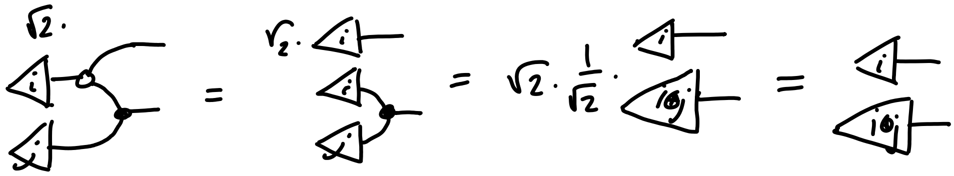
 $= |+\rangle\langle ++| + |-\rangle\langle --| = \ldots$

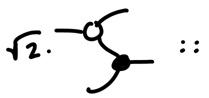
$$= \frac{1}{\sqrt{2}}\left(|0\rangle\langle 00| + |0\rangle\langle 11| + |1\rangle\langle 01| + |1\rangle\langle 10|\right)$$

$$= \frac{1}{\sqrt{2}} \cdot \text{XOR}$$

i.e.:  $= \frac{1}{\sqrt{2}}$ 

<u>Ex</u> CNOT = 



So:  $:: |i,j\rangle \mapsto |i, i\oplus j\rangle$

<u>Thm</u> (universality) any n-qubit unitary can be constructed using only:
- single qubit gates
- CNOT

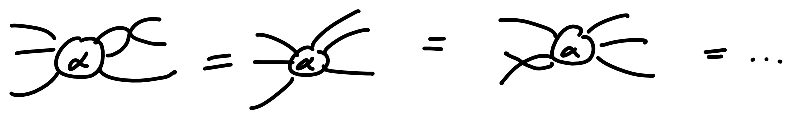
<u>Cor</u> Any n-qubit unitary can be constructed as a ZX-diagram.

# ZX Rewriting

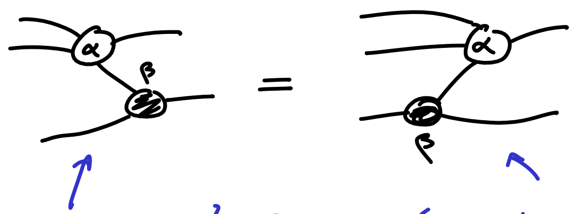
ZX diagrams have "extreme" OCM.

They are invariant under:

- SWAPPING SPIDER-LEGS:



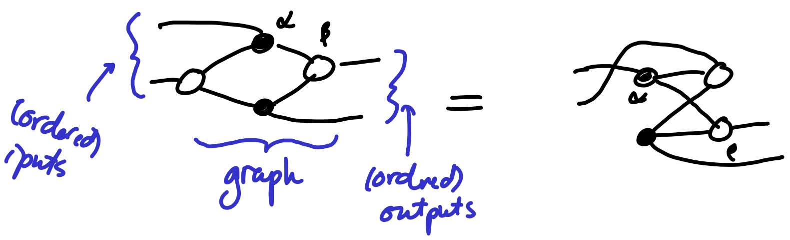
- CHANGING DIRECTION



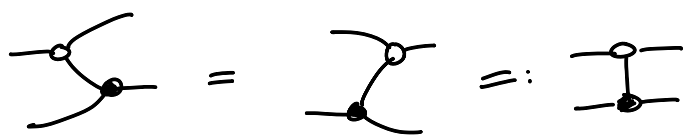
$$(I\otimes X[\beta]^1_2)(Z[\alpha]^2_2\otimes I) = (Z[\alpha]^1_3\otimes I)(I\otimes I\otimes X[\beta]^2_1)$$

$\Rightarrow$ they can be treated as <u>undirected graphs</u> (w lists of inputs & outputs)

eg.



