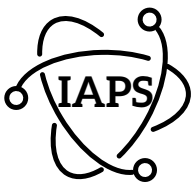
Lecture 8

# CLASSICAL AND QUANTUM GATES AND CIRCUITS

*of the course "Fundamentals of Quantum Computing"*

Stoyan Mishev




INSTITUTE *for* ADVANCED
PHYSICAL STUDIES


May 13, 2022

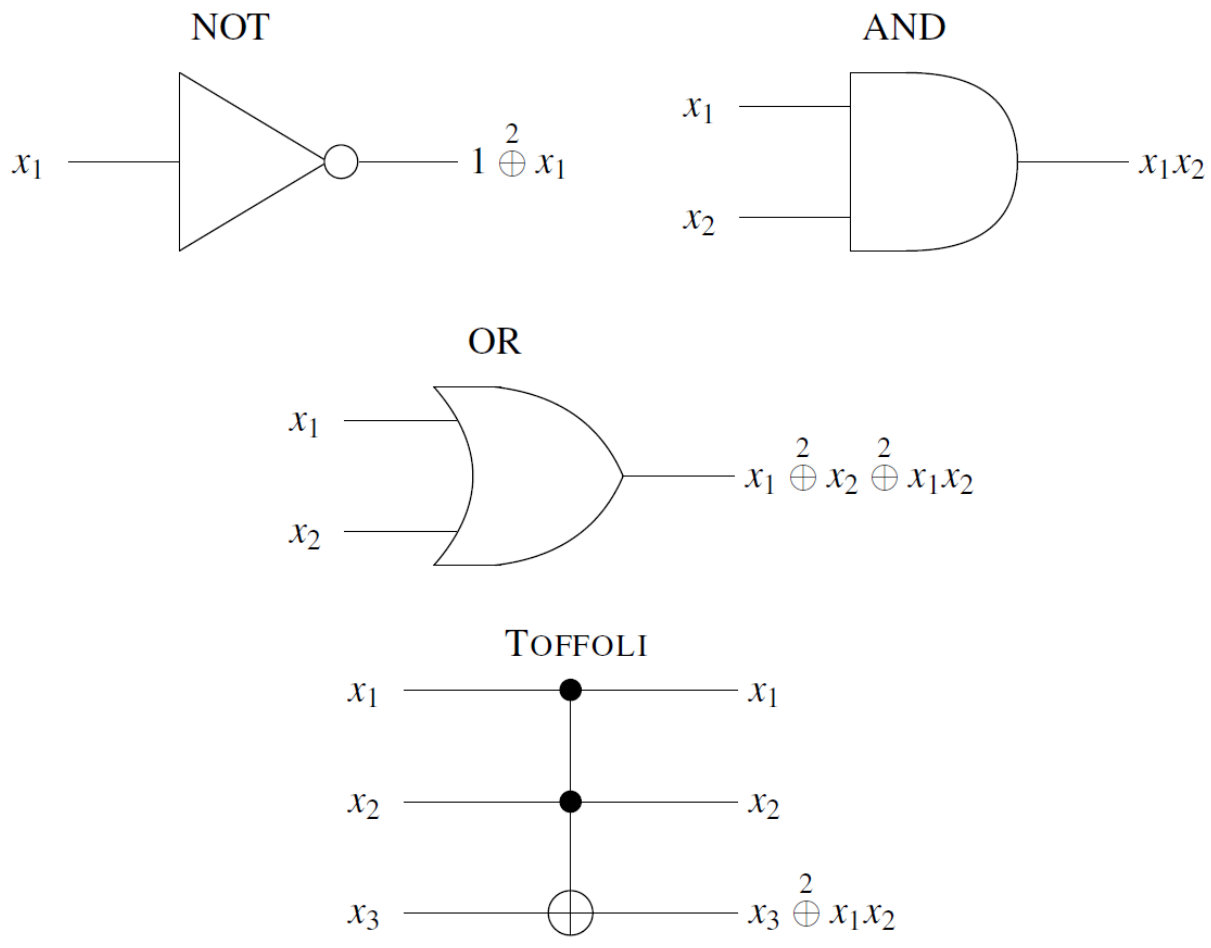
# План



Classical gates and circuits

Quantum gates and circuits

# Classical gates and circuits



# Classical gates. Definition.



*"Elementary"* ***classical*** *(logical)* ***gates*** *are the maps* $f : \{0,1\}^n \to \{0,1\}^m$ *which can be grouped and aligned to construct more complex mappings.*

# Classical gates. Definition.



*"Elementary"* ***classical*** *(logical)* ***gates*** *are the maps* $f : \{0,1\}^n \to \{0,1\}^m$ *which can be grouped and aligned to construct more complex mappings.*

A particlar set $\{0,1\}^n$ is called a **state**.

# Classical gates. Definition.



*"Elementary"* ***classical*** *(logical)* ***gates*** *are the maps* $f : \{0,1\}^n \to \{0,1\}^m$ *which can be grouped and aligned to construct more complex mappings.*

A particlar set $\{0,1\}^n$ is called a **state**.

So the classical computational process is the transformation of one "classical" state to another "classical" state.

# Classical gates. Definition.



*"Elementary"* ***classical*** *(logical)* ***gates*** *are the maps* $f : \{0,1\}^n \to \{0,1\}^m$ *which can be grouped and aligned to construct more complex mappings.*

A particlar set $\{0,1\}^n$ is called a **state**.

So the classical computational process is the transformation of one "classical" state to another "classical" state.

A classical gate is **reversible** if from its output it can recreate its input state uniquely, i.e. it's a bijection.

