1 The Mathematical Model of Quantum Computing

1.1 Qubit

The qubit (**qu**antum **bit**) — is the minimal unit of quantum information which describes the state of the simplest quantum system (just like 1 bit describes the state of the simplest classical system (fig. 1)).

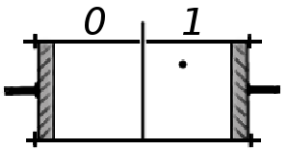

Fig. 1. Szilard's Engine

On the fig. 2 you can see the quantum system where information is encoded by the polarization of a photon.

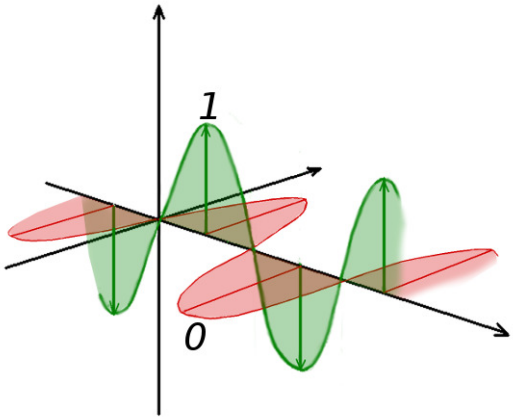

Fig. 2. Quantum information

Mathematically qubit is a unitary vector in the 2-dimensional Hilbert's space. The real parts of coordinates in the example above can encode the angle of the photon polarization, while the imaginary parts - it's phase.

$$|\phi\rangle \in H, \quad \|\phi\| = 1, \quad \dim H = 2. \tag{1}$$

Hilbert's space is a vector space with inner product:

$$|x\rangle = \begin{pmatrix} x_1 \\ x_2 \\ \dots \\ x_n \end{pmatrix}, \quad |y\rangle = \begin{pmatrix} y_1 \\ y_2 \\ \dots \\ y_n \end{pmatrix},$$

$$\langle x|y\rangle = \sum_{i=1}^{n} x_i^* \cdot y_i.$$

Brackets $|\cdots\rangle$ from now on will denote vectors (Dirac's notation in the name of the English physicist Paul Dirac, who invented and used it).

Inner (scalar) product allows us to define angles between vectors:

$$\begin{aligned} \cos\theta &= \frac{|\langle x|y\rangle|}{\|x\| \cdot \|y\|}, \\ \theta = \arccos \frac{|\langle x|y\rangle|}{\|x\| \cdot \|y\|}, &\quad \theta \in [0, \frac{\pi}{2}]. \end{aligned} \tag{2}$$

In Hilbert's spaces all angles vary from 0 to $\pi/2$. Since qubits are unitary vectors, we can simplify (2) by removing the norms:

$$\begin{aligned} \cos\theta &= |\langle x|y\rangle|, \\ \theta &= \arccos|\langle x|y\rangle|. \end{aligned} \tag{3}$$

Orthogonal vectors have zero inner product:

$$|x\rangle \perp |y\rangle \Leftrightarrow \langle x|y\rangle = 0$$

The axes on the fig. 3 are the projections of two orthogonal complex planes. Just as a photon (fig. 2) a qubit can be in the infinite possible number of states.

Classical systems (like Szilard's engine) also can have enormous number of states but we choose to distinguish only few of them (digitization).

For quantum systems there's a similar concept — measurement.

1.2 Qubit Measurement

To obtain the information stored by a quantum system we have to measure it. To do that we have to choose an orthonormal basis in the system's state space. After measurement we obtain one of the vectors of this basis, and the system (subjectively for us) changes its state to this vector.