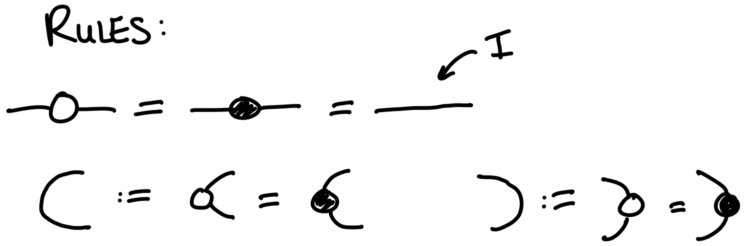

eg. CNOT =



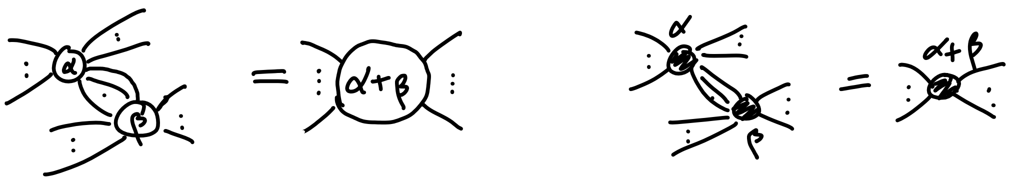
# The ZX-calculus

:= a set of equations for ZX-diagrams

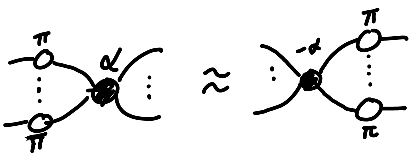
(0) "WIRE" RULES:



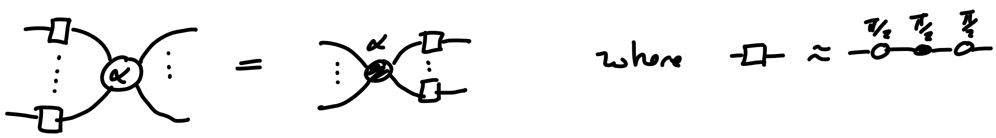

(1) SPIDER-FUSION



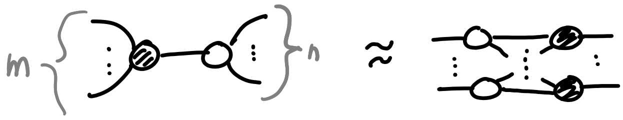

(2) π-rule*:




(3) COLOUR CHANGE:

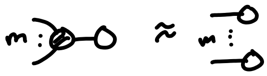


## (4) Strong complementarity



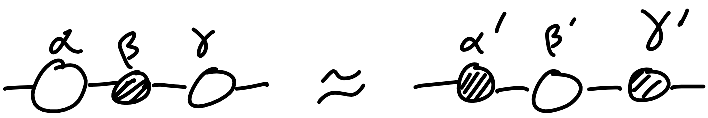

Special cases: $m=0 \Rightarrow$ 


COPY RULES

$n=0 \Rightarrow$ 


$m=2, n=2 \Rightarrow$ 


## (EU) rule:

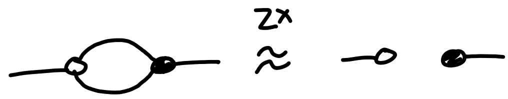



$$\alpha' = \alpha'(\alpha, \beta, \gamma)$$
$$\beta' = \beta'(\alpha, \beta, \gamma)$$
$$\gamma' = \gamma'(\alpha, \beta, \gamma)$$

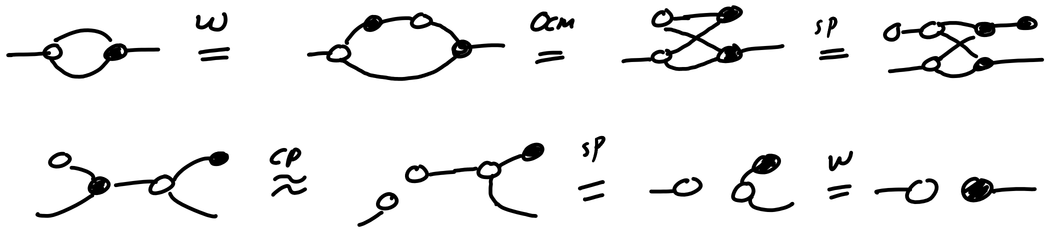
trig. fns.