- **NOT** : $\{0,1\} \to \{0,1\} : x \to (1+x) \bmod 2 \equiv (1 \oplus^2 x)$
  where the notation $u \oplus^2 v = (u+v) \bmod 2$ is used.
  $\bar{x}$ is a shorthand for NOT(x)

[1] after Tommaso Toffoli

https://en.wikipedia.org/wiki/Tommaso_Toffoli

- **NOT** : $\{0,1\} \rightarrow \{0,1\} : x \rightarrow (1+x) \bmod 2 \equiv (1 \oplus^2 x)$ where the notation $u \oplus^2 v = (u+v) \bmod 2$ is used. $\bar{x}$ is a shorthand for NOT(x)
- **AND** : $\{0,1\}^2 \rightarrow \{0,1\} : (x_1, x_2) \rightarrow x_1.x_2$

[1] after Tommaso Toffoli

- **NOT** : $\{0,1\} \to \{0,1\} : x \to (1+x) \bmod 2 \equiv (1 \oplus^2 x)$ where the notation $u \oplus^2 v = (u+v) \bmod 2$ is used. $\bar{x}$ is a shorthand for NOT(x)
- **AND** : $\{0,1\}^2 \to \{0,1\} : (x_1, x_2) \to x_1.x_2$
- **OR** : $\{0,1\}^2 \to \{0,1\} : (x_1, x_2) \to x_1 \oplus^2 x_2 \oplus^2 x_1.x_2$

[1] after Tommaso Toffoli

- **NOT** : $\{0,1\} \to \{0,1\} : x \to (1+x) \bmod 2 \equiv (1 \oplus^2 x)$ where the notation $u \oplus^2 v = (u+v) \bmod 2$ is used. $\bar{x}$ is a shorthand for NOT(x)
- **AND** : $\{0,1\}^2 \to \{0,1\} : (x_1, x_2) \to x_1.x_2$
- **OR** : $\{0,1\}^2 \to \{0,1\} : (x_1, x_2) \to x_1 \oplus^2 x_2 \oplus^2 x_1.x_2$
- **XOR** : $\{0,1\}^2 \to \{0,1\} : (x_1, x_2) \to x_1 \oplus^2 x_2$

[1] after Tommaso Toffoli

- **NOT** : $\{0,1\} \to \{0,1\} : x \to (1+x) \bmod 2 \equiv (1 \oplus^2 x)$
  where the notation $u \oplus^2 v = (u+v) \bmod 2$ is used.
  $\bar{x}$ is a shorthand for NOT(x)
- **AND** : $\{0,1\}^2 \to \{0,1\} : (x_1, x_2) \to x_1.x_2$
- **OR** : $\{0,1\}^2 \to \{0,1\} : (x_1, x_2) \to x_1 \oplus^2 x_2 \oplus^2 x_1.x_2$
- **XOR** : $\{0,1\}^2 \to \{0,1\} : (x_1, x_2) \to x_1 \oplus^2 x_2$
- **Toffoli**[1] : $\{0,1\}^3 \to \{0,1\}^3$ :
  $(x_1, x_2, x_3) \to (x_1, x_2, x_1.x_2 \oplus^2 x_3)$

[1] after Tommaso Toffoli

# DeMorgan rules



- $\overline{A.B} = \bar{A} + \bar{B}$

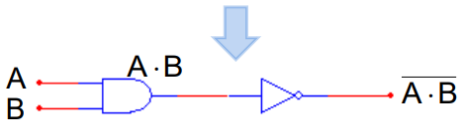
# DeMorgan rules



- $\overline{A.B} = \bar{A} + \bar{B}$

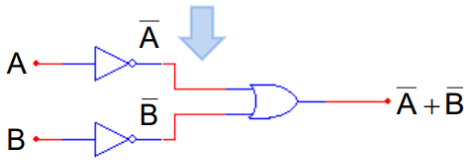
*Proof*

$\overline{A \cdot B}$




| A | B | A·B | $\overline{A \cdot B}$ |
|---|---|---|---|
| 0 | 0 | 0 | 1 |
| 0 | 1 | 0 | 1 |
| 1 | 0 | 0 | 1 |
| 1 | 1 | 1 | 0 |

$\overline{A} + \overline{B}$



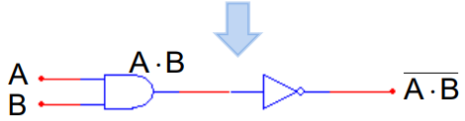

| A | B | $\overline{A}$ | $\overline{B}$ | $\overline{A}+\overline{B}$ |
|---|---|---|---|---|
| 0 | 0 | 1 | 1 | 1 |
| 0 | 1 | 1 | 0 | 1 |
| 1 | 0 | 0 | 1 | 1 |
| 1 | 1 | 0 | 0 | 0 |

# DeMorgan rules



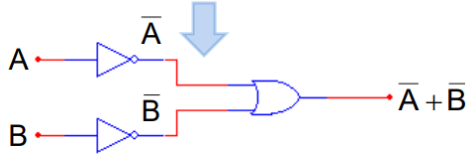
- $\overline{A.B} = \bar{A} + \bar{B}$

*Proof* $\overline{A \cdot B}$




| A | B | A·B | $\overline{A \cdot B}$ |
|---|---|---|---|
| 0 | 0 | 0 | 1 |
| 0 | 1 | 0 | 1 |
| 1 | 0 | 0 | 1 |
| 1 | 1 | 1 | 0 |

$\overline{A} + \overline{B}$




| A | B | $\overline{A}$ | $\overline{B}$ | $\overline{A}+\overline{B}$ |
|---|---|---|---|---|
| 0 | 0 | 1 | 1 | 1 |
| 0 | 1 | 1 | 0 | 1 |
| 1 | 0 | 0 | 1 | 1 |
| 1 | 1 | 0 | 0 | 0 |

