II. Quantum Circuits

- "circuit model": sequence of building blocks that carry out elementary computations, called gates

Single qubit gates

- classical example: NOT $\quad 0 \to 1,\ 1 \to 0$

- quantum examples: as quantum theory is unitary, quantum gates are represented by unitary matrices: $U^\dagger U = \mathbb{1}$

recall Dirac notation: $U = \begin{pmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{pmatrix} = u_{00}|0\rangle\langle 0| + u_{01}|0\rangle\langle 1| + u_{10}|1\rangle\langle 0| + u_{11}|1\rangle\langle 1|$

- $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = |0\rangle\langle 1| + |1\rangle\langle 0|$

  ↳ $\sigma_x|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$, $\sigma_x|1\rangle = (|0\rangle\langle 1| + |1\rangle\langle 0|) \cdot |1\rangle = |0\rangle\underbrace{\langle 1|1\rangle}_{1} + |1\rangle\underbrace{\langle 0|1\rangle}_{0} = |0\rangle$ (Dirac notation)

  ⇒ bit flip ≙ NOT-gate, e.g. $|0\rangle$ — σ_x — $|1\rangle$ ⇒ rotation around x-axis by π

- $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1|$

  ↳ $\sigma_z|+\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = |-\rangle$, $\sigma_z|-\rangle = (|0\rangle\langle 0| - |1\rangle\langle 1|) \cdot \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle$

  ⇒ phase flip ⇒ rotation around z-axis by π

- $\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = i \cdot \sigma_x \cdot \sigma_z$ ⇒ bit & phase flip

⇒ σ_x, σ_y & σ_z are the so-called Pauli matrices and $\sigma_i^2 = \mathbb{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ (does nothing)

⇒ together with identity $\mathbb{1}$ they form a basis of 2×2 matrices

(→ any 1-qubit rotation can be written as a linear combination of them)

- Hadamard gate: one of the most important gates for quantum circuits

$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}} (|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|)$

↳ $H|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = |+\rangle$, $H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|) \cdot |1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle$

⇒ creates superposition! also $H|+\rangle = |0\rangle$, $H|-\rangle = |1\rangle$ ⇒ used to change between X & Z basis

- similarly, as $S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$ adds 90° to the phase φ: $S \cdot |+\rangle = |+i\rangle$, $S|-\rangle = |-i\rangle$

⇒ $S \cdot H$ is applied to change from Z to Y basis

Multipartite quantum states

- we use tensor products to describe multiple states: $|a\rangle \otimes |b\rangle = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \otimes \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = \begin{pmatrix} a_1 b_1 \\ a_1 b_2 \\ a_2 b_1 \\ a_2 b_2 \end{pmatrix}$
- example: system A is in state $|1\rangle_A$ and system B is in state $|0\rangle_B$

  $\Rightarrow$ the total (bipartite) state is $|10\rangle_{AB} := |1\rangle_A \otimes |0\rangle_B = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$

↳ remark: states of this form are called uncorrelated, but there are also bipartite states that cannot be written as $|\psi\rangle_A \otimes |\varphi\rangle_B$. These states are correlated and sometimes even entangled (→ very strong correlation), e.g. $|\psi^{(\infty)}\rangle_{AB} = \frac{1}{\sqrt{2}} (|00\rangle_{AB} + |11\rangle_{AB}) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$

a so-called Bell state, used for teleportation, cryptography, Bell tests, etc.

Two-qubit gates

- classical example: XOR

→ irreversible (→ given the output we cannot recover the input)

BUT: as quantum theory is unitary, we only consider unitary and therefore reversible gates

- quantum example:

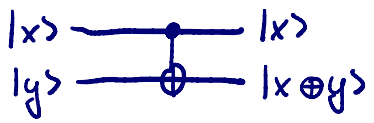
$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10|$$

↳ $CNOT \cdot |00\rangle_{xy} = CNOT \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = |00\rangle_{xy}$, $CNOT\,|10\rangle_{xy} = |11\rangle_{xy}$

$\Rightarrow$

input		output	
x	y	x	x⊕y
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

$\Rightarrow$ circuit:



$\hat{=}$ reversible XOR

$\Rightarrow$ we can show that every function f can be described by a reversible circuit

$\Rightarrow$ quantum circuits can perform all functions that can be calculated classically

III. Entanglement

- If a pure state $|\psi\rangle_{AB}$ on systems A, B cannot be written as $|\varphi\rangle_A \otimes |\xi\rangle_B$, it is entangled

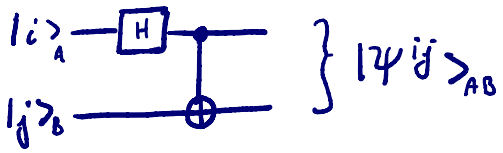
Bell states

There are four so-called Bell states that are maximally entangled and build an orthonormal basis:

$$|\psi^{00}\rangle := \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \qquad |\psi^{01}\rangle := (|01\rangle + |10\rangle)$$
$$|\psi^{10}\rangle := \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \qquad |\psi^{11}\rangle := (|01\rangle - |10\rangle)$$

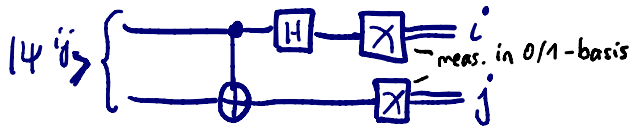
$\Rightarrow$ in general we can write $|\psi^{ij}\rangle = (\mathbb{1} \otimes \sigma_x^j \cdot \sigma_z^i)|\psi^{00}\rangle$

