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>.

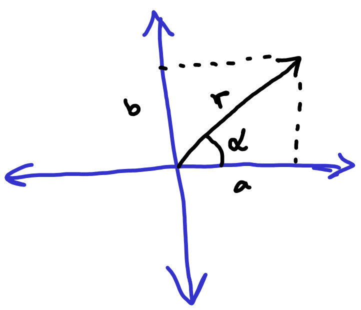
(M) <u>Measurement</u> probabilities come from the Born rule.

(*) Complex numbers can be written in:

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

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

PROPERTIES

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

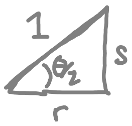
Def A quantum pure state is a normalised vector ($\langle\psi|\psi\rangle = 1$) $|\psi\rangle \in \mathcal{H}$, upto a global phase: $|\psi\rangle \sim e^{i\alpha} \cdot |\psi\rangle$.

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 $|\psi\rangle \in \mathbb{C}^2$.

$$|\psi\rangle = re^{i\beta}|0\rangle + se^{i\gamma}|1\rangle$$

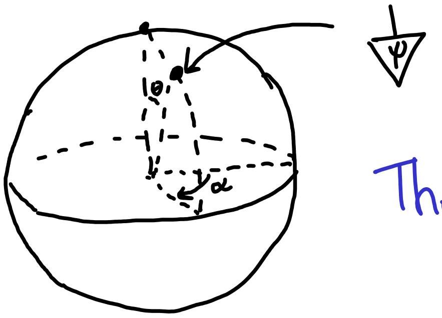
ψ normalised $\iff$ $r^2 + s^2 = 1$ $\iff$ for some θ: $r = \cos\frac{\theta}{2}$ $\quad s = \sin\frac{\theta}{2}$



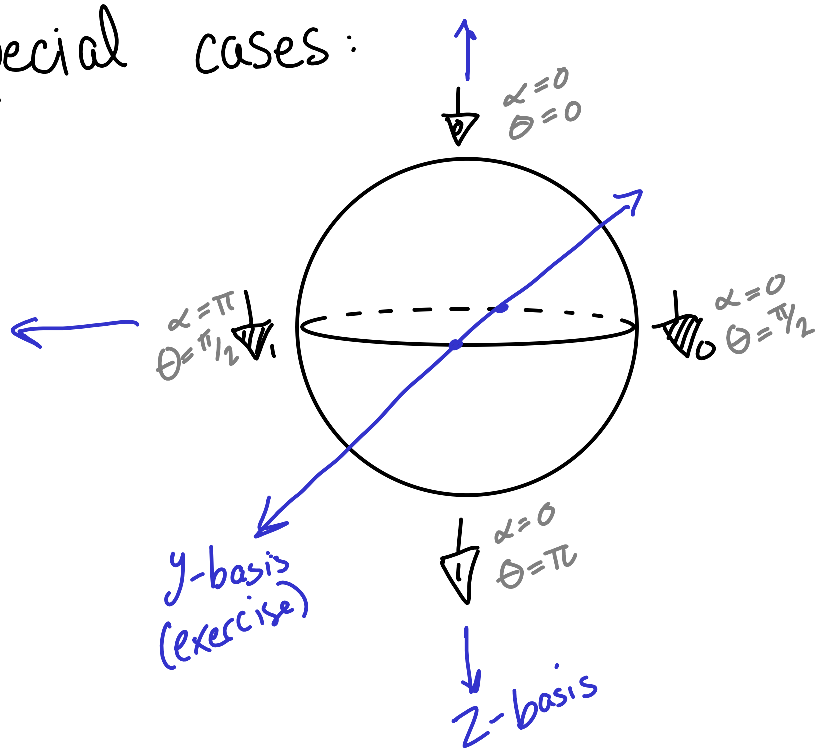
$$|\psi\rangle = \cos\frac{\theta}{2} e^{i\beta}|0\rangle + \sin\frac{\theta}{2} e^{i\gamma}|1\rangle$$

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

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



Special cases:



Compound systems

... are described by the tensor product:

$\mathcal{H}$, $\mathcal{K}$ $\rightsquigarrow$ $\mathcal{H} \otimes \mathcal{K}$