# Rewriting Examples

**Thm** (COMPLEMENTARITY)

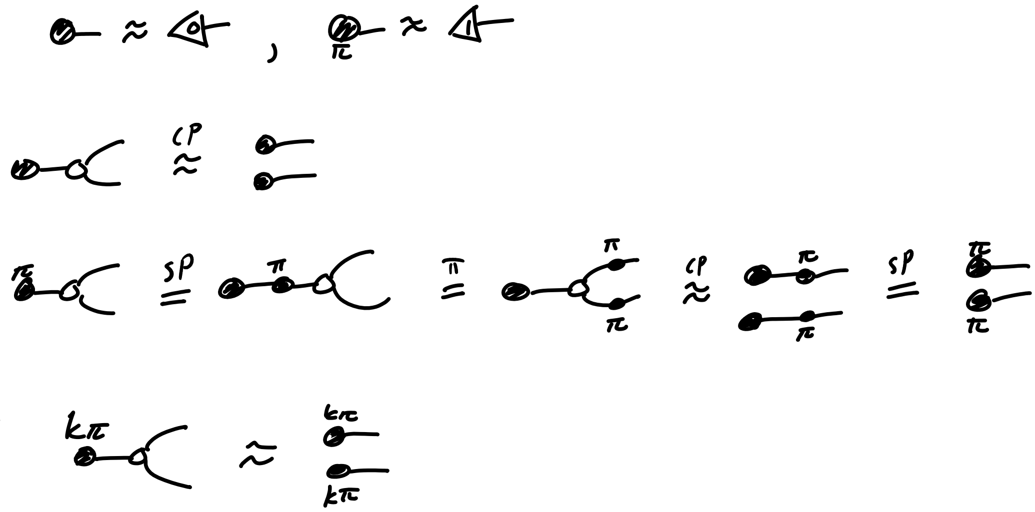


**Pf**

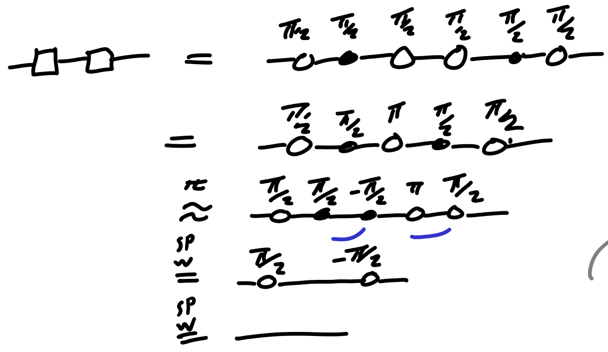


∎

**Ex** Basis state copy:

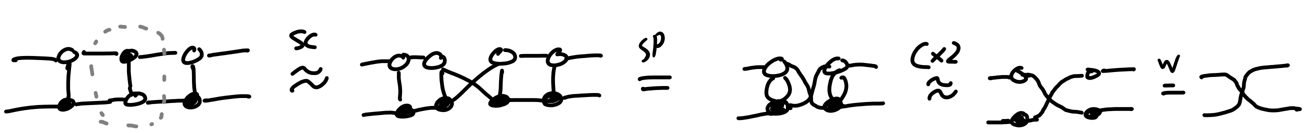


**Ex** HH



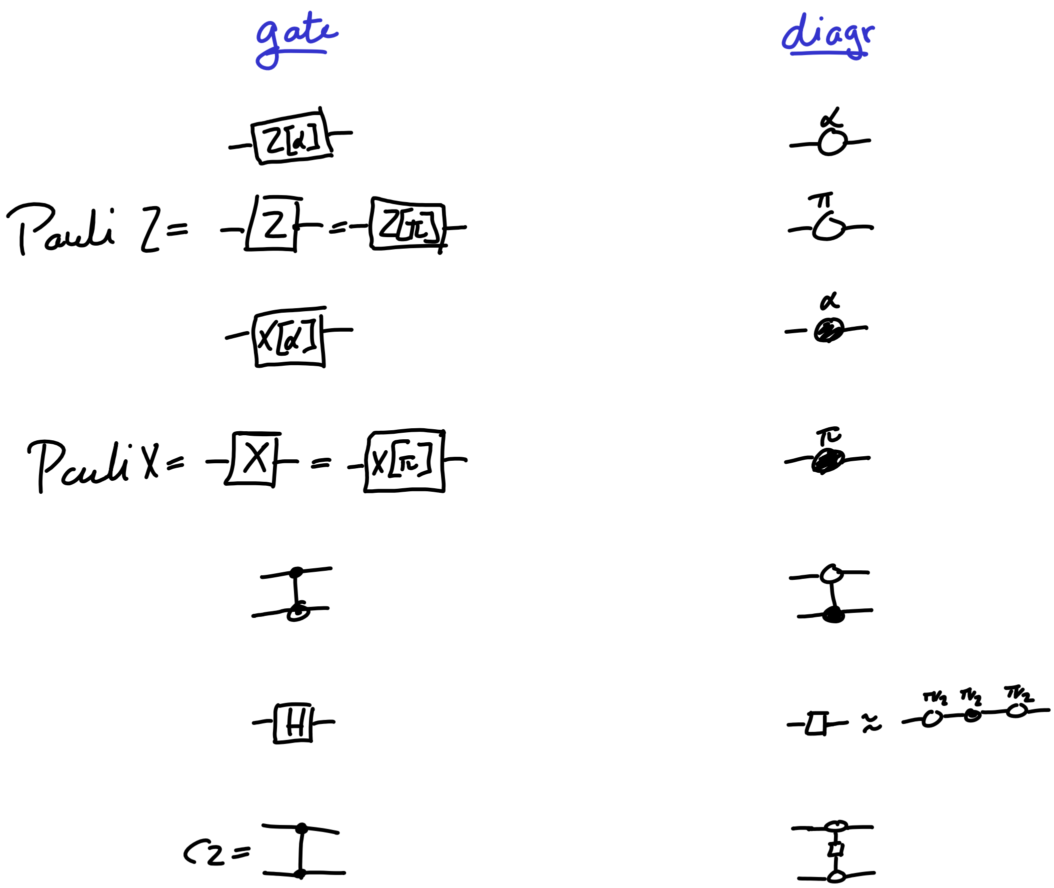
(because $\pi + \frac{\pi}{2} \equiv -\frac{\pi}{2} \pmod{2\pi}$)

