Remark: These are notes from a lecture I gave several years ago.
I seem to have lost the editable version, just the pdf printout remains.
I'll do things slightly differently this time around - but the document
is close enough that I won't redo the notes for now.

The file contains a first introduction to the setting and notation used for
quantum circuits, leading up to the "quantum teleportation protocol".

I'll go over this topic at the beginning of the course, so that one full protocol
will be explained early on. I'll then restart with a more systematic intro to QM.
If you had little prior exposure to QM and feel a bit lost... don't worry: We'll cover
the basics next.

"Spin" a quantum system with two dist. states: $\uparrow$, $\downarrow$ or 0, 1.

Quantize:

$$0 \longmapsto |0\rangle$$

$$1 \longmapsto |1\rangle$$

and consider the two-dim. Hilbert space

$$\mathcal{H} = \{ \alpha |0\rangle + \beta |1\rangle \mid \alpha, \beta \in \mathbb{C} \}.$$

QM allows for superpositions

$$\mathcal{H} \ni |\Psi\rangle = \alpha |0\rangle + \beta |1\rangle$$

$$|\alpha|^2 + |\beta|^2 = 1.$$

Classical information can be read out e.g. via measurement in $0,1$-basis on $|\Psi\rangle$, by

Born's rule, get

$$0 \quad \text{with prob. } |\alpha|^2$$

$$1 \quad \text{with prob. } |\beta|^2.$$

Time evolution in QM specified by

Hamiltonian H, a Hermitian matrix

$$H = \begin{bmatrix} \alpha & \gamma \\ \bar{\gamma} & \beta \end{bmatrix} \qquad \alpha, \beta \in \mathbb{R}, \; \gamma \in \mathbb{C}$$

$$H = H^{+}.$$

After acting for time t, get time evol. operator

$$U(t) = \exp(itH) \quad \in U(\mathcal{H}),$$

where

$$U(\mathcal{H}) = \{ U \mid UU^{+} = \mathbb{1} \}$$

are the unitary operators. Since every unitary can be generated by some Hamiltonian, it's OK to only ever specify unitaries.

Examples of important time evolutions:

- NOT $\quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

"bit flip" $\hat{=}$ "negation of classical bit".

- $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

$$Z: \quad |0\rangle \mapsto |0\rangle$$
$$|1\rangle \mapsto -|1\rangle$$

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

$$\Rightarrow \quad \langle + | - \rangle = 0$$

- "phase gate" $\quad S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$.

$$S^2 = Z.$$

- Hadamard gate: $\quad H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$

$$H^\dagger H = \mathbb{1}, \quad \text{but } H^\dagger = H$$

$$\Rightarrow H^2 = \mathbb{1}$$

```
In[4]:= $PrePrint = MatrixForm
Out[4]= MatrixForm
```

In[5]:= $H = \frac{1}{\sqrt{2}}$ {{1, 1}, {1, -1}}

Out[5]= $\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$

```
In[6]:= X = {{0, 1}, {1, 0}}
```

Out[6]= $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

```
In[8]:= S = {{1, 0}, {0, I}}
```

Out[8]= $\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$

```
In[10]:= SN = H.S.H
```

Out[10]= $\begin{pmatrix} \frac{1}{2}+\frac{i}{2} & \frac{1}{2}-\frac{i}{2} \\ \frac{1}{2}-\frac{i}{2} & \frac{1}{2}+\frac{i}{2} \end{pmatrix}$

```
In[11]:= SN.SN
```

Out[11]= $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

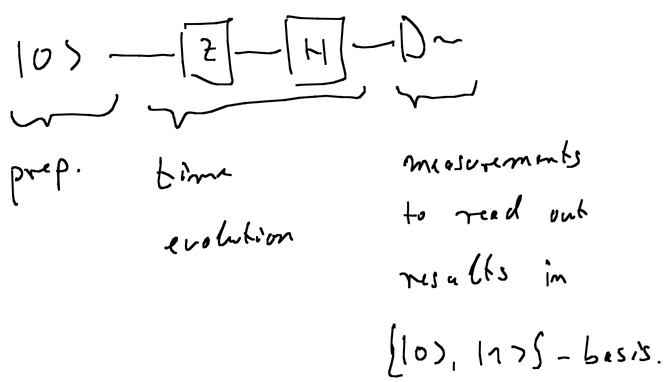
$\Rightarrow$ can define "square root of not-gate".