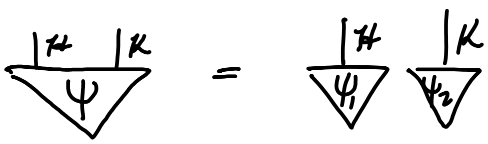
d-dim'l, e-dim'l $\qquad$ d·e dim'l

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

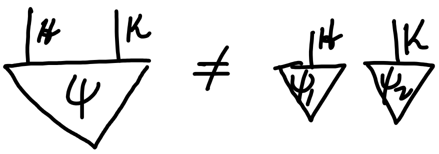
$$(\mathbb{C}^2)^{\otimes n} := \underbrace{\mathbb{C}^2 \otimes \ldots \otimes \mathbb{C}^2}_{n}$$

$N = 2^n$-dim'l

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



separable

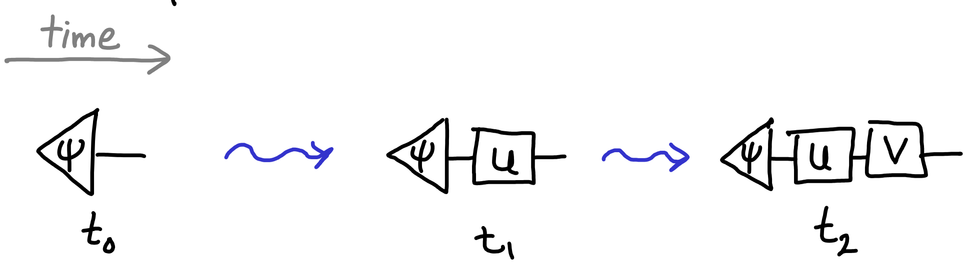


non-separable / entangled

Unitaries

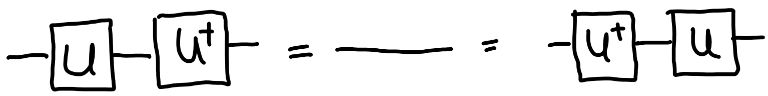
Time evolution in QT is:

* linear
* preserves normalisation.



the same

Thm 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:

$$i\hbar \frac{d}{dt} |\psi_t\rangle = H |\psi_t\rangle$$

Hamiltonian ← where the physics lives!

$H = H^\dagger$

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

matrix exponential

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

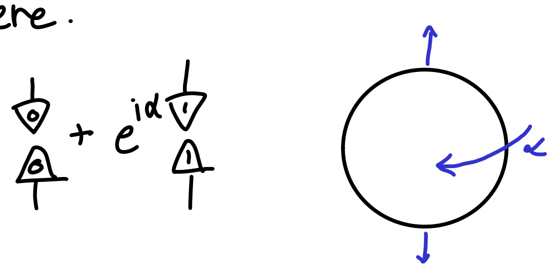
<u>BUT</u> for us the only important thing is:

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

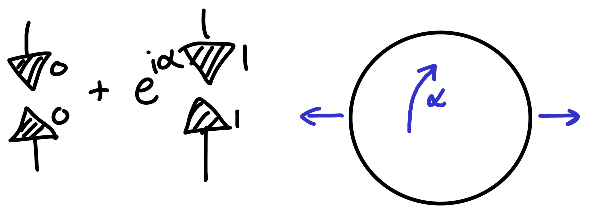
$U \longleftrightarrow$ "evolving for a fixed amount of time t"

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

e.g. $Z[\alpha] =$



$X[\alpha] =$

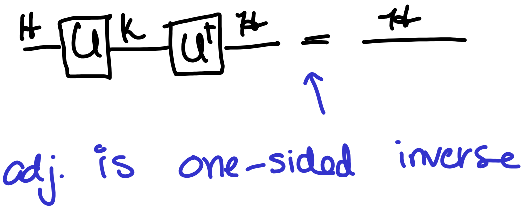


<u>Any</u> unitary can be written:

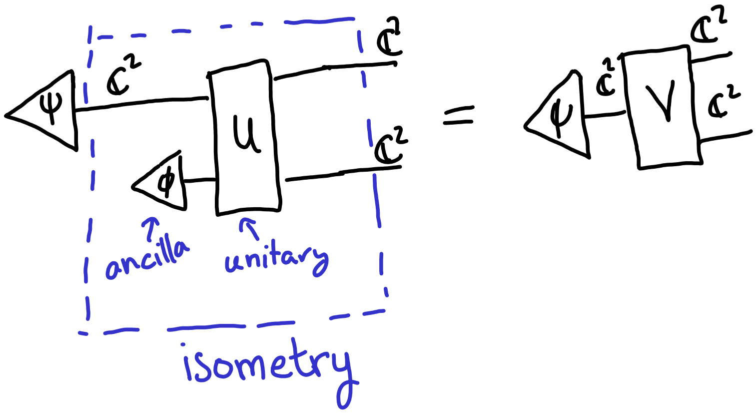
$$-\boxed{U}- = e^{i\theta} -\boxed{Z[\alpha]}-\boxed{X[\beta]}-\boxed{Z[\gamma]}-$$

Euler decomposition.

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



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>.

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

A projector spits a space into two orthogonal pieces:

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

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

(identity matrix → I)

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

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:

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

"The Born rule."

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

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

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

Ex: ONB measurements:

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

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

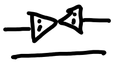
$$M_i^2 = M_i M_i = |i\rangle\underbrace{\langle i|i\rangle}_{1}\langle i| = |i\rangle\langle i| = M_i = M_i^\dagger$$

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

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

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

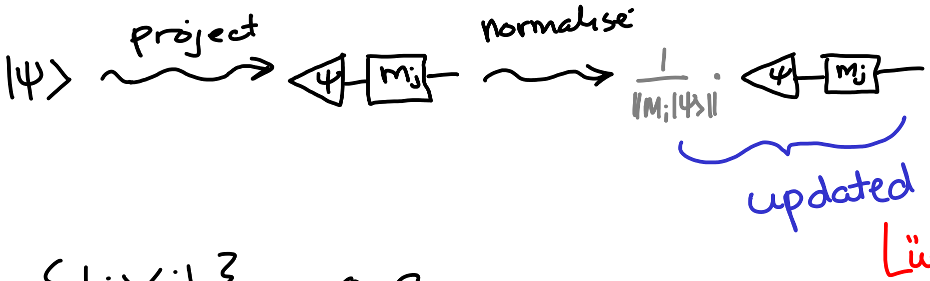
Ex: Measuring 1 system:

$\{ M_i :=$  $\}$

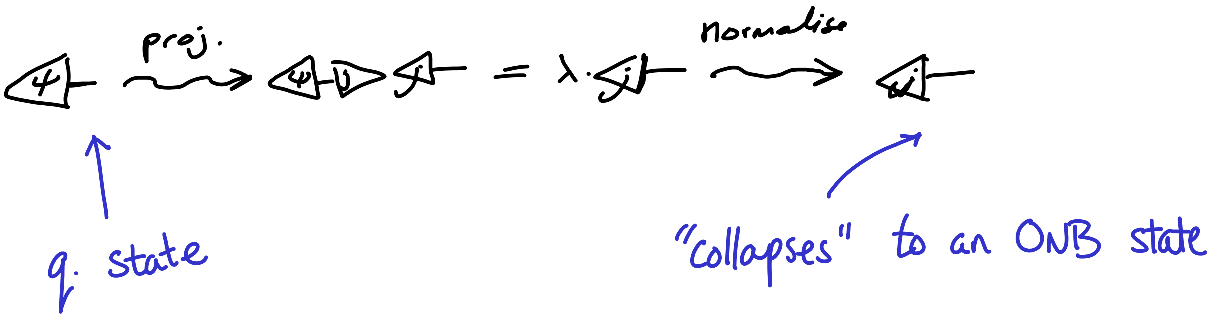
Ex: Distinguishing subspaces: $\text{span}\{|0\rangle, |1\rangle\} \leq \mathbb{C}^3$ vs. $\text{span}\{|2\rangle\} \leq \mathbb{C}^3$