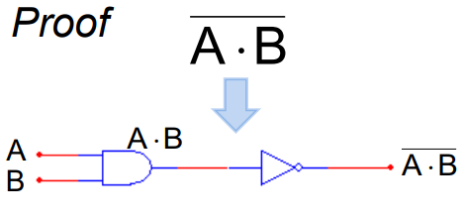
- $\overline{A + B} = \bar{A}.\bar{B}$

# DeMorgan rules

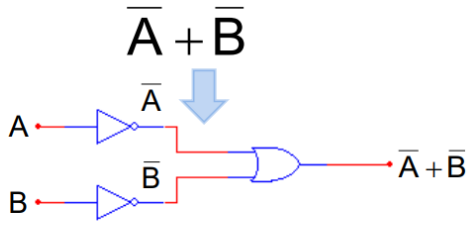


- $\overline{A.B} = \bar{A} + \bar{B}$

*Proof*



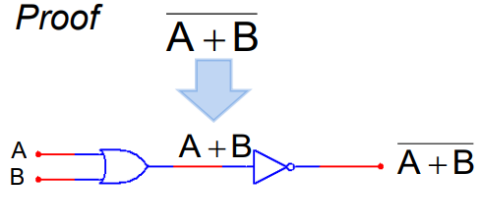

| A | B | A·B | $\overline{A \cdot B}$ |
|---|---|---|---|
| 0 | 0 | 0 | 1 |
| 0 | 1 | 0 | 1 |
| 1 | 0 | 0 | 1 |
| 1 | 1 | 1 | 0 |



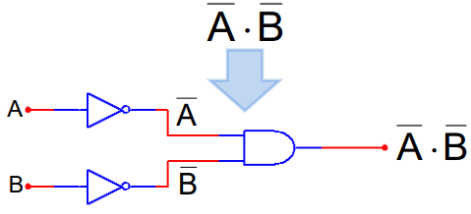

| A | B | $\overline{A}$ | $\overline{B}$ | $\overline{A} + \overline{B}$ |
|---|---|---|---|---|
| 0 | 0 | 1 | 1 | 1 |
| 0 | 1 | 1 | 0 | 1 |
| 1 | 0 | 0 | 1 | 1 |
| 1 | 1 | 0 | 0 | 0 |

- $\overline{A + B} = \bar{A}.\bar{B}$

*Proof*




| A | B | A+B | $\overline{A + B}$ |
|---|---|---|---|
| 0 | 0 | 0 | 1 |
| 0 | 1 | 1 | 0 |
| 1 | 0 | 1 | 0 |
| 1 | 1 | 1 | 0 |

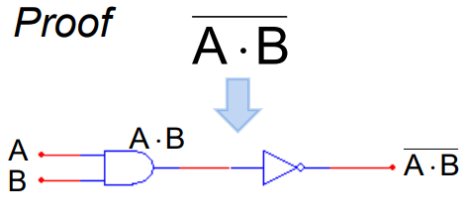



| A | B | $\overline{A}$ | $\overline{B}$ | $\overline{A} \cdot \overline{B}$ |
|---|---|---|---|---|
| 0 | 0 | 1 | 1 | 1 |
| 0 | 1 | 1 | 0 | 0 |
| 1 | 0 | 0 | 1 | 0 |
| 1 | 1 | 0 | 0 | 0 |

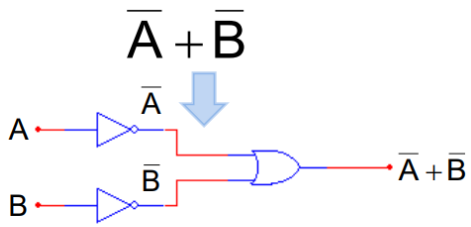
# DeMorgan rules

- $\overline{A.B} = \bar{A} + \bar{B}$

*Proof*



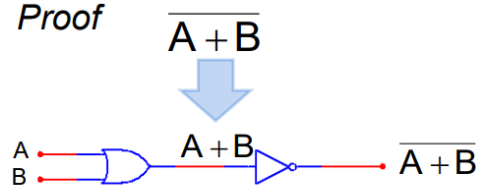

| A | B | A·B | $\overline{A \cdot B}$ |
|---|---|---|---|
| 0 | 0 | 0 | 1 |
| 0 | 1 | 0 | 1 |
| 1 | 0 | 0 | 1 |
| 1 | 1 | 1 | 0 |



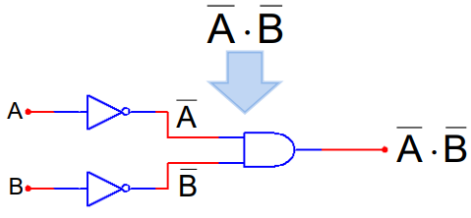

| A | B | $\overline{A}$ | $\overline{B}$ | $\overline{A} + \overline{B}$ |
|---|---|---|---|---|
| 0 | 0 | 1 | 1 | 1 |
| 0 | 1 | 1 | 0 | 1 |
| 1 | 0 | 0 | 1 | 1 |
| 1 | 1 | 0 | 0 | 0 |

- $\overline{A + B} = \bar{A}.\bar{B}$

*Proof*




| A | B | A+B | $\overline{A + B}$ |
|---|---|---|---|
| 0 | 0 | 0 | 1 |
| 0 | 1 | 1 | 0 |
| 1 | 0 | 1 | 0 |
| 1 | 1 | 1 | 0 |

