



Introduction to Quantum Information and Quantum Machine Learning

Laboratory - class 4

**Dr Gustaw Szawioła, docent PUT
D. Sc. Eng. Przemysław Głowacki**



Quantum Oracle - Preparation for Grover's Algorithm



Grover's algorithm is a quantum algorithm designed to run on a quantum computer, presented by Lov K. Grover in 1996 [1] and published in 2001 [2]. The algorithm involves searching a database consisting of N elements in order to find a highlighted element in it. This is a similar problem to "reverse" searching a phone book. In a book containing N data, we want to find the name of the owner of a given number.

Computational complexity

While the number of steps required to solve the problem using the classical algorithm is of the order of $O(N)$ Grover's quantum algorithm only needs about $O(\sqrt{N})$ steps, so it allows for a quadratic acceleration of the program execution time.

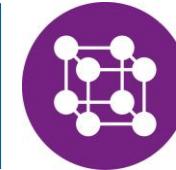
The algorithm involves searching for a given element in an unsorted N -element set. The search problem comes down to determining, by means of unitary transformations, the appropriate index defining a given element in the set.

[1] L. K. Grover. *A fast quantum mechanical algorithm for database search*. In STOC '96: Proceedings p. 212-219, New York, NY, USA (1996)

[2] Grover L.K.: *From Schrödinger's equation to quantum search algorithm*, American Journal of Physics, 69(7): 769-777 (2001)



1. XOR Oracle and Phase Oracle



XOR Oracle

The problem of N data in an unstructured database

Clasiccal maps (function)

$$f: \{0,1\}^n \rightarrow \{0,1\}$$

$$f(x) = \begin{cases} 1, & x = a \\ 0, & x \neq a \end{cases}$$

$a = ?$

↓

$f(x) = 1?$

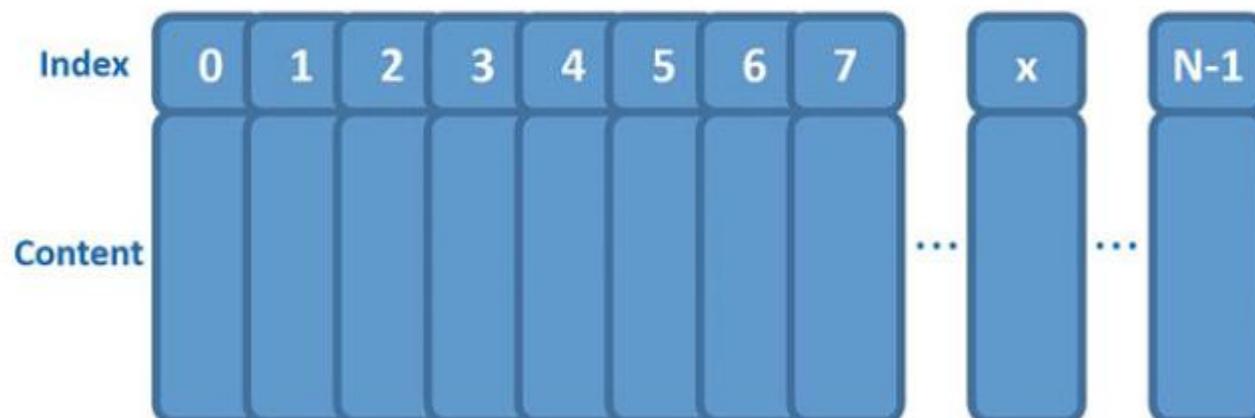


Illustration of a searching process in a database with N entries.
 A function $f(x)$ s used to determine if the target is located at entry x.

Computational Complexity

Classic search

→ Average $\mathcal{O}\left(\frac{N}{2}\right) \sim \mathcal{O}(N)$

Grover's quantum algorithm

→ Average $\mathcal{O}(\sqrt{N})$

Grover's algorithm provides a quadratic speedup over the classical one



XOR Oracle

$$U_f (|y\rangle \otimes |x\rangle) = |y \oplus f(x)\rangle \otimes |x\rangle$$

a = 10

$ i\rangle$	$ y\rangle x\rangle$	$U_f (y\rangle \otimes x\rangle)$
$ 0\rangle$	$ 0\ 00\rangle$	$ 0\ 00\rangle$
$ 1\rangle$	$ 0\ 01\rangle$...
$ 2\rangle$	$ 0\ \textcolor{red}{10}\rangle$	$ 1\ \textcolor{red}{10}\rangle$
$ 3\rangle$	$ 0\ 11\rangle$...
...
$ n-1\rangle$	$ 1\ 11\rangle$	$ 1\ 11\rangle$