- $H|0\rangle = |+\rangle \quad \overset{H^2 = \mathbb{1}}{\Rightarrow} \quad |0\rangle = HH|0\rangle = H|+\rangle$

  $H|1\rangle = |-\rangle \qquad\qquad |1\rangle = \sim\sim = H|-\rangle.$

Will ~~interpret~~ $|\pm\rangle \in \mathcal{H} = \mathbb{C}^2$ as "quantum bits", i.e. "two state systems", but with superpositions allowed. Use "diagrammatic notation" (quantum circuits) to symbolize time evolution.

E.g.:



"coin toss"

Pass to many qubits:

n spin configuration

$\uparrow\downarrow \cdots \uparrow\uparrow$

mapped to bit string

$01 \cdots 00$,

a "quantum register" if superpositions are allowed:

$$|\Psi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x \, |x\rangle \qquad \alpha_x \in \mathbb{C}$$

$$\sum_x |\alpha_x|^2 = 1.$$

$\Rightarrow$ roughly 2^n complex parameters needed to describe state $|\Psi\rangle$. $\Rightarrow$ no obvious way to keep track of n-qubit register on classical computer for moderately large n.

Formally:

$$\underbrace{\mathcal{H}}_{\text{global Hilbert space}} = \bigotimes_{i=1}^{n} \underbrace{\mathcal{H}_i}_{\text{single qubit H.S.}}$$

$\mathcal{H}_i = \mathbb{C}^2$.

Time evolution for two qubits, described by

4×4 matrices with respect to $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$-

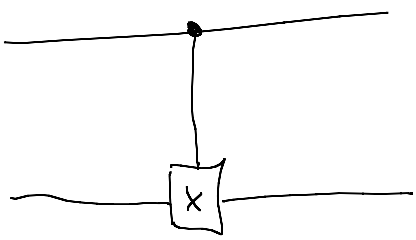
basis.

Examples:

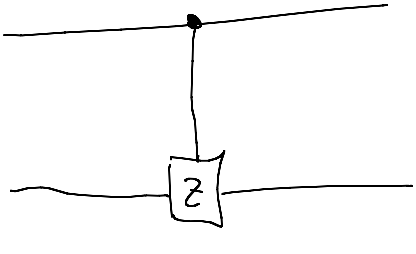
- "controlled not" gate:

$$\begin{array}{c|cccc|c} & 00 & 01 & 10 & 11 & \\ \hline & 1 & & & & 00 \\ & & 1 & & & 01 \\ & & & 0 & 1 & 10 \\ & & & 1 & 0 & 11 \end{array}$$

"flips 2nd qubit iff 1st qubit is in state $|1\rangle$."



- controlled-Z gate



$$\begin{aligned} |00\rangle &\mapsto |00\rangle \\ |01\rangle &\quad\;\; |01\rangle \\ |10\rangle &\quad\;\; |10\rangle \\ |11\rangle &\mapsto -|11\rangle \end{aligned}$$

First protocol: quantum teleportation

Two player setting: Alice and Bob.

Alice has qubit in state $|\Psi\rangle$.

Wants to "send" this qubit to Bob, i.e. perf. some protocol that will Bob with a qubit in state $|\Psi\rangle$.

However:

(a) $|\Psi\rangle$ not <u>known</u> to either player

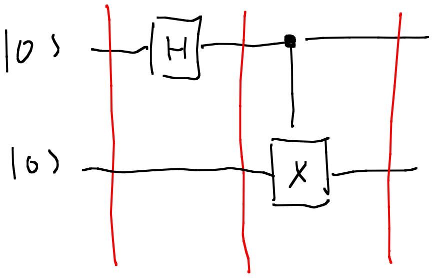
(b) A & B widely separated, can exchange only two classical bits.

Could be impossible, because:

(a) Definition of $|\Psi\rangle$ depends on <u>continuous</u> parameters α, β which contain in principle infinite amount of information.

(b) Uncertainty principle forbids one to learn α and β from single copy. Also, would violate "no cloning".