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

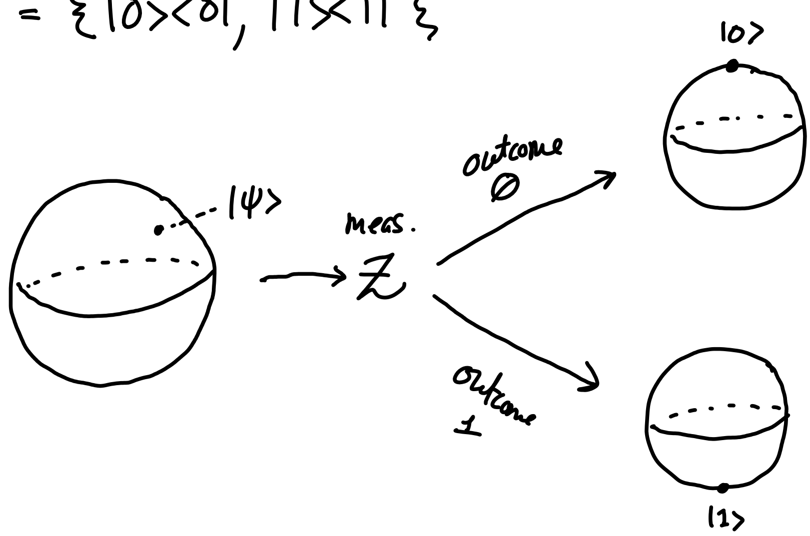
2. Post-measurement state:



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



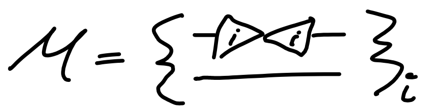
Ex $\mathcal{Z} = \{ |0\rangle\langle 0| , |1\rangle\langle 1| \}$

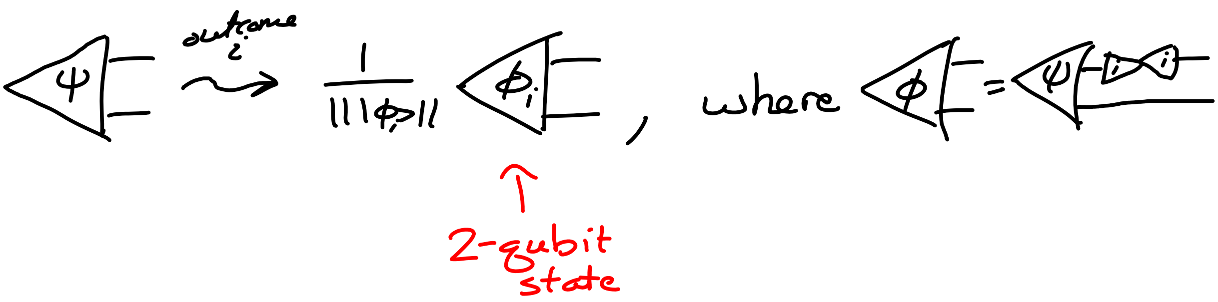


$\text{Prob}(0 \mid |\psi\rangle) = \langle\psi|0\rangle\langle 0|\psi\rangle = \| \langle 0|\psi\rangle \|^2$

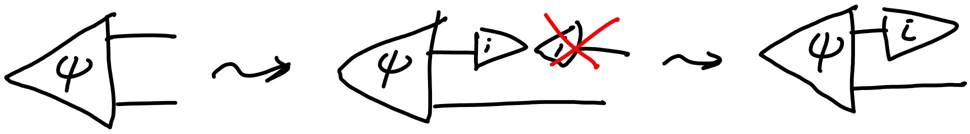
$\text{Prob}(1 \mid |\psi\rangle) = \| \langle 1|\psi\rangle \|^2$

Ex Measuring a subsystem, e.g.



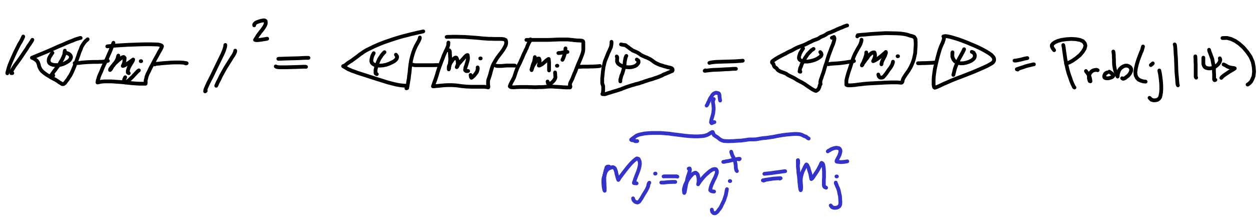


The first qubit is not entangled, so we can ignore it and write the state of the 2nd qubit:

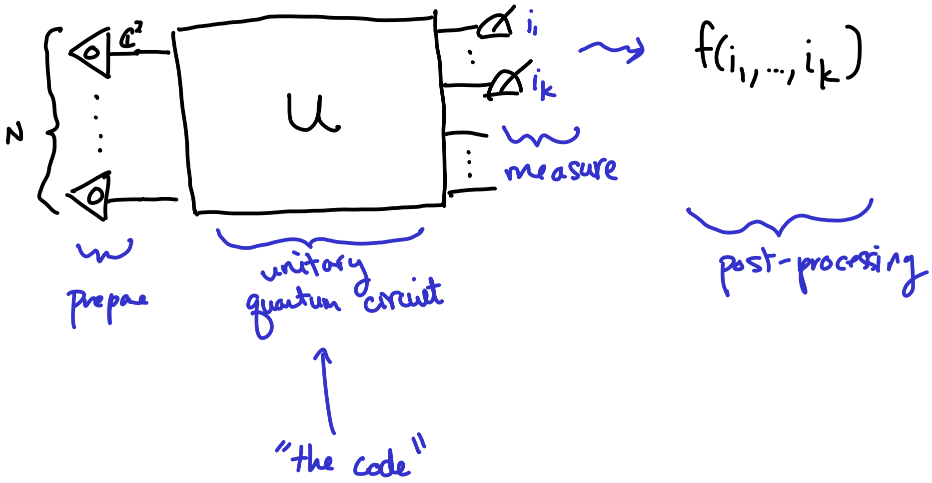


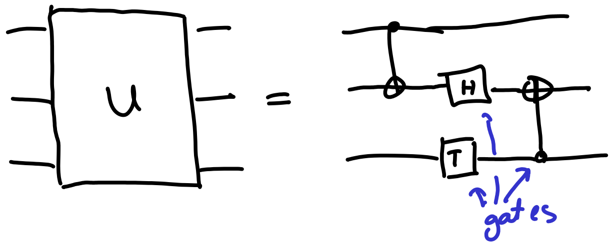
* n.b. this is only allowed because the qubits are not entangled. If they are entangled, this results in a mixed state, cf. Section 2.7.1 of the Crow book.

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:

$\pi : \mathbb{B}^n \to \mathbb{B}^n \rightsquigarrow U_\pi :: |\vec{x}\rangle \mapsto |\pi(\vec{x})\rangle$

reversible fn (aka permutation) — unitary

Ex

$\text{NOT} : \mathbb{B} \to \mathbb{B} \rightsquigarrow X :: \begin{matrix} |0\rangle \mapsto |1\rangle \\ |1\rangle \mapsto |0\rangle \end{matrix}$

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

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

any function

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

unitary ("Bennett trick")

<u>Thm</u> For <u>any</u> f, U_f is unitary.

<u>Pf</u> 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. ▨

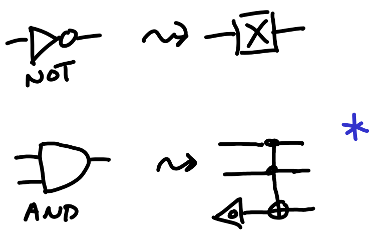
<u>Ex</u>: $\text{AND} : \mathbb{B}^2 \to \mathbb{B}$ $\quad \rightsquigarrow \quad$ $\text{Tof} :: |x, y, z\rangle \mapsto |x, y, (xy) \oplus z\rangle$