Phase Oracle

$$U_f |x\rangle = (-1)^{f(x)} |x\rangle$$

a = 010

$ i\rangle$	$ x\rangle$	$U_f x\rangle$
$ 0\rangle$	$ 0\ 00\rangle$	$ 0\ 00\rangle$
$ 1\rangle$	$ 0\ 01\rangle$...
$ 2\rangle$	$\textcolor{red}{ 0\ 10\rangle}$	$- \textcolor{red}{0\ 10}\rangle$
$ 3\rangle$	$ 0\ 11\rangle$...
...
$ n-1\rangle$	$ 1\ 11\rangle$	$ 1\ 11\rangle$



Create the Matrix of U_f operation

XOR Oracle

<i>j column</i>							
0	1	2	3	4	5	6	7
<i>i row</i>	0	1	2	3	4	5	6
1	0	1	0	1	0	1	0
2	1	0	1	0	1	0	1
3	0	1	0	1	0	1	0
4	1	0	1	0	1	0	1
5	0	1	0	1	0	1	0
6	1	0	1	0	1	0	1
7	0	1	0	1	0	1	0



quantum gate

Phase Oracle

<i>j column</i>							
0	1	2	3	4	5	6	7
<i>i row</i>	0	1	2	3	4	5	6
1	0	1	0	1	0	1	0
2	0	1	0	1	0	1	0
3	1	0	1	0	1	0	1
4	0	1	0	1	0	1	0
5	1	0	1	0	1	0	1
6	0	1	0	1	0	1	0
7	1	0	1	0	1	0	1



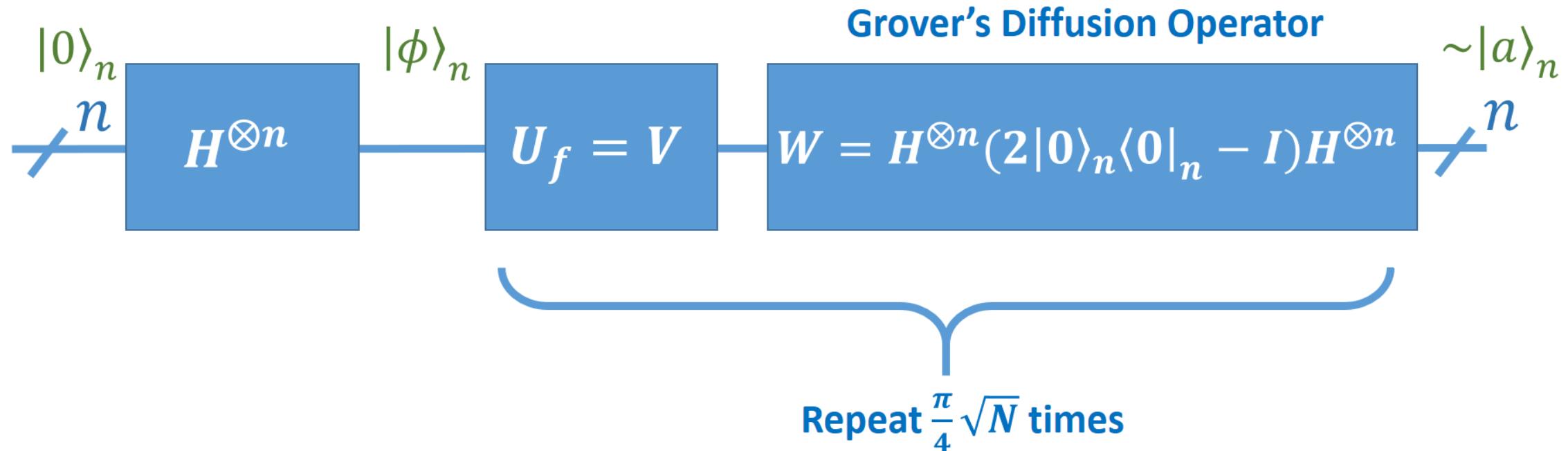
quantum gate



2. Grover's Diffusion operator



Implementation of the Grover's diffusion operator





Implementation of the Grover's diffusion operator

- $|0\rangle_n n\langle 0| = (\)$

- $\hat{\mathbb{I}} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$

- $2 |0\rangle_n n\langle 0| - \hat{\mathbb{I}} = 2(\) - \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} = (\)$