**Ex** 3CNOT:

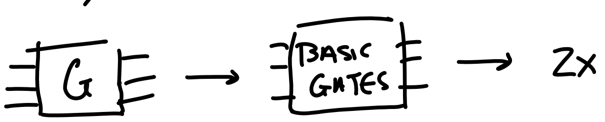


# ZX dictionary

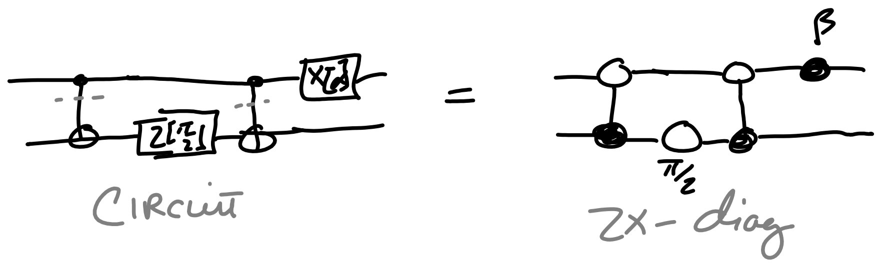
Circuits ⟶ ZX-diagrams




other stuff
(e.g. CCZ, Tof, ...)




Ex



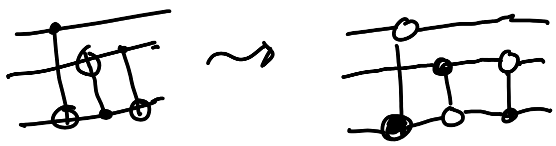
# Lecture 8

## CNOT Circuits & Phase Free ZX Diagrams

CIRCUITS MADE JUST OUT OF 

ZX-DIAGS MADE OUT OF  AND 

**Prop** Any CNOT circuit is equal to a phase free ZX-diagram.



Q: What about the converse?

Today: (Unitary) phase-free ZX-diags $\rightsquigarrow$ CNOT circuits.

$$\mathrm{CNOT}\,|x,y\rangle \mapsto |x, x\oplus y\rangle$$

$$\mathrm{CNOT}\,|x,y\rangle \mapsto |f_1(x,y), f_2(x,y)\rangle \quad \text{where} \quad \begin{cases} f_1(x,y) = x \\ f_2(x,y) = x\oplus y \end{cases}$$

**Def** A function of the form $f(x_1,\dots,x_n) = x_{i_1} \oplus \dots \oplus x_{i_k}$ is called a parity map.

# Parities.

<u>Def</u> The field $\mathbb{F}_2$ has elements $\{0,1\}$ where:

$$x \cdot y := x \wedge y \qquad x + y = x \oplus y \qquad (\text{ie. } x+y \bmod 2)$$

Sometimes we call some $x \in \mathbb{F}_2$ a parity.

$$\mathrm{par}(\vec{b}) = \overset{\text{in } \mathbb{F}_2}{\sum_i} b_i$$

$\mathrm{par}(\vec{b}) = 0$ means $\vec{b}$ has an <u>even</u> # of <u>1's</u>

$\mathrm{par}(\vec{b}) = 1$ means <u>odd</u> #.