Creation of Bell states



initial state $\lvert ij\rangle_{AB}$		$(H_A \otimes \mathbb{1}_B)\lvert ij\rangle_{AB}$		$\lvert\psi^{ij}\rangle$
$\lvert 00\rangle$		$(\lvert 00\rangle + \lvert 10\rangle)/\sqrt{2}$		$(\lvert 00\rangle + \lvert 11\rangle)/\sqrt{2} = \lvert\psi^{00}\rangle$
$\lvert 01\rangle$	$\xrightarrow{H_A}$	$(\lvert 01\rangle + \lvert 11\rangle)/\sqrt{2}$	$\xrightarrow{CNOT_{A,B}}$	$(\lvert 01\rangle + \lvert 10\rangle)/\sqrt{2} = \lvert\psi^{01}\rangle$
$\lvert 10\rangle$		$(\lvert 00\rangle - \lvert 10\rangle)/\sqrt{2}$		$(\lvert 00\rangle - \lvert 11\rangle)/\sqrt{2} = \lvert\psi^{10}\rangle$
$\lvert 11\rangle$		$(\lvert 01\rangle - \lvert 11\rangle)/\sqrt{2}$		$(\lvert 01\rangle - \lvert 10\rangle)/\sqrt{2} = \lvert\psi^{11}\rangle$

$\rightarrow$ opposite direction: Bell measurement



$\Rightarrow$ classical outcomes i,j correspond to a meas. of the state $|\psi^{ij}\rangle$

Teleportation

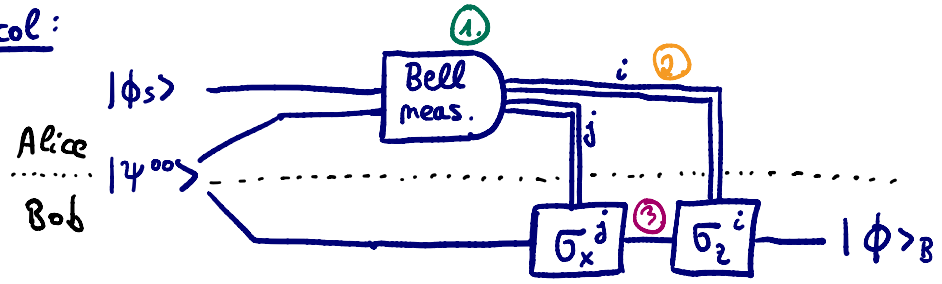
- **Goal**: Alice wants to send her (unknown) state $|\phi\rangle_S := \alpha|0\rangle_S + \beta|1\rangle_S$ to Bob.

  She can only send him two classical bits though. They both share the maximally entangled state $|\psi^{00}\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})$.

⇒ **initial state of the total system:**

$$
\begin{aligned}
|\phi\rangle_S \otimes |\psi^{00}\rangle_{AB} &= \frac{1}{\sqrt{2}}\left(\alpha|000\rangle_{SAB} + \alpha|011\rangle_{SAB} + \beta|100\rangle_{SAB} + \beta|111\rangle_{SAB}\right) \\
&= \frac{1}{2\sqrt{2}}\Big[(|00\rangle_{SA} + |11\rangle_{SA}) \otimes (\alpha|0\rangle_B + \beta|1\rangle_B) + (|01\rangle_{SA} + |10\rangle_{SA}) \otimes (\alpha|1\rangle_B + \beta|0\rangle_B) \\
&\quad + (|00\rangle_{SA} - |11\rangle_{SA}) \otimes (\alpha|0\rangle_B - \beta|1\rangle_B) + (|01\rangle_{SA} - |10\rangle_{SA}) \otimes (\alpha|1\rangle_B - \beta|0\rangle_B)\Big] \\
&= \frac{1}{2}\Big[|\psi^{00}\rangle_{SA} \otimes |\phi\rangle_B + |\psi^{01}\rangle_{SA} \otimes (\sigma_x|\phi\rangle_B) \\
&\quad + |\psi^{10}\rangle_{SA} \otimes (\sigma_z|\phi\rangle_B) + |\psi^{11}\rangle_{SA} \otimes (\sigma_x\sigma_z|\phi\rangle_B)\Big]
\end{aligned}
$$

- **Protocol:**



1. Alice performs a meas. on S & A in the Bell basis.
2. She sends her classical outputs i, j to Bob.
3. Bob applies $\sigma_z^i \sigma_x^j$ to his qubit and gets $|\phi\rangle$!

1. Alice's measurement		→ Bob's state	2. Alice sends $i\ j$	3. Bob applies →	Bob's final state
$\|\psi^{00}\rangle$	$\otimes$	$\|\phi\rangle_B$	0 0	11	$\|\phi\rangle_B$
$\|\psi^{01}\rangle$		$\sigma_x\|\phi\rangle_B$	0 1	σ_x	"
$\|\psi^{10}\rangle$		$\sigma_z\|\phi\rangle_B$	1 0	σ_z	"
$\|\psi^{11}\rangle$		$\sigma_x\sigma_z\|\phi\rangle_B$	1 1	$\sigma_z\sigma_x$	"

Note, that Alice's state collapsed during the measurement, so she does not have the initial state $|\phi\rangle$ anymore. This is expected due to the no-cloning theorem, as she cannot copy her state, but just send her state to Bob when destroying her own.