The probability of the basis vector to become our measurement outcome is defined by the coefficient before this vector in the state description before the measurement:

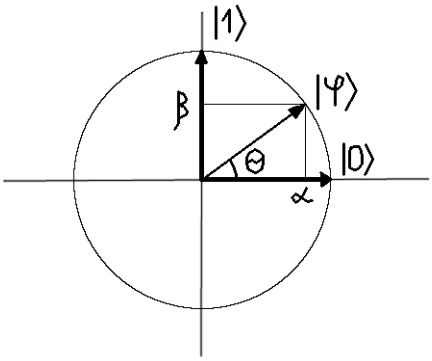

Fig. 3. Qubit

$$\begin{aligned} |\phi\rangle &= \alpha\,|0\rangle + \beta\,|1\rangle\,, \\ \alpha,\ \beta &\in \mathbb{C}, \\ |\alpha|^2 + |\beta|^2 &= 1 \end{aligned} \tag{4}$$

$$\begin{aligned} P(|0\rangle) &= |\alpha|^2. \\ P(|1\rangle) &= |\beta|^2. \end{aligned} \tag{5}$$

Please note:

$$\begin{aligned} \alpha &= \langle 0|\phi\rangle\,, \\ |\alpha| &= \cos\theta, \\ \beta &= \langle 1|\phi\rangle\,, \\ |\beta| &= \sin\theta. \end{aligned} \tag{6}$$

In some sense measurement is similar to digitization — instead of the infinite number of possible states we again distinguish only two.

The choice of basis is important. Consider measuring the following qubit (which is either in the state $|\phi\rangle$ or $|\psi\rangle$ — we don't know which one is it).

$$\begin{aligned} |\phi\rangle &= \frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle\,, \\ |\psi\rangle &= \frac{1}{\sqrt{2}}\,|1\rangle - \frac{1}{\sqrt{2}}\,|0\rangle\,. \end{aligned} \tag{7}$$

In the basis $|0\rangle\,, |1\rangle$ we obtain zero information about the state:

$$\begin{aligned} P(|0\rangle|\phi) = |\langle\phi|0\rangle|^2 = \frac{1}{2} = |\langle\psi|0\rangle|^2 = P(|0\rangle|\psi), \\ P(|1\rangle|\phi) = \frac{1}{2} = P(|1\rangle|\psi). \end{aligned} \tag{8}$$

But with the Hadamard basis $(|+\rangle, |-\rangle)$ we can find out which state was implemented by the system:

$$\begin{aligned} |+\rangle &= \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, \\ |-\rangle &= \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle, \end{aligned} \tag{9}$$

$$\begin{aligned} P(|+\rangle|\phi) = |\langle\phi|+\rangle|^2 = 1, \\ P(|+\rangle|\psi) = |\langle\psi|+\rangle|^2 = 0. \end{aligned} \tag{10}$$

1.3 Multiple qubits

We are going to represent the composite state of several quantum systems as unitary vector in some Hilbert space. To do that we first introduce the basis of this new space:

qubit I	qubit II
$\|0\rangle$	$\|0\rangle$
$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$
$\|1\rangle$	$\|1\rangle$

qubit I	qubit II	vector
$\|0\rangle$	$\|0\rangle$	$\|00\rangle$
$\|0\rangle$	$\|1\rangle$	$\|01\rangle$
$\|1\rangle$	$\|0\rangle$	$\|10\rangle$
$\|1\rangle$	$\|1\rangle$	$\|11\rangle$

And then we describe this composite system in this basis:

qubit I	qubit II
$\|0\rangle$	$\alpha\|0\rangle + \beta\|1\rangle$

qubit I	qubit II	vector
$\|0\rangle$	$\alpha\|0\rangle + \beta\|1\rangle$	$\alpha\|00\rangle + \beta\|01\rangle$

$$\begin{aligned} P(|00\rangle) &= |\alpha|^2, \\ P(|01\rangle) &= |\beta|^2, \\ P(|10\rangle) = P(|11\rangle) &= 0. \end{aligned} \tag{11}$$

qubit I	qubit II	vector
$\alpha\|0\rangle + \beta\|1\rangle$	$\gamma\|0\rangle + \delta\|1\rangle$	$\alpha\gamma\|00\rangle + \alpha\delta\|01\rangle + \beta\gamma\|10\rangle + \beta\delta\|11\rangle$

$$|\alpha\gamma|^2 + |\alpha\delta|^2 + |\beta\gamma|^2 + |\beta\delta|^2 = 1.$$

Now we have to define how these new basis vectors are represented as columns:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

$$|00\rangle = |0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ 0 \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix},$$

$$|01\rangle = |0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ 0 \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix},$$

$$|10\rangle = |1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ 1 \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix},$$

$$|11\rangle = |1\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ 1 \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