Parities for subsets of bits:

$$\begin{pmatrix} 1 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \end{pmatrix} = b_1 \oplus b_3 \oplus b_4$$

Multiple parities at once:

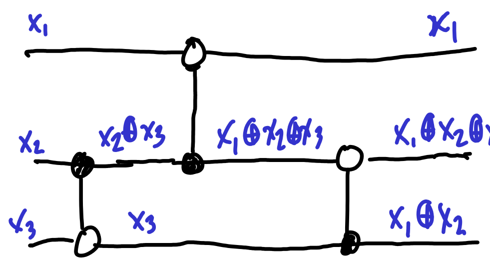
$$\underbrace{\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}}_{\text{parity matrix.}} \begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \end{pmatrix} = \begin{pmatrix} b_1 \oplus b_3 \oplus b_4 \\ b_2 \oplus b_3 \\ b_1 \oplus b_4 \\ b_4 \end{pmatrix}$$

**Thm** The action of a CNOT circuit on basis elements is defined by an invertible parity matrix:

$$C|b_1,\dots,b_n\rangle = |c_1,\dots,c_n\rangle$$

where
$$P\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}.$$

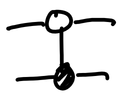
e.g.

$C =$ 


$$C|x_1, x_2, x_3\rangle = |x_1, x_1 \oplus x_2 \oplus x_3, x_1 \oplus x_2\rangle$$

$$\underbrace{\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}}_{P}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \oplus x_3 \\ x_1 \oplus x_2 \end{pmatrix}$$

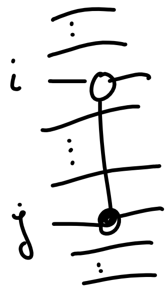
Special case: Single CNOT.



$$|x,y\rangle \mapsto |x, x \oplus y\rangle$$

$$\underbrace{\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}}_{P}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ x \oplus y \end{pmatrix}$$

More generally:




$$\longleftrightarrow \quad \begin{array}{c c} j \rightarrow & \begin{pmatrix} 1 & & & & \\ & 1 & & & \\ & & 1 & & \\ & \square & & 1 & \\ & & & & 1 \end{pmatrix} \\ & \quad\; \uparrow \\ & \quad\; i \end{array} = \underbrace{E^{ij}}_{\text{elementary matrix}}$$

$$E^{ij} A = \underset{\substack{\uparrow \\ \text{row } j = \text{row } j + \text{rows } i}}{A'}$$

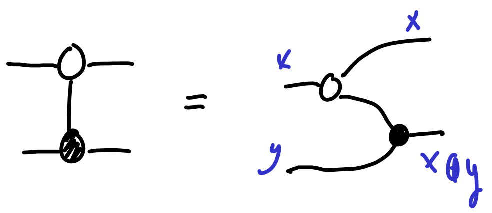
$$A E^{ji} = \underset{\substack{\uparrow \\ \text{col } j := \text{col } i + \text{col } j}}{A'}$$

Suppose $P E^{i_1 j_1} \cdots E^{i_k j_k} = I$,

then $\underset{\substack{\uparrow \\ \text{parity matrix}}}{P} = \underbrace{E^{i_k j_k} \cdots E^{i_1 j_1}}_{\text{CNOT gates!}}$

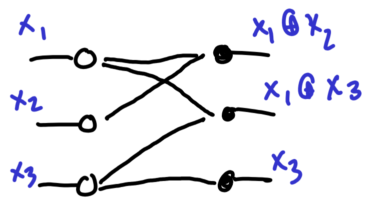
Algorithm: CNOT-SYNTH:

* Start w/ Parity matrix $P$, empty circ. $C$.
* Do Gauss-Jordan reduction of columns of $P$.
  - whenever an elem. col operation $E^{ji}$ is applied, append $CNOT^{ji}$ to $C$.
* $C$ now implements $P$.