$\text{AND}(x, y) := xy$

Toffoli / CCNOT

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

AND + NOT $\qquad$ 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

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

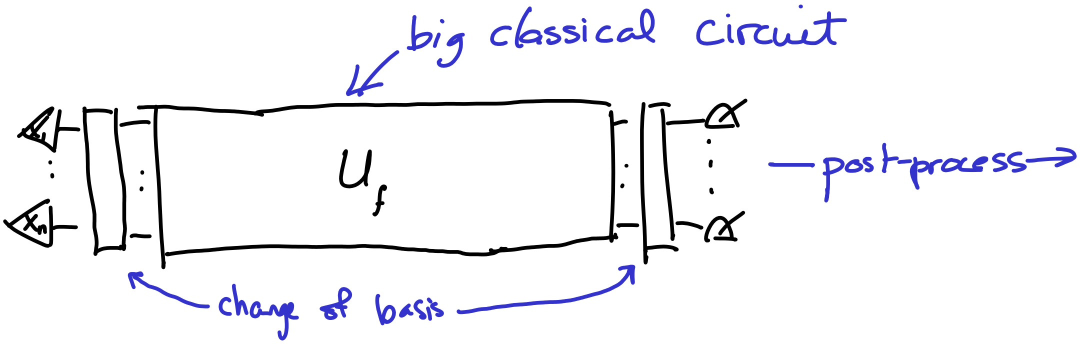
$H|1\rangle = |-\rangle := \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

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

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

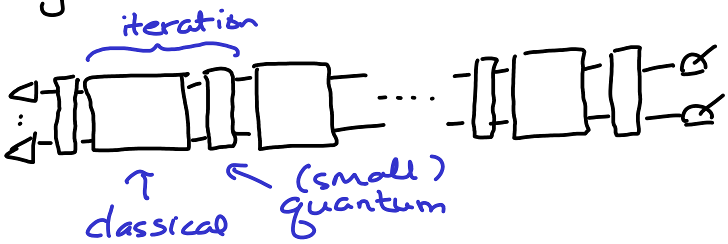
- Most quantum algorithms fall into a handful of forms:

- "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 $G -\boxed{f}- X = G -\boxed{f}- G/H -\boxed{i}- X$, where G, H Abelian groups, i injective, we can find H.)

- Grover-style:

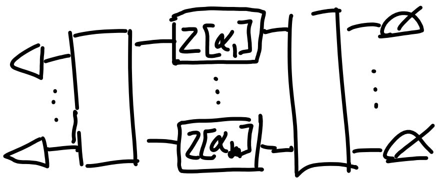


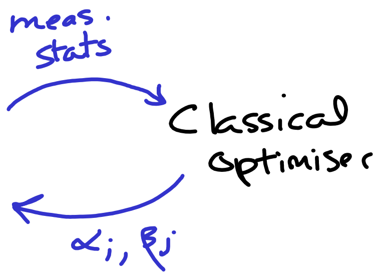
  * Grover search
  * amplitude amplification
  * quantum walks

- Hamiltonian simulation (wk 7)

- Hybrid / quantum ML

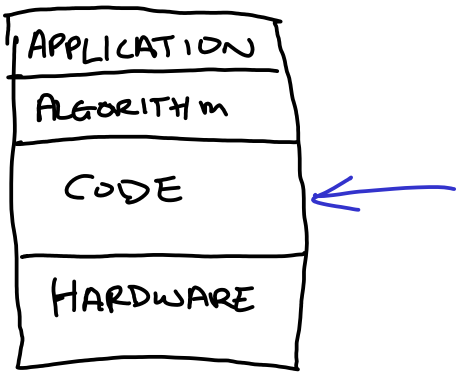
Variational circuits





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

"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 → * compute measurement probabilities for $U|\psi\rangle$, or
weak simulation → * Sample measurement outcomes for $U|\psi\rangle$

ZX-diagrams

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

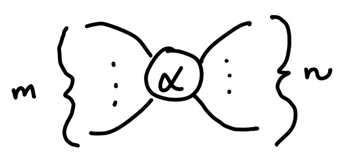
Perspective 1: ZX-diagrams are "circuits" made of spiders.

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

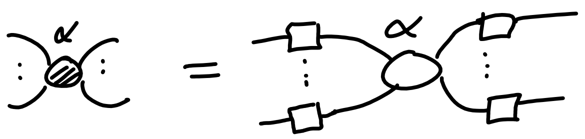
$$Z[\alpha]_m^n = |00..0\rangle\langle 00..0| + e^{i\alpha}|11..1\rangle\langle 11..1| \quad \longleftrightarrow \quad \begin{pmatrix} 1 & & & 0 \\ & 0 & & \\ & & \ddots & \\ & & & 0 \\ 0 & & & & e^{i\alpha} \end{pmatrix}$$

rank 2
(usually not unitary!)