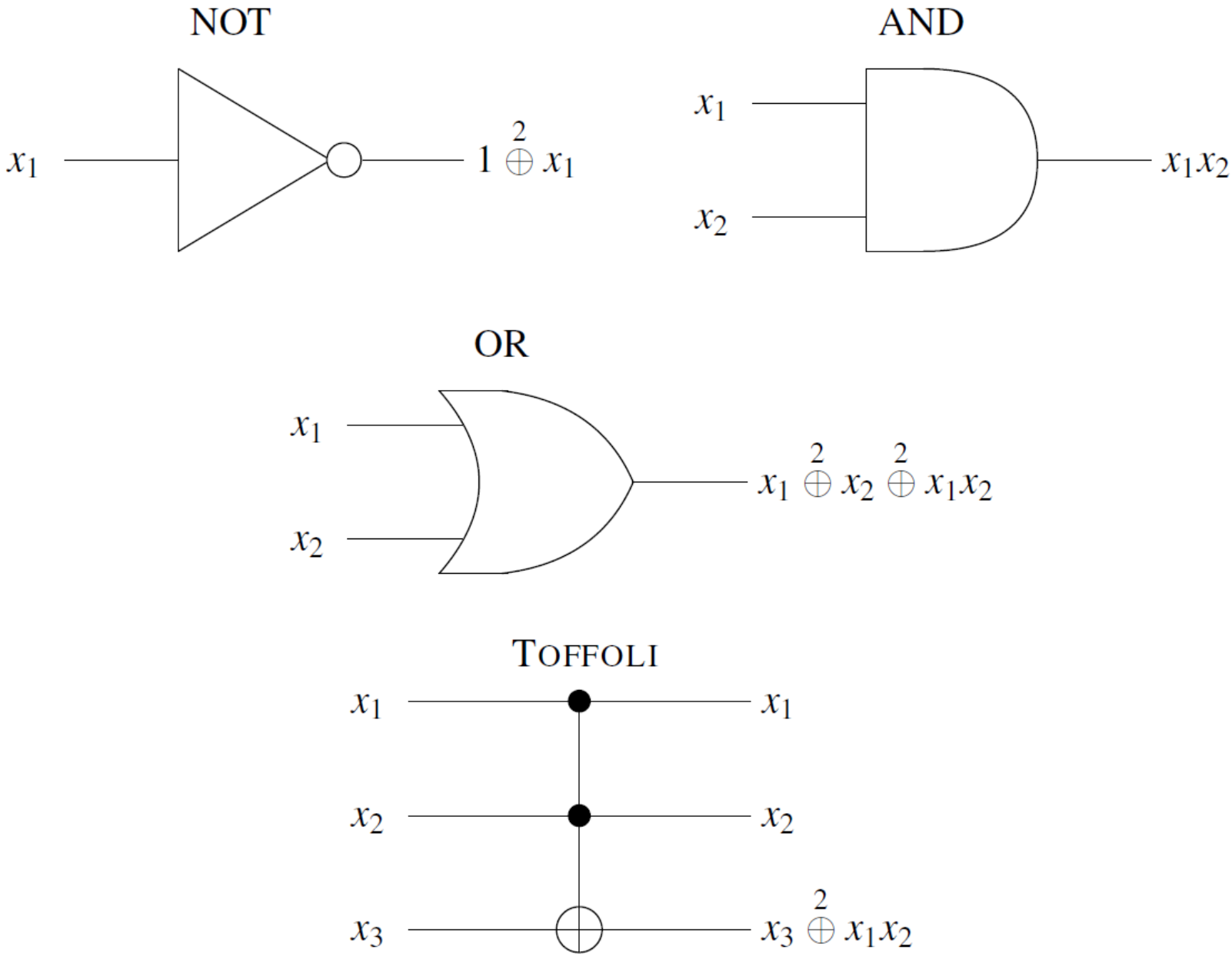



| A | B | $\overline{A}$ | $\overline{B}$ | $\overline{A} \cdot \overline{B}$ |
|---|---|---|---|---|
| 0 | 0 | 1 | 1 | 1 |
| 0 | 1 | 1 | 0 | 0 |
| 1 | 0 | 0 | 1 | 0 |
| 1 | 1 | 0 | 0 | 0 |

*"BREAK THE LINE, CHANGE THE SIGN!"*

Can you prove that

- $\overline{(\overline{x.\bar{y}}).(\bar{y}.z)} = x.\bar{y} + y.\bar{z}$
- $\overline{(\bar{x} + z)(\overline{x.y})} = x.\bar{z} + x.y$ ?


NOT
$x_1$
$1 \overset{2}{\oplus} x_1$
AND
$x_1$
$x_2$
$x_1 x_2$
OR
$x_1$
$x_2$
$x_1 \overset{2}{\oplus} x_2 \overset{2}{\oplus} x_1 x_2$
TOFFOLI
$x_1$
$x_2$
$x_3$
$x_1$
$x_2$
$x_3 \overset{2}{\oplus} x_1 x_2$

# Additional (trivial) gates



$$\begin{aligned}
\mathrm{ID} : \{0,1\} &\longrightarrow \{0,1\} \\
(x_1) &\longmapsto \mathrm{ID}(x_1) := x_1
\end{aligned}$$

$$\begin{aligned}
\mathrm{FALSE} : \{0,1\} &\longrightarrow \{0,1\} \\
(x_1) &\longmapsto \mathrm{FALSE}(x_1) := 0
\end{aligned}$$

$$\begin{aligned}
\mathrm{TRUE} : \{0,1\} &\longrightarrow \{0,1\} \\
(x_1) &\longmapsto \mathrm{TRUE}(x_1) := 1
\end{aligned}$$

$$\begin{aligned}
\mathrm{COPY}^{(1)} : \{0,1\} &\longrightarrow \{0,1\}^2 \\
(x_1) &\longmapsto \mathrm{COPY}(x_1) := (x_1, x_1)
\end{aligned}$$

A set $\mathcal{F}$ of gates $g_1, \ldots, g_L$ is universal if any gate can be expressed as a function of $\mathcal{F}$ only.
$\mathcal{F}$ is constructed using special rules (it is not only a combination of gates). See the following two slides [2].
A series of connected gates is called a **classical circuit**.

[2] from Wolfgang Scherer - Mathematics Of Quantum Computing. An Introduction, Springer (2019)

(i) the $g_1, \ldots, g_K$ are elements of this set, that is,

$$g_1, \ldots, g_K \in \mathcal{F}[g_1, \ldots, g_K]$$

(ii) **padding** operations of the form

$$\begin{aligned} p^{(n)}_{y_1,\ldots,y_l;j_1,\ldots,j_l} : \quad \{0,1\}^n &\longrightarrow \{0,1\}^{n+l} \\ (x_1, \ldots, x_n) &\longmapsto (x_1, \ldots, x_{j_1-1}, y_{j_1}, x_{j_1+1}, \ldots, x_n) \end{aligned}$$

which insert pre-determined bit values $y_1, \ldots, y_l \in \{0,1\}$ at pre-determined slots $j_1, \ldots, j_l \in \{1, \ldots, n+l\}$ are elements of the set, that is, for any $l, n \in \mathbb{N}$, $y_1, \ldots, y_l \in \{0,1\}$ and pairwise distinct $j_1, \ldots, j_l \in \{1, \ldots, n+l\}$