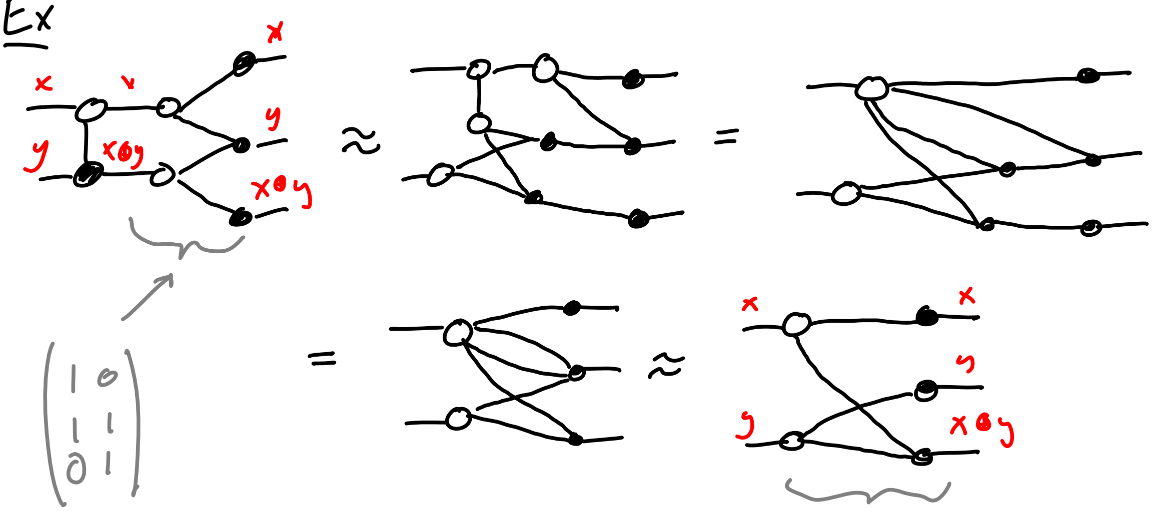

More general parity maps:

$$P = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_1 \oplus x_2 \\ x_1 \oplus x_3 \\ x_3 \end{pmatrix}$$



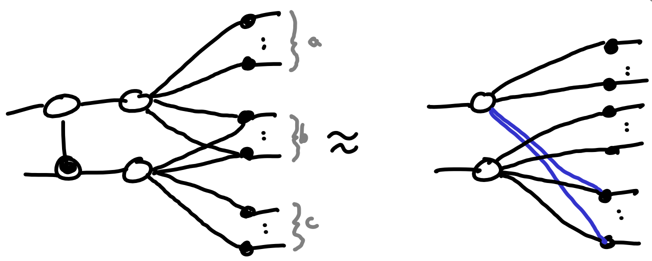

⟵ implements $P$!

## Ex




$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{pmatrix}$$

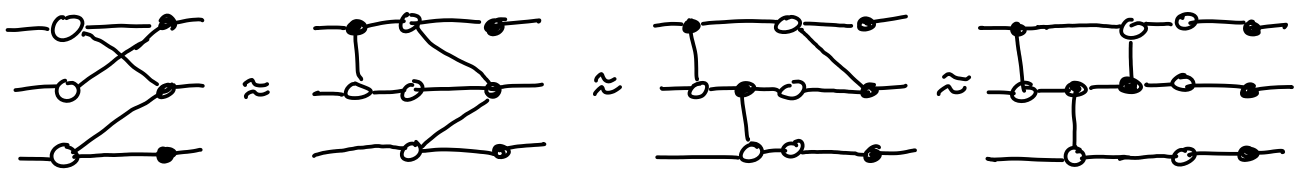
## Lem 4.2.3




$$\begin{array}{c} a\{ \\ \\ b\{ \\ \\ c\{ \end{array} \begin{pmatrix} 1 & 0 \\ \vdots & \vdots \\ 1 & 0 \\ 1 & 1 \\ \vdots & \vdots \\ 1 & 1 \\ 0 & 1 \\ \vdots & \vdots \\ 0 & 1 \end{pmatrix} \underset{C_1 = C_1 + C_2}{\overset{C_1 = C_1 + C_2}{\rightleftarrows}} \begin{pmatrix} 1 & 0 \\ \vdots & \vdots \\ 1 & 0 \\ 0 & 1 \\ \vdots & \vdots \\ 0 & 1 \\ 1 & 1 \\ \vdots & \vdots \\ 1 & 1 \end{pmatrix}$$

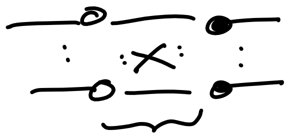
## Ex

$$\begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{C_2 = C_2 + C_1} \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{C_3 = C_3 + C_2} \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{C_1 = C_1 + C_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$



**Def** A spider is called
* an *input* spider if it is conn. to an input
* an *output* spider ... output
* an *interior* spider otherwise.

