II. Quantum Circuits

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

input — $\boxed{\text{algorithm}}$ — output

Single qubit gates

- classical example: NOT 
- quantum examples: as quantum theory is unitary, quantum gates are represented by

unitary matrices: $U^\dagger U = \mathbb{1}$

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

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

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

⇒ bit flip $\hat{=}$ NOT-gate, e.g. $|0\rangle - \boxed{\sigma_x} - |1\rangle$ ⇒ 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 2x2 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 $|10\rangle_{AB} := |1\rangle_A \otimes |0\rangle_B = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$

  $\hookrightarrow$ 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. $|\psi^{(00)}\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|00\rangle_{AB} + |11\rangle_{AB}\right) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$

  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:

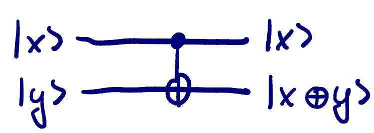
$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10|$$

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

$\Rightarrow$

input x	input y	output x	output $x \oplus y$
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