$$p^{(n)}_{y_1,\ldots,y_l;j_1,\ldots,j_l} \in \mathcal{F}[g_1, \ldots, g_K]$$

(iii) **restriction and/or re-ordering** operations

$$\begin{aligned} r^{(n)}_{j_1,\ldots,j_l} : \quad \{0,1\}^n &\longrightarrow \{0,1\}^l \\ (x_1, \ldots, x_n) &\longmapsto (x_{j_1}, \ldots, x_{j_l}) \end{aligned} \tag{5.8}$$

are elements of the set, that is, for any $l, n \in \mathbb{N}$, and pairwise distinct $j_1, \ldots, j_l \in \{1, \ldots, l\}$

$$r^{(n)}_{j_1,\ldots,j_l} \in \mathcal{F}[g_1,\ldots,g_K]$$

(iv) **compositions** of elements of the set belong to the set, that is, for any $h_1 : \{0,1\}^n \to \{0,1\}^m$ and $h_2 : \{0,1\}^l \to \{0,1\}^n$ we have that

$$h_1, h_2 \in \mathcal{F}[g_1,\ldots,g_K] \qquad \Rightarrow \qquad h_1 \circ h_2 \in \mathcal{F}[g_1,\ldots,g_K]$$

(v) **cartesian products** of elements of the set belong to the set, that is, for any $h : \{0,1\}^n \to \{0,1\}^m$ and $k : \{0,1\}^p \to \{0,1\}^q$ we have that

$$h, k \in \mathcal{F}[g_1,\ldots,g_K] \qquad \Rightarrow \qquad h \times k \in \mathcal{F}[g_1,\ldots,g_K]\,,$$

where $h \times k : \{0,1\}^{n+p} \to \{0,1\}^{m+q}$ with

$$\begin{aligned} & h \times k(x_1,\ldots,x_{n+p}) \\ = \; & (h(x_1,\ldots,x_n)_1,\ldots,h(x_1,\ldots,x_n)_m, k(x_{n+1},\ldots,x_{n+p})_1,\ldots,k(x_{n+1},\ldots,x_{n+p})_q)\,. \end{aligned}$$

# Example of product and composition of gates



$$
\begin{aligned}
&\big(\mathrm{ID}\times\mathrm{ID}\times\mathrm{XOR}\big)\circ\big(\mathrm{ID}\times\mathrm{ID}\times\mathrm{AND}\times\mathrm{ID}\big)\circ r^{(5)}_{1,3,2,4,5}\\
&\circ\big(\mathrm{COPY}\times\mathrm{COPY}\times\mathrm{ID}\big)(x_1,x_2,x_3)\\
\underbrace{=}_{(5.7)}&\big(\mathrm{ID}\times\mathrm{ID}\times\mathrm{XOR}\big)\circ\big(\mathrm{ID}\times\mathrm{ID}\times\mathrm{AND}\times\mathrm{ID}\big)\circ r^{(5)}_{1,3,2,4,5}(x_1,x_1,x_2,x_2,x_3)\\
\underbrace{=}_{(5.8)}&\big(\mathrm{ID}\times\mathrm{ID}\times\mathrm{XOR}\big)\circ\big(\mathrm{ID}\times\mathrm{ID}\times\mathrm{AND}\times\mathrm{ID}\big)(x_1,x_2,x_1,x_2,x_3)\\
\underbrace{=}_{(5.4)}&\big(\mathrm{ID}\times\mathrm{ID}\times\mathrm{XOR}\big)(x_1,x_2,x_1x_2,x_3)\\
\underbrace{=}_{(5.5)}&(x_1,x_2,x_1x_2\overset{2}{\oplus}x_3)\\
\underbrace{=}_{(5.6)}&\mathrm{TOF}(x_1,x_2,x_3)\,.
\end{aligned}
$$

# Toffoli gate is universal and reversible



Let us see that a single gate can be considered an universal "set". For n=1, n=2 we show that every gate $\{0,1\}^n \to \{0,1\}$ is a Toffoli "specialization":
for $n = 1$:

$$\mathrm{ID}(x_1) = x_1 = \mathrm{TOF}_1(x_1,1,1) = r_1^{(3)} \circ \mathrm{TOF} \circ p_{1,1;2,3}^{(1)}(x_1)$$

$$\mathrm{FALSE}(x_1) = 0 = \mathrm{TOF}_1(0,0,0) = r_1^{(3)} \circ \mathrm{TOF} \circ p_{0,0,0;1,2,3}^{(0)}(x_1)$$

$$\mathrm{TRUE}(x_1) = 1 = \mathrm{TOF}_1(1,0,0) = r_1^{(3)} \circ \mathrm{TOF} \circ p_{1,0,0;12,3}^{(1)}(x_1)$$

$$\mathrm{NOT}(x_1) = 1 \overset{2}{\oplus} x_1 = \mathrm{TOF}_3(1,1,x_1) = r_3^{(3)} \circ \mathrm{TOF} \circ p_{1,1;1,2}^{(1)}(x_1)\,.$$

for $n = 2$:

$$\mathrm{AND}(x_1,x_2) = x_1x_2 = \mathrm{TOF}_3(x_1,x_2,0) = r_3^{(3)} \circ \mathrm{TOF} \circ p_{0;3}^{(2)}(x_1,x_2)$$

$$\mathrm{XOR}(x_1,x_2) = x_1 \overset{2}{\oplus} x_2 = \mathrm{TOF}_3(1,x_1,x_2) = r_3^{(3)} \circ \mathrm{TOF} \circ p_{1;1}^{(2)}(x_1,x_2)$$

In the book it is proven by induction that if the gates $\{0,1\}^{n-1} \to \{0,1\}$ are Toffoli representable, then this hold for the gates $\{0,1\}^n \to \{0,1\}$ as well.

# Toffoli gate is universal and reversible



With Toffoli gates **only** one can build any classical circuit!