1.4 Measuring multiple qubits

The most amazing thing about the introduced above way of describing multiple qubits systems is that any unitary vector in the constructed space describes some real quantum system that can be implemented on real particles.

$$\begin{aligned} \alpha\,|00\rangle + \beta\,|01\rangle + \gamma\,|10\rangle + \delta\,|11\rangle\,, \\ |\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1 \end{aligned} \tag{12}$$

But not all such vectors can be constructed as a tensor product of smaller systems. Consider for example the following set of states:

$$\begin{aligned} &\alpha\,|00\rangle + \beta\,|11\rangle\,, \\ &\alpha\,|01\rangle + \beta\,|10\rangle\,, \\ &|\alpha|^2 + |\beta|^2 = 1. \end{aligned} \tag{13}$$

These are the unitary vectors in a 4-dimensional Hilbert's space so they represent some quantum systems on 2 particles. But these vectors are not tensor products of 2-dimensional vectors, which means that those 2 particles don't have their separate states. The states of this kind are called the entangled states, and particles implementing these states - the entangled particles.

The composite systems can be measured just like the simple 1-qubit systems. To measure a system with 2 qubits we can measure each qubit separately. After measuring the first qubit (let it be $|0\rangle$ for example), we have the following description of the system:

$$|0\rangle \left(\frac{\alpha\,|0\rangle}{\sqrt{|\alpha|^2 + |\beta|^2}} + \frac{\beta\,|1\rangle}{\sqrt{|\alpha|^2 + |\beta|^2}} \right).$$

Measuring the first qubit doesn't alter the state of the second qubit, which is expectable, since those qubits reside on different particles, and when we measure the first particle we don't touch the second.

Now if we try to do the same thing with an entangled state, we can observe, that measuring of the first particle immediately assigns a state to the second particle (the spooky action at a distance).

The many-worlds interpretation of quantum mechanics can describe this situation without any notion of action. For a not entangled state with 2 particles we have 4 different measurement outcomes, each existing in Multiverse:

$\|00\rangle$	$\|01\rangle$
$\|10\rangle$	$\|11\rangle$

The shares of the parts on this picture correspond to the squared coefficients in (12). When we measure the first particle, our state splits on two, each observing only the half of this picture (the upper or the lower).

The Multiverse for an entangled state looks like this:

$\|00\rangle$	$\|11\rangle$

There are only 2 types of universes and measurement of any particle defines for us subjectively the Universe we are in from now.

2 Quntum System Evolution

The evolution of a quantum system can be described by a unitary operator. It means for us that any algorithm for processing quantum data is represented as a unitary operator in the state's space.

Operator U is unitary if and only if

$$UU^* = U^*U = I.$$

Another definition of unitarity:

$$\begin{array}{ll} & \forall \phi \in H \qquad \|U\,|\phi\rangle\,\| = \|\,|\phi\rangle\,\|, \\ \forall \phi, \psi \in H & |\,\langle\, U\,|\phi\rangle \;|\, U\,|\psi\rangle\,\rangle\,| = |\,\langle\phi|\psi\rangle\,|. \end{array} \tag{14}$$

Examples.

Hadamard Tranform

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Unitarity of Hadamard transform:

$$H^* = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = H,$$

$$H^*H = HH = \left(\frac{1}{\sqrt{2}}\right)^2 \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = I.$$

Action of Hadamard transform on $|0\rangle$ and $|1\rangle$:

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

$$H\,|1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = |-\rangle\,.$$

Hadamard transform maps the basis ($|0\rangle$, $|1\rangle$) to the Hadamard basis.

Gate X

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Unitarity:

$$X^* = X,$$

$$XX = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = I.$$

Action:

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

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

Gate X is the quantum NOT gate.

Gate CNOT

CNOT is a 2-qubits gate:

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Unitarity:

$$CNOT|00\rangle = |00\rangle,$$
$$CNOT|01\rangle = |01\rangle,$$
$$CNOT|10\rangle = |11\rangle,$$
$$CNOT|11\rangle = |10\rangle.$$

CNOT maps an orthonormal basis to an orthonormal basis, which means it's a unitary operator.