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

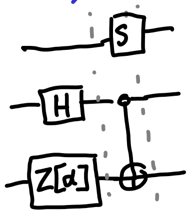


$$X[\alpha]_m^n = |++\dots+\rangle\langle++\dots+| + e^{i\alpha}|--\dots-\rangle\langle--\dots-|$$



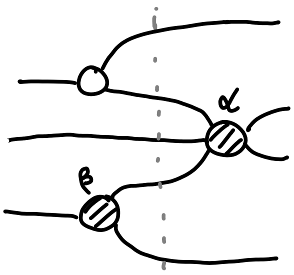
where $-\square- = -\boxed{H}- = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$

For circuits, we can compute the linear map as:



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

Similarly for ZX-diagrams:

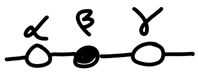


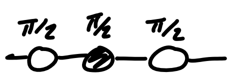
$$(I \otimes X[\alpha]_3^2 \otimes I)(Z[0]_1^2 \otimes I \otimes X[\beta]_1^2)$$


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

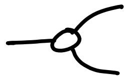

$= X[\alpha]$ ⟵ X phase gate

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

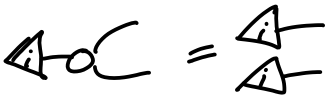
$U = e^{i\theta} \cdot$ 

Ex $\quad -\boxed{H}- = e^{-i\pi/4}$ 

$=: -\square-$

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

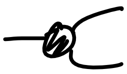
↑ "copies Z-basis"



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

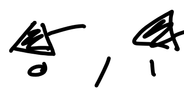
↑ "deletes Z-basis"

 $= 1$

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

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

 $= 1$

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

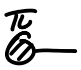
X-basis

Basis states in ZX:

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

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

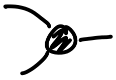
Z basis states

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

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

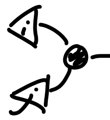
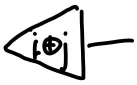
Similarly:  $= \sqrt{2} \cdot |+\rangle$,  $= \sqrt{2} \cdot |-\rangle$

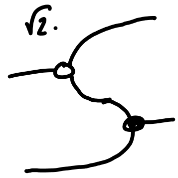
X-basis states

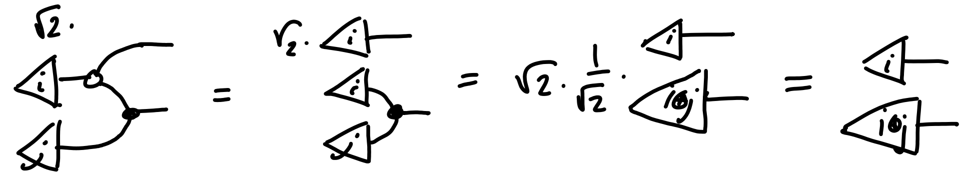
 $= |+\rangle\langle ++| + |-\rangle\langle --| = \ldots$

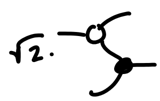
$= \frac{1}{\sqrt{2}} \left(|0\rangle\langle 00| + |0\rangle\langle 11| + |1\rangle\langle 01| + |1\rangle\langle 10| \right)$

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

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

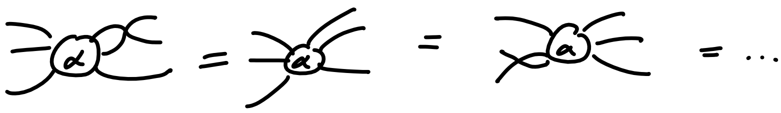
<u>Cor</u> Any n-qubit unitary can be constructed as a ZX-diagram.

ZX Rewriting

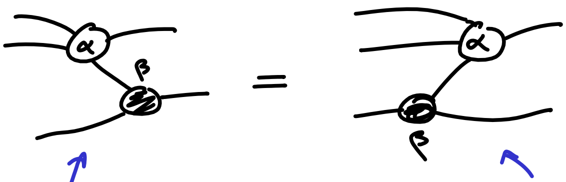
ZX diagrams have "extreme" OCM.

