Classical gates

State of classical computers: sequence of 0 and 1.
Transformations are called gates.

Def.: a classical (logical) gate is $g: \{0,1\}^n \to \{0,1\}$ (elementary), $g: \{0,1\}^n \to \{0,1\}^m$ (extended).

Ex.: NOT: $\quad$ Notation: $\oplus$ is $+ \pmod 2$

$\text{NOT}(x_1) = 1 \oplus x_1$;

AND: $(x_1, x_2) \mapsto x_1 \cdot x_2$;

XOR: $(x_1, x_2) \mapsto x_1 \oplus x_2$;

OR: $(x_1, x_2) \mapsto x_1 \oplus x_2 + x_1 \cdot x_2$;

TOFFOLI: $\{0,1\}^3 \to \{0,1\}^3$.
$(x_1, x_2, x_3) \mapsto (x_1, x_2, x_1 \cdot x_2 \oplus x_3)$

Def.: a gate is reversible if its associated function is a bijection.

Remark: $\text{TOF}(x_1, x_2, 0) = (x_1, x_2, \text{AND}(x_1, x_2))$;
$\text{TOF}(1, x_2, x_3) = (1, x_2, \text{XOR}(x_2, x_3))$;
$\text{TOF}(1, 1, x_3) = (1, 1, \text{NOT}(x_3))$.

More useful gates: ID: $x_1 \mapsto x_1$;
FALSE: $x_1 \mapsto 0$;
TRUE: $x_1 \mapsto 1$;
COPY: $x_1 \mapsto (x_1, x_1)$.
(FANOUT)

Rules for combining gates

Let $g_1, \dots, g_k$ gates. Define $F(g_1, \dots, g_k)$ the set of gates that can be constructed from $g_1, \dots, g_k$ according to the following rules:

(1) $g_1, \dots, g_k \in F(g_1, \dots, g_k)$;

(2) padding, $P^{(m)}_{y_1, \dots, y_l; j_1, \dots, j_l}: \{0,1\}^m \to \{0,1\}^{m+l}$;
$(x_1, \dots, x_m) \mapsto (x_1, \dots, x_{j_1 - 1}, y_1, x_{j_1}, x_{j_1+1}, \dots)$

(3) restrictions and reordering: $\pi^{(m)}_{j_1, \dots, j_l}: \{0,1\}^m \to \{0,1\}^l$, $l \le m$, j_k distinct;
$(x_1, \dots, x_m) \mapsto (x_{j_1}, \dots, x_{j_l})$

(4) composition of gates: $h_1, h_2 \in F(g_1, \dots, g_k) \overset{\text{when it makes sense}}{\Rightarrow} h_1 \circ h_2 \in F(g_1, \dots, g_k)$;

(5) cartesian products: $\quad$ " , " $\in$ " $\Rightarrow h_1 \times h_2 \in$ " .

Def.: a set of gates $g_1, \dots, g_k$ is universal if $\forall$ gate g, $g \in F(g_1, \dots, g_k)$.

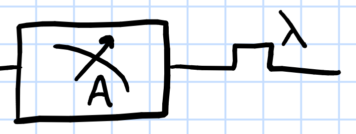
Theorem: the Toffoli gate is universal and reversible. Proof: book. $\square$

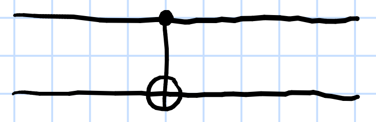
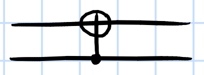
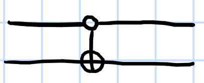
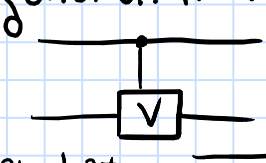
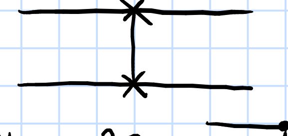
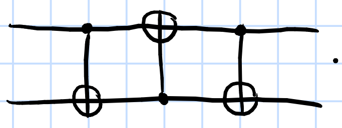
Quantum Gates

Def.: a quantum n-gate is a unitary operator $U: \mathbb{H}^{\otimes n} \to \mathbb{H}^{\otimes n}$. $\quad \mathbb{H} \cong \mathbb{C}^2$

The qubits on which we apply quantum gates form a quantum register.

Ex.:
- identity $\quad$ ——— $\quad \mathbb{1} \quad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$;
- phase factor $\quad -\boxed{M(\alpha)}- \quad M(\alpha) = e^{i\alpha}\mathbb{1} \quad \begin{pmatrix} e^{i\alpha} & 0 \\ 0 & e^{i\alpha} \end{pmatrix}$;
- phase shift $\quad -\boxed{P(\alpha)}- \quad P(\alpha) = |0\rangle\langle 0| + e^{i\alpha}|1\rangle\langle 1| \quad \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix}$;
- Q NOT (Pauli X) $\quad -\boxed{X}- \quad \sigma_x \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$;
- Pauli Y $\quad -\boxed{Y}- \quad \sigma_y \quad \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$;
- Pauli Z $\quad -\boxed{Z}- \quad \sigma_z \quad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$;
- Hadamard $\quad -\boxed{H}- \quad H = \frac{\sigma_x + \sigma_z}{\sqrt{2}} \quad \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$;
- spin rotation $\quad -\boxed{D_{\hat{n}}(\alpha)}- \quad D_{\hat{n}}(\alpha) \quad (\dots)$.

Measurement of observable A:  (λ = measured value).

- C NOT (controlled quantum NOT)  $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$
$\Lambda^1(X) = |0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes X$
(variants: $\Lambda_1(X)$  $\mathbb{1} \otimes |0\rangle\langle 0| + X \otimes |1\rangle\langle 1|$,
$\Lambda^{|0\rangle}(X)$  $|0\rangle\langle 0| \otimes X + |1\rangle\langle 1| \otimes \mathbb{1}$);
- in general: if V is a quantum (unary) gate, controlled V is
 $\Lambda^1(V) = |0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes V \quad \left(\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & \multicolumn{2}{c}{\multirow{2}{*}{V}} \\ 0 & 0 & & \end{array}\right)$;
- swap gate  $S = |00\rangle\langle 00| + |11\rangle\langle 11| + |01\rangle\langle 10| + |10\rangle\langle 01|$,
can be written as .

Rules for combining quantum gates:

given $U_1, \dots, U_k$, $U_j \in \mathcal{U}(\mathbb{H}^{\otimes m_j})$, the set $F(U_1, \dots, U_k)$ of gates that can be obtained from $U_1, \dots, U_k$ is defined by:

(1) $U_1, \dots, U_k \in F(U_1, \dots, U_k)$;

(2) $\mathbb{1}^{\otimes n} \in F(U_1, \dots, U_k)$;

(3) $V_1, V_2 \in F(U_1, \dots, U_k) \Rightarrow V_1 V_2 \in F(U_1, \dots, U_k)$;

(4) if $V_1 \in \mathcal{U}(\mathbb{H}^{\otimes m_1})$, $V_2 \in \mathcal{U}(\mathbb{H}^{\otimes m_2})$, $V_1, V_2 \in F(U_1, \dots, U_k) \Rightarrow V_1 \otimes V_2 \in F(U_1, \dots, U_k)$.

$\{U_1, \dots, U_k\}$ is a universal set of gates if any unitary operator on $\mathbb{H}^{\otimes n}$ belongs to $F(U_1, \dots, U_k)$.

Theorem: $\{M, D_{\hat{y}}, D_{\hat{z}}, \text{C NOT}\}$ is a universal set.