Implementation of the Grover's diffusion operator

- $$\hat{X}^{\otimes n} (2|0\rangle_{nn}\langle 0| - \hat{\mathbb{I}}) \hat{X}^{\otimes n} = 2\hat{X}^{\otimes n}|0\rangle_{nn}\langle 0|\hat{X}^{\otimes n} - \hat{X}^{\otimes n}\hat{\mathbb{I}}\hat{X}^{\otimes n} = 2|1\rangle_{nn}\langle 1| - \underbrace{\hat{X}^{\otimes n}\hat{X}^{\otimes n}}_{=\hat{\mathbb{I}}} =$$

$$= 2|1\rangle_{nn}\langle 1| - \hat{\mathbb{I}}$$

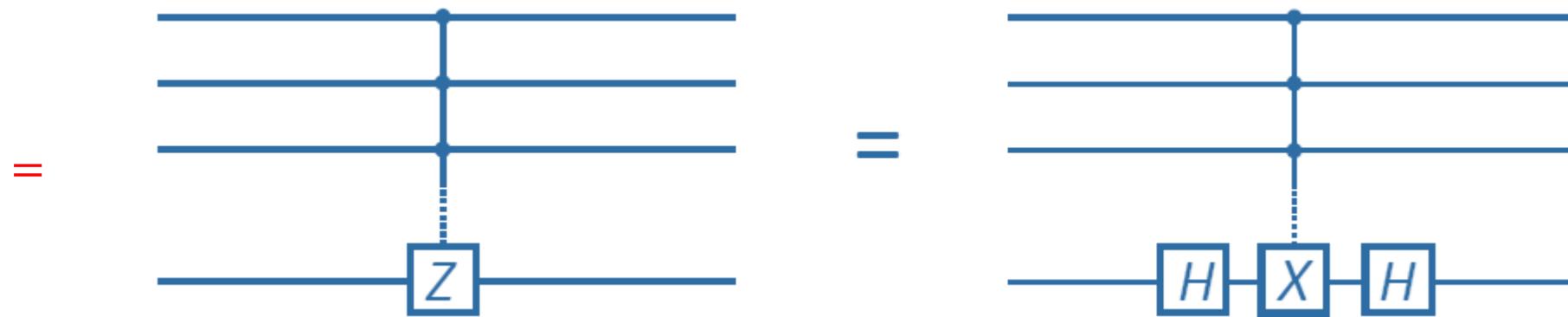
gdzie $|1\rangle_n = \underbrace{|11\dots 1\rangle}_n$

- $$2|1\rangle_{nn}\langle 1| - \hat{\mathbb{I}} = 2(\quad) - \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} = -(\quad) = -(\hat{\mathbb{I}} - 2|1\rangle_{nn}\langle 1|)$$



Implementation of the Grover's diffusion operator

- $(\hat{\mathbb{I}} - 2|1\rangle_n \langle 1|)$



$$C_{n-1}\hat{Z} = (\hat{H} \otimes \hat{\mathbb{I}}) C_{n-1} \hat{X} (\hat{H} \otimes \hat{\mathbb{I}})$$

$$\hat{Z} = \hat{H} \hat{X} \hat{H}, \hat{X}^{\otimes n} \hat{X}^{\otimes n} = \hat{\mathbb{I}}$$

$$\hat{W} = -\hat{H}^{\otimes n} \hat{X}^{\otimes n} C_{n-1} \hat{Z} = \hat{X}^{\otimes n} (\hat{H} \otimes \hat{\mathbb{I}}) C_{n-1} \hat{X} (\hat{H} \otimes \hat{\mathbb{I}}) \hat{X}^{\otimes n} \hat{H}^{\otimes n}$$