They are invariant under:

- Swapping spider-legs:



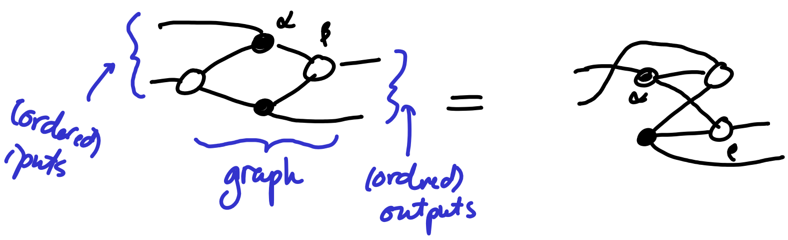
- Changing direction



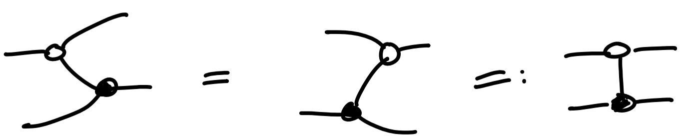
$$(I\otimes X[\beta]^1_2)(Z[\alpha]^2_2\otimes I) = (Z[\alpha]^1_3\otimes I)(I\otimes I\otimes X[\beta]^2_1)$$

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

e.g.



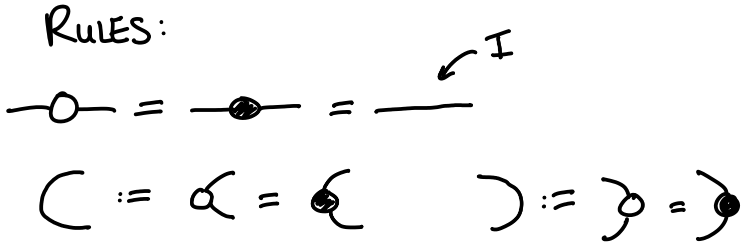
e.g. CNOT =



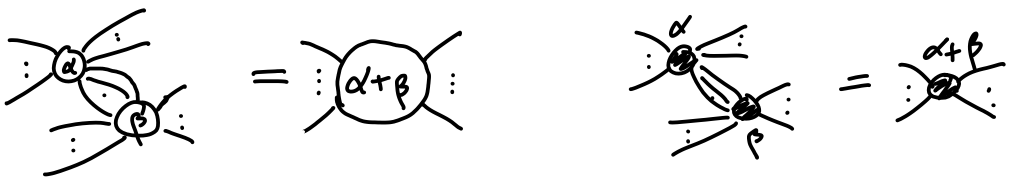
The ZX-calculus

:= a set of equations for ZX-diagrams

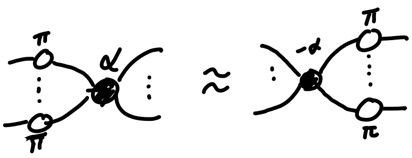
(0) "WIRE" RULES:



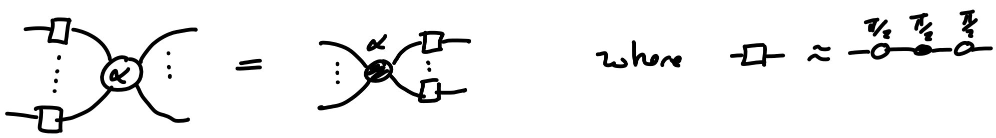
(1) SPIDER-FUSION



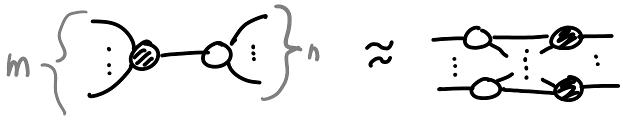
(2) π-rule*:



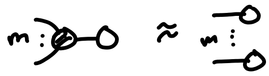
(3) COLOUR CHANGE:



(4) Strong complementarity



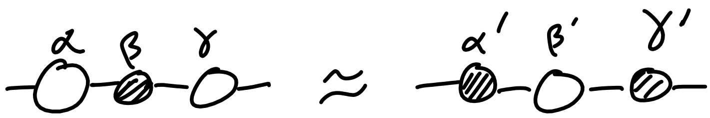
Special cases: $m=0 \Rightarrow$ 

$n=0 \Rightarrow$ 

COPY RULES

$m=2, n=2 \Longrightarrow$ 

(EU) rule:



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

← trig. fns.