# Quantum gates and circuits

| | Classical | Quantum |
|---|---|---|
| State | $\{0,1\}^n$ | $\psi \in^{\P} H^{\otimes n}$ |
| Gate | $f : \{0,1\}^n \to \{0,1\}^m$ | $U :^{\P} H^{\otimes n} \to^{\P} H^{\otimes n}$ |

Classical and quantum computational processes

Quantum gates transform (multi-)qubit states.

# Quantum gates and circuits

| | Classical | Quantum |
|---|---|---|
| State | $\{0,1\}^n$ | $\psi \in^{\P} H^{\otimes n}$ |
| Gate | $f : \{0,1\}^n \to \{0,1\}^m$ | $U :^{\P} H^{\otimes n} \to^{\P} H^{\otimes n}$ |

Classical and quantum computational processes

Quantum gates transform (multi-)qubit states.

- $U$ is unitary! ($UU^T = I$)

# Quantum gates and circuits

| | Classical | Quantum |
|---|---|---|
| State | $\{0,1\}^n$ | $\psi \in^{¶} H^{\otimes n}$ |
| Gate | $f : \{0,1\}^n \to \{0,1\}^m$ | $U :^{¶} H^{\otimes n} \to^{¶} H^{\otimes n}$ |

Classical and quantum computational processes

Quantum gates transform (multi-)qubit states.

- $U$ is unitary! ($UU^T = I$)
- $^{¶}H$ is a two dimensional Hilbert (qubit) space; $^{¶}H^{\otimes n}$ is a $2n$ dimensional Hilbert space

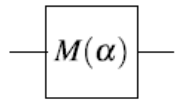
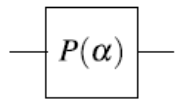
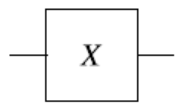
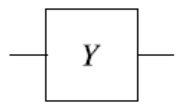
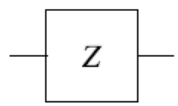
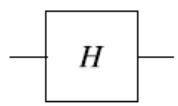
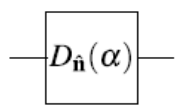
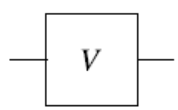
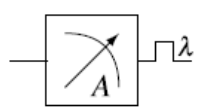
# Quantum gates and circuits

| | Classical | Quantum |
|---|---|---|
| State | $\{0,1\}^n$ | $\psi \in^{¶} H^{\otimes n}$ |
| Gate | $f : \{0,1\}^n \to \{0,1\}^m$ | $U :^{¶} H^{\otimes n} \to^{¶} H^{\otimes n}$ |

Classical and quantum computational processes

Quantum gates transform (multi-)qubit states.

- $U$ is unitary! ($UU^T = I$)
- $^{¶}H$ is a two dimensional Hilbert (qubit) space; $^{¶}H^{\otimes n}$ is a $2n$ dimensional Hilbert space
- the state is read (measured) by a non-unitary operator.

| Name | Symbol | Operator | Matrix in basis $\{\|0\rangle, \|1\rangle\}$ |
|---|---|---|---|
| Identity |  | $\mathbf{1}$ | $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ |
| Phase-factor |  | $M(\alpha) := e^{i\alpha}\mathbf{1}$ | $\begin{pmatrix} e^{i\alpha} & 0 \\ 0 & e^{i\alpha} \end{pmatrix}$ |
| Phase-shift |  | $P(\alpha) := \|0\rangle\langle 0\| + e^{i\alpha}\|1\rangle\langle 1\|$ | $\begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix}$ |
| PAULI-X or Q-NOT |  | $X := \sigma_x$ | $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ |
| PAULI-Y |  | $Y := \sigma_y$ | $\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ |
| PAULI-Z |  | $Z := \sigma_z$ | $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ |
| HADAMARD |  | $H := \frac{\sigma_x+\sigma_z}{\sqrt{2}}$ | $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ |
| Spin-rotation by angle $\alpha$ around $\hat{\mathbf{n}}$ |  | $D_{\hat{\mathbf{n}}}(\alpha)$ | $\begin{pmatrix} \cos\frac{\alpha}{2} - i\sin\frac{\alpha}{2}n_z & -i\sin\frac{\alpha}{2}(n_x - in_y) \\ -i\sin\frac{\alpha}{2}(n_x + in_y) & \cos\frac{\alpha}{2} + i\sin\frac{\alpha}{2}n_z \end{pmatrix}$ |
| Arbitrary unary gate |  | $V$ unitary | $\begin{pmatrix} v_{00} & v_{01} \\ v_{10} & v_{11} \end{pmatrix}$ |
| Measurement of observable $A$ |  | [Not a gate, but a non-unitary transformation of the input-state to an eigenstate of $A$ and delivery of measured value $\lambda$] | |

unary

- X (NOT)-gate: $X = \sigma_x$

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

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

- X (NOT)-gate: $X = \sigma_x$

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

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

It is also denoted by $\oplus$.

- X (NOT)-gate: $X = \sigma_x$

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

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

It is also denoted by $\oplus$.

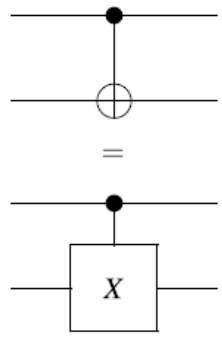
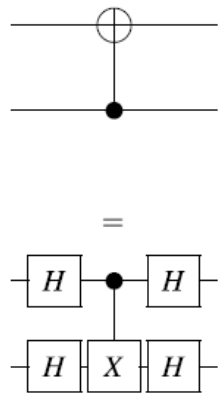
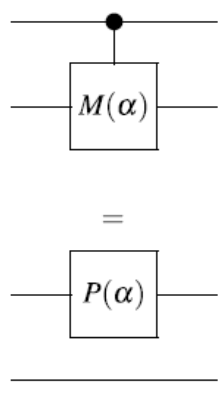
- Hadamard gate $H$