Tasks:

$$f(x) = \begin{cases} 1, & x = a \\ 0, & x \neq a \end{cases}$$

1. Create the Matrix of U_f operation:

- 1.1 as XOR Oracle (**Group @9:45 take a=00, Group @11:45 take a=01**)
- 1.2 as Phase Oracle (**Group @9:45 take a=011, Group @11:45 a=100**)

2. From the Matrix of U_f operation create quantum gate

For $n = 3$

3. Calculate the explicit matrix form of operator (lecture 6, frame 35): $|0\rangle_n n\langle 0|$
4. Calculate the explicit matrix form of operator (lecture 6, frame 35-36): $2|0\rangle_n n\langle 0| - \hat{\mathbb{I}}$
5. Prove that (lecture 6, frame 34): $\hat{X}^{\otimes n}(2|0\rangle_n n\langle 0| - \hat{\mathbb{I}})\hat{X}^{\otimes n} = 2|1\rangle_n n\langle 1| - \hat{\mathbb{I}}$
6. Calculate the explicit matrix form of operator: W Grover's diffusion operator (lecture 6, frame 33-43)
7. Using the Qiskit template (file lab4_template.ipynb) create quantum gates representing U_f and W . (Tip use X, H and CNOT gates to create W)



A1 Appendix



XOR Oracle

$$U_f (|y\rangle \otimes |x\rangle) = |y \oplus f(x)\rangle \otimes |x\rangle \quad \textcolor{red}{a = 10}$$

$ i\rangle$	$ y\rangle x\rangle$	$U_f (y\rangle \otimes x\rangle)$
$ 0\rangle$	$ 0\ 00\rangle$	$ 0\ 00\rangle$
$ 1\rangle$	$ 0\ 01\rangle$	$ 0\ 01\rangle$
$ 2\rangle$	$ 0\ \textcolor{red}{10}\rangle$	$ 1\ \textcolor{red}{10}\rangle$
$ 3\rangle$	$ 0\ 11\rangle$	$ 0\ 11\rangle$
$ 4\rangle$	$ 1\ 00\rangle$	$ 1\ 00\rangle$
$ 5\rangle$	$ 1\ 01\rangle$	$ 1\ 01\rangle$
$ 6\rangle$	$ 1\ \textcolor{red}{10}\rangle$	$ 0\ \textcolor{red}{10}\rangle$
$ 7\rangle$	$ 1\ 11\rangle$	$ 1\ 11\rangle$

Phase Oracle

$$U_f |x\rangle = (-1)^{f(x)} |x\rangle \quad \textcolor{red}{a = 010}$$

$ i\rangle$	$ x\rangle$	$U_f x\rangle$
$ 0\rangle$	$ 0\ 00\rangle$	$ 0\ 00\rangle$
$ 1\rangle$	$ 0\ 01\rangle$	$ 0\ 01\rangle$
$ 2\rangle$	$\textcolor{red}{ 0\ 10\rangle}$	$- \textcolor{red}{010}\rangle$
$ 3\rangle$	$ 0\ 11\rangle$	$ 0\ 11\rangle$
$ 4\rangle$	$ 1\ 00\rangle$	$ 1\ 00\rangle$
$ 5\rangle$	$ 1\ 01\rangle$	$ 1\ 01\rangle$
$ 6\rangle$	$ 1\ 10\rangle$	$ 1\ 10\rangle$
$ 7\rangle$	$ 1\ 11\rangle$	$ 1\ 11\rangle$



Construct the matrix for XOR Oracle $a = 10$

base = $\{|0\rangle, |0\rangle, \dots, |n-1\rangle\}$ $\langle 0||0\rangle \Leftrightarrow \langle 0|0\rangle = 1$
base vector numbers \Leftrightarrow decimal numbers