To anyway do it, need one ingredient: <u>Bell state</u> generated by following circuit:



$|\Psi_0\rangle$ $|\Psi_1\rangle$ $|\Psi_2\rangle$.

$$|\Psi_0\rangle = |0\rangle|0\rangle = |00\rangle.$$

$\longmapsto$ H on 1st qbit

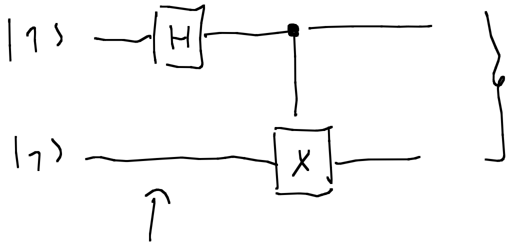
$$|\Psi_1\rangle = (H|0\rangle)|0\rangle$$

$$= \left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right)|0\rangle$$

$$= \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|10\rangle$$

$\longmapsto$ C-NOT

$$|\Psi_2\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle =: \underbrace{|B_{00}\rangle}_{\in \text{ of triplet space.}} \text{ Bell state.}$$



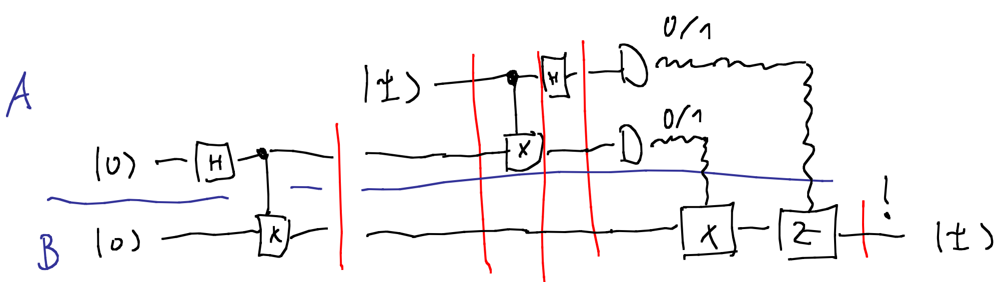
Hamiltonian = 0

$$|B_{11}\rangle = \underbrace{\frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right)}_{\text{singlet state}}$$

$\boxed{\text{check this!}}$

$$(C\text{-}N)(H \otimes 1)|1\rangle|1\rangle = |\beta_{11}\rangle$$

Teleportation circuit



$|B_{00}\rangle$

$|\phi_0\rangle$ $|\phi_1\rangle$ $|\phi_2\rangle$ $|\phi_3\rangle$

$$|\phi_0\rangle = \frac{1}{\sqrt{2}}|\psi\rangle(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}\left(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle\right)$$

$$|\phi_1\rangle = \frac{1}{\sqrt{2}}\left(\alpha|000\rangle + \alpha|011\rangle + \beta|110\rangle + \beta|101\rangle\right)$$

$$\begin{aligned}
|\phi_2\rangle = \frac{1}{2}\Big(&\alpha|000\rangle + \alpha|100\rangle \\
&+ \alpha|011\rangle + \alpha|111\rangle \\
&+ \beta|010\rangle - \beta|110\rangle \\
&+ \beta|001\rangle - \beta|101\rangle\Big)
\end{aligned}$$

$$\begin{aligned}
&= \frac{1}{2}|00\rangle(\alpha|0\rangle + \beta|1\rangle) \\
&+ \frac{1}{2}|01\rangle(\alpha|1\rangle + \beta|0\rangle) \\
&+ \frac{1}{2}|10\rangle(\alpha|0\rangle - \beta|1\rangle) \\
&+ \frac{1}{2}|11\rangle(\alpha|1\rangle - \beta|0\rangle)
\end{aligned}$$

$$\begin{aligned}
&= \frac{1}{2}|00\rangle|\psi\rangle + \frac{1}{2}|01\rangle(X|\psi\rangle) \\
&+ \frac{1}{2}|10\rangle(Z|\psi\rangle) + \frac{1}{2}|11\rangle(XZ)|\psi\rangle
\end{aligned}$$

$$|\phi_3\rangle = |\psi\rangle.$$