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

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

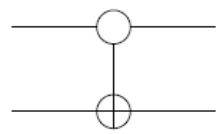
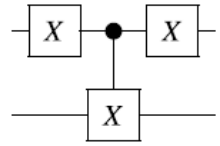
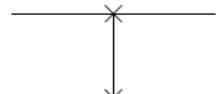
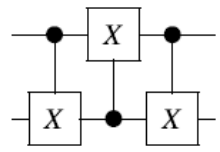
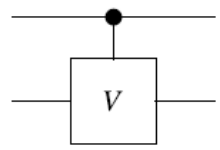
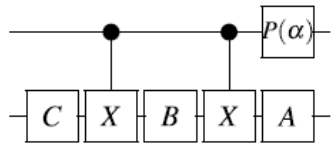
$$H|x_j\rangle = \frac{|0\rangle + e^{\pi i x_j}|1\rangle}{\sqrt{2}}$$

https://qiskit.org/textbook/ch-states/single-qubit-gates.html

| Name | Symbol | Operator | Matrix in computational basis $\{\|0\rangle^2 = \|00\rangle, \|1\rangle^2 = \|01\rangle$ $\|2\rangle^2 = \|10\rangle, \|3\rangle^2 = \|11\rangle\}$ |
|---|---|---|---|
| Controlled NOT (C-NOT) |  | $\Lambda^1(X)$ $=$ $\|0\rangle\langle 0\| \otimes \mathbf{1}$ $+$ $\|1\rangle\langle 1\| \otimes X$ | $\begin{pmatrix} 1&0&0&0 \\ 0&1&0&0 \\ 0&0&0&1 \\ 0&0&1&0 \end{pmatrix}$ |
| C-NOT with control in 2. qbit |  | $\Lambda_1(X)$ $=$ $\mathbf{1} \otimes \|0\rangle\langle 0\|$ $+$ $X \otimes \|1\rangle\langle 1\|$ $=$ $H^{\otimes 2}\Lambda^1(X)H^{\otimes 2}$ | $\begin{pmatrix} 1&0&0&0 \\ 0&0&0&1 \\ 0&0&1&0 \\ 0&1&0&0 \end{pmatrix}$ |
| Controlled phase-multiplication |  | $\Lambda^1(M(\alpha))$ $=$ $\|0\rangle\langle 0\| \otimes \mathbf{1}$ $+$ $\|1\rangle\langle 1\| \otimes e^{i\alpha}\mathbf{1}$ $=$ $P(\alpha) \otimes \mathbf{1}$ | $\begin{pmatrix} 1&0&0&0 \\ 0&1&0&0 \\ 0&0&e^{i\alpha}&0 \\ 0&0&0&e^{i\alpha} \end{pmatrix}$ |

- dots and circles mean condition;
- the gates connected to **dots** ( $\bullet$ ) will apply only if the qubit to be transformed is in state $|1\rangle$. If the input qubit is in state $|0\rangle$ then the gate do not apply and the state remains unchanged.
- the gates connected to **circles** ( $\circ$ ) will apply only if the qubit to be transformed is in state $|0\rangle$.
- $\Lambda : (\cdot)$ is called controlled gate defined as

$$\begin{aligned}\Lambda^{|a\rangle}_{|b\rangle}(V) &:= \mathbf{1}^{\otimes n+1} + |a\rangle\langle a| \otimes (V - \mathbf{1}) \otimes |b\rangle\langle b| \\ &= \mathbf{1}^{\otimes n+1} + \bigotimes_{j=n_a-1}^{0} |a_j\rangle\langle a_j| \otimes (V - \mathbf{1}) \otimes \bigotimes_{j=n_b-1}^{0} |b_j\rangle\langle b_j|\end{aligned}$$

| Name | Symbol | Operator | Matrix in computational basis $\{\|0\rangle^2 = \|00\rangle, \|1\rangle^2 = \|01\rangle$ $\|2\rangle^2 = \|10\rangle, \|3\rangle^2 = \|11\rangle\}$ |
|---|---|---|---|
| C-NOT controlled with $\|0\rangle$ |  | $\Lambda^{\|0\rangle}(X)$ $=$ $\|1\rangle\langle 1\| \otimes \mathbf{1}$ $+$ $\|0\rangle\langle 0\| \otimes X$ | $\begin{pmatrix} 0&1&0&0 \\ 1&0&0&0 \\ 0&0&1&0 \\ 0&0&0&1 \end{pmatrix}$ |
| | $=$  | $=$ $(X \otimes \mathbf{1})\Lambda^1(X)\,(X \otimes \mathbf{1})$ | |
| Swap |  | $S$ $=$ $\|00\rangle\langle 00\| + \|11\rangle\langle 11\|$ $+$ $\|01\rangle\langle 10\| + \|10\rangle\langle 01\|$ | $\begin{pmatrix} 1&0&0&0 \\ 0&0&1&0 \\ 0&1&0&0 \\ 0&0&0&1 \end{pmatrix}$ |
| | $=$  | $=$ $\Lambda^1(X)\Lambda_1(X)\Lambda^1(X)$ | |
| Controlled $V$ |  | $\Lambda^1(V)$ $=$ $\|0\rangle\langle 0\| \otimes \mathbf{1}$ $+$ $\|1\rangle\langle 1\| \otimes V$ | $\begin{pmatrix} 1&0&0&0 \\ 0&1&0&0 \\ 0&0&v_{00}&v_{01} \\ 0&0&v_{10}&v_{11} \end{pmatrix}$ |
| | $=$  | $=$ $(P(\alpha) \otimes A)\Lambda^1(X)\,(\mathbf{1} \otimes B)\Lambda^1(X)\,(\mathbf{1} \otimes C)$ mit $V = M(\alpha)AXBXC$ und $\mathbf{1} = ABC$ | |

# Universal set of quantum gates



**Definition 5.8** For $U_j \in \mathcal{U}\left(\mathbb{H}^{\otimes n_j}\right)$ with $j \in \{1,\ldots,K\}$ we denote by $\mathcal{F}[U_1,\ldots,U_K]$ the set of gates which can be constructed with the $U_1,\ldots,U_K$. This set is defined by the following rules:

(i)
$$U_1,\ldots,U_K \in \mathcal{F}[U_1,\ldots,U_K]$$

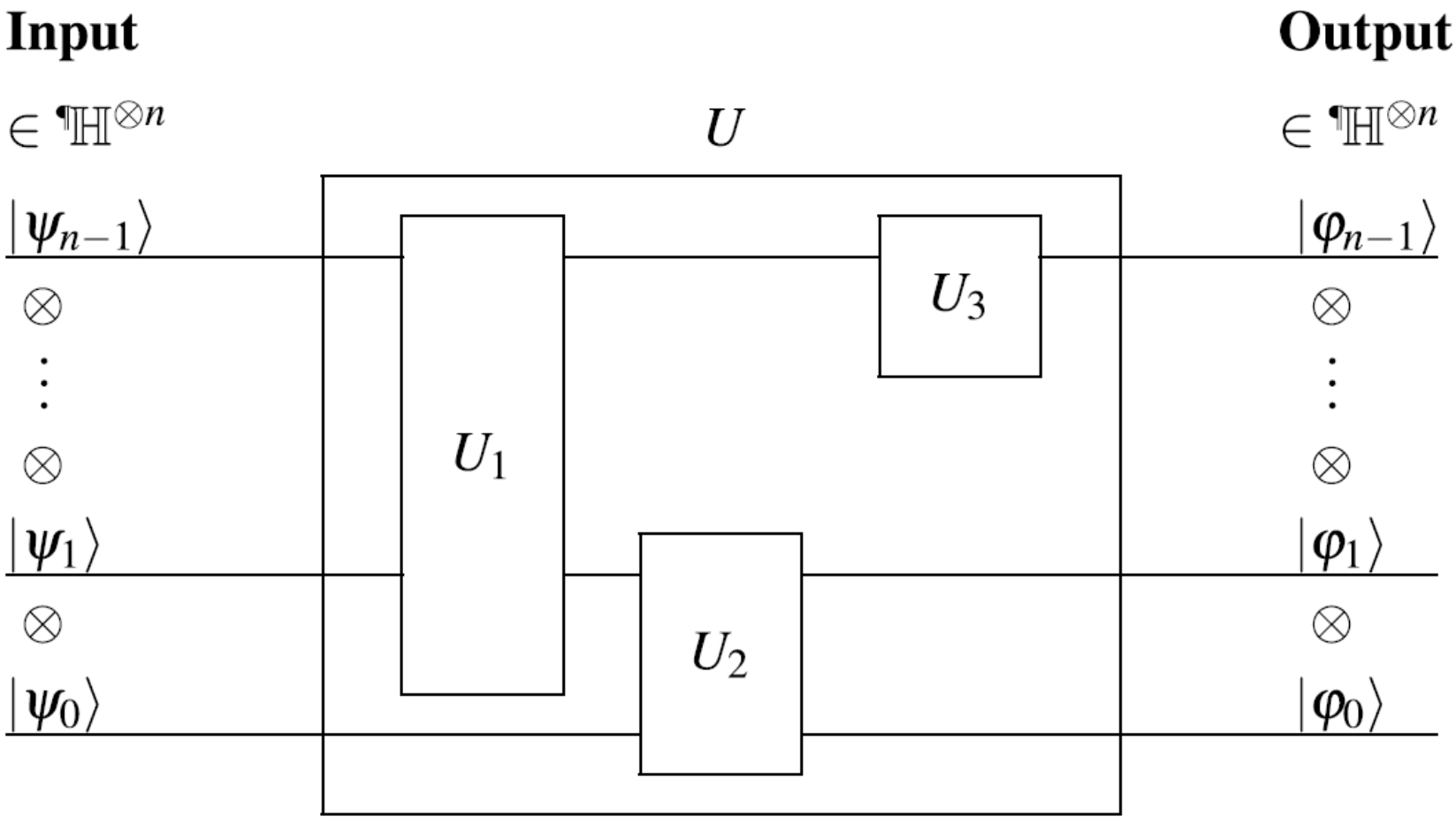
(ii) for any $n \in \mathbb{N}$
$$\mathbf{1}^{\otimes n} \in \mathcal{F}[U_1,\ldots,U_K]$$

(iii) for any $V_1, V_2 \in \mathcal{U}\left(\mathbb{H}^{\otimes n}\right)$ we have
$$V_1, V_2 \in \mathcal{F}[U_1,\ldots,U_K] \quad \Rightarrow \quad V_1 V_2 \in \mathcal{F}[U_1,\ldots,U_K]$$

(iv) for any $V_i \in \mathcal{U}(\mathbb{H}^{\otimes n_i})$ with $i \in \{1,2\}$ we have
$$V_1, V_2 \in \mathcal{F}[U_1,\ldots,U_K] \quad \Rightarrow \quad V_1 \otimes V_2 \in \mathcal{F}[U_1,\ldots,U_K].$$

A set of quantum gates $\mathrm{U} = \{U_1,\ldots,U_J\}$ is called **universal** if any quantum gate $U$ can be constructed with gates from U, that is, if for every quantum gate $U$
$$U \in \mathcal{F}[U_1,\ldots,U_J] \qquad \text{for } U_1,\ldots,U_J \in \mathrm{U}.$$

When acting on a system in the state $\rho \in \mathrm{D}(\mathbb{H})$ the gate $U$ transforms it to a new state $U\rho U^*$.


Input
Output
$\in \mathbb{H}^{\otimes n}$
$U$
$\in \mathbb{H}^{\otimes n}$
$|\psi_{n-1}\rangle$
$\otimes$
$\vdots$
$\otimes$
$|\psi_1\rangle$
$\otimes$
$|\psi_0\rangle$
$U_1$
$U_2$
$U_3$
$|\varphi_{n-1}\rangle$
$\otimes$
$\vdots$
$\otimes$
$|\varphi_1\rangle$
$\otimes$
$|\varphi_0\rangle$

THANK YOU FOR YOUR ATTENTION!

БЛАГОДАРЯ ЗА ВНИМАНИЕТО!