$|j\rangle$ – row, $\langle i|$ – column

$$U_f = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} \langle j| U_f |i\rangle |j\rangle \langle i|$$

$$U_{f,j,i} = \langle j| U_f |i\rangle$$

$$U_{f20} = \langle 2| U_f |0\rangle = \langle 010|000\rangle = 0$$

$$U_{f21} = \langle 2| U_f |1\rangle = \langle 010|001\rangle = 0$$

$$U_{f22} = \langle 2| U_f |2\rangle = \langle 010|1\textcolor{red}{1}0\rangle = 0$$

$$U_{f26} = \langle 2| U_f |6\rangle = \langle 010|0\textcolor{red}{1}0\rangle = 1$$

$$U_{f62} = \langle 6| U_f |2\rangle = \langle 110|1\textcolor{red}{1}0\rangle = 1$$

$$\delta_{ji} = \begin{cases} 1, & j = i \\ 0, & j \neq i \end{cases}$$

$$\begin{aligned} \langle 2| U_f |6\rangle &= \langle 2| \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} \langle j| U_f |i\rangle |j\rangle \langle i| 6\rangle = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} \langle j| U_f |i\rangle \langle 2| j\rangle \langle i| 6\rangle = \\ &= \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} \langle j| U_f |i\rangle \delta_{2j} \delta_{i6} = \sum_{i=0}^{N-1} \langle j| U_f |6\rangle \delta_{2j} = \langle 2| \boxed{U_f |6\rangle} = \langle 010|0\textcolor{red}{1}0\rangle = 1 \end{aligned}$$

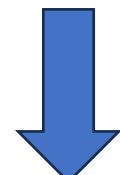
$U_f (|y\rangle \otimes |x\rangle)$
 See table



Create the Matrix of U_f operation

XOR Oracle

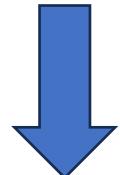
<i>j column</i>							
0	1	2	3	4	5	6	7
<i>i row</i>	0	1	2	3	4	5	6
0	1	0	0	0	0	0	0
1	0	1	0	0	0	0	0
2	0	0	0	0	0	1	0
3	0	0	0	1	0	0	0
4	0	0	0	0	1	0	0
5	0	0	0	0	0	1	0
6	0	0	1	0	0	0	0
7	0	0	0	0	0	0	1



quantum gate

Phase Oracle

<i>j column</i>							
0	1	2	3	4	5	6	7
<i>i row</i>	0	1	2	3	4	5	6
0	1	0	0	0	0	0	0
1	0	1	0	0	0	0	0
2	0	0	-1	0	0	0	0
3	0	0	0	1	0	0	0
4	0	0	0	0	1	0	0
5	0	0	0	0	0	1	0
6	0	0	0	0	0	0	1
7	0	0	0	0	0	0	0



quantum gate



Hint Task 3-5

$$|0\rangle_{n=3} = |000\rangle = |0\rangle \otimes |0\rangle \otimes |0\rangle$$

$$_{n=3}\langle 0| = \langle 000| = \langle 0| \otimes \langle 0| \otimes \langle 0|$$

$$|0\rangle_{n=3} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \otimes (1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0) = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$



Construct the matrix for a 2 bits NOT-gate (N=2)

- $|j\rangle$ – row, $\langle i|$ – column (22.6), $\forall |x\rangle_n = (-1)^{f(x)}|x\rangle_n$ (23.9)

$$\begin{aligned}
 U_{NOT} &= \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} \langle j| U_{NOT} |i\rangle |j\rangle \langle i| = \\
 &= \langle 0| U_{NOT} |0\rangle |0\rangle \langle 0| + \langle 1| U_{NOT} |0\rangle |1\rangle \langle 0| + \langle 0| U_{NOT} |1\rangle |0\rangle \langle 1| + \langle 1| U_{NOT} |1\rangle |1\rangle \langle 1| = \\
 &= \langle 0| |1\rangle |0\rangle \langle 0| + \langle 1| |1\rangle |1\rangle \langle 0| + \langle 0| |0\rangle |0\rangle \langle 1| + \langle 1| |0\rangle |1\rangle \langle 1| = \\
 &= 0 * |0\rangle \langle 0| + 1 * |1\rangle \langle 0| + 1 * |0\rangle \langle 1| + 0 * |1\rangle \langle 1| = |1\rangle \langle 0| + |0\rangle \langle 1| = \\
 &= \begin{pmatrix} 0 \\ 1 \end{pmatrix} * (1 \ 0) + \begin{pmatrix} 1 \\ 0 \end{pmatrix} * (0 \ 1) = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}
 \end{aligned}$$

[źródło: H. Y. Wong, *Introduction to Quantum Computing*, Springer 2022]



The End