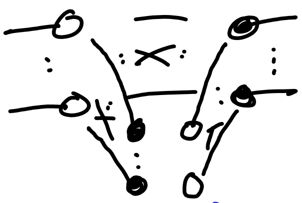
**Def** A phase-free ZX-diagram is in *parity normal form*
- every Z spider is conn. to exactly 1 input
- every X ... ... output
- no wires between spiders of the same type
- no parallel wires



P parity matrix.

**Def** A phase-free ZX diag. is in *generalised parity form* if:

1. every input is conn. to a Z spider
2. every output ... X spider
3. no wires Z-Z or X-X
4. no parallel wires
5. no wires btw interior Z-spiders and interior X-spiders.



non-output X

non-input Z

## Algorithm 2: Reduction to generalised PNF.

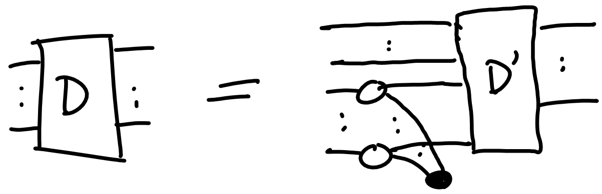
1. apply (sp), (comp), and $\circ = \bullet = 2$ as much as possible.
2. try to apply (sc) to a pair $\circ\!-\!\bullet$ where:
   - $\circ$ is not an input
   - $\bullet$ is not an output
3. if step 2 applied (sc), goto step 1. otherwise:
4. use (id) to make sure every input is conn. to Z & output conn. to X.

**Thm** Alg 2 terminates efficiently in generalised PNF.

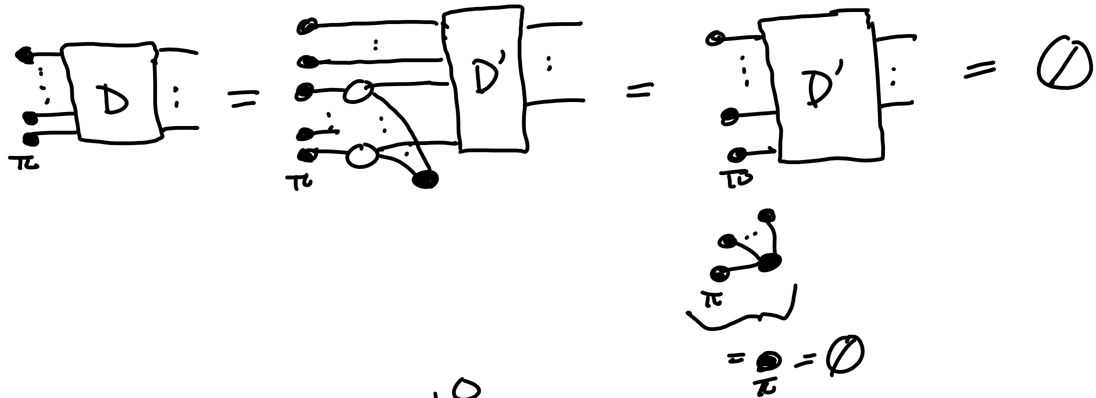
(sketch)
**Pf** • Each iteration of steps 1-3 removes non-input Z spiders (and non-output X-spiders) without making new ones.
$\Rightarrow$ # iterations bounded by # of spiders
• after the loop, conds 3-5 are satisfied.
• after step 4, conds 1-2 are satisfied. ∎

**Prop** If D is unitary and in generalised PNF, then it is in PNF.

Pf If D has an interior X spider, then:




So:




So, there exists $|\psi\rangle^{\neq 0}$ s.t $D|\psi\rangle = \emptyset$. But:

$D^\dagger D|\psi\rangle = |\psi\rangle \neq 0$. ↯

So D has no interior X-spiders. Similarly,

D has no
- Z-sp's connected to >1 input
- interior X sp's
- X-sp's connected to >1 output. $\boxed{Z}$

$$\text{Unitary Phase-free ZX} \overset{*}{\Longrightarrow} \text{PNF} \Longrightarrow \text{CNOT circuit}.$$