CNOT is the quantum conditional NOT operator.

To describe the quantum algorithms we are going to use the diagrams of the following type — (fig. 4).

Horizontal lines are qubits (the most significant is on top), the operators are placed on these lines in the order of their application (from left to right). Fig. 4 depicts the application of the Hadamard transform to 2 qubits — $|01\rangle$.

The matrix of this tranform is a 4×4 matrix. What is the look of this matrix?

$$H_2 = H \otimes H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} H & H \\ H & -H \end{pmatrix} =$$

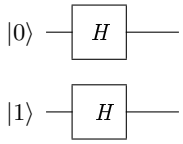

Fig. 4. Quatum Algorithm

$$= \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

$$A\left|x\right\rangle \otimes B\left|y\right\rangle = (A \otimes B)\left|xy\right\rangle. \tag{15}$$

More examples:

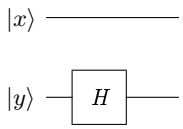

Fig. 5. H on one qubit

$$I \otimes H = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} H & 0 \\ 0 & H \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}.$$

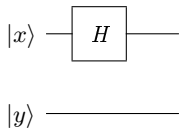

Fig. 6. H on one qubit

$$H \otimes I = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1\,0 \\ 0\,1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} I & I \\ I & -I \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1\,0 & 1 & 0 \\ 0\,1 & 0 & 1 \\ 1\,0 & -1 & 0 \\ 0\,1 & 0 & -1 \end{pmatrix}.$$

CNOT — fig. 7.

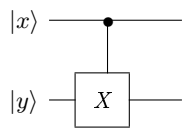

Fig. 7. CNOT, $|x\rangle$ — control, $|y\rangle$ — controlled

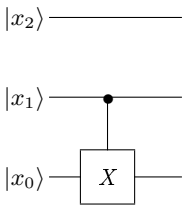

Fig. 8. CNOT. 3 qubits

$$I \otimes CNOT = \begin{pmatrix} CNOT & 0 \\ 0 & CNOT \end{pmatrix}.$$

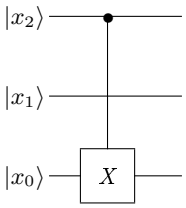

Fig. 9. CNOT. 3 qubits

To discover the matrix let's use the following property:

$$Ae_k = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1k} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2k} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nk} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ \cdots \\ 1 \\ \cdots \\ 0 \end{pmatrix} = \begin{pmatrix} a_{1k} \\ a_{2k} \\ \cdots \\ a_{nk} \end{pmatrix}.$$

The operator from fig. 9:

$$\begin{aligned} |000\rangle &\to |000\rangle, \\ |001\rangle &\to |001\rangle, \\ |010\rangle &\to |010\rangle, \\ |011\rangle &\to |011\rangle, \\ |100\rangle &\to |101\rangle, \\ |101\rangle &\to |100\rangle, \\ |110\rangle &\to |111\rangle, \\ |111\rangle &\to |110\rangle, \end{aligned} \tag{16}$$

$$\begin{pmatrix} 1&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0 \\ 0&0&0&0&0&1&0&0 \\ 0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&0&0&1 \\ 0&0&0&0&0&0&1&0 \end{pmatrix}.$$

2.1 The Hadamard Transform for n qubits

$$H_n |x\rangle = \frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} (-1)^{x \bullet y} |y\rangle, \tag{17}$$

$$x \bullet y = x_0 y_0 \oplus x_1 y_1 \oplus \cdots \oplus x_{n-1} y_{n-1}.$$

Proof by induction

Base:

$$H_1 |x\rangle = \frac{1}{2^{1/2}} (|0\rangle + (-1)^x |1\rangle) = \frac{1}{2^{1/2}} \sum_{y=0}^{1} (-1)^{x \bullet y} |y\rangle.$$

Induction step:

$$H_n |x\rangle = \frac{1}{2^{n/2}} (|0\rangle + (-1)^{x_{n-1}} |1\rangle) \otimes \cdots \otimes (|0\rangle + (-1)^{x_0} |1\rangle) =$$

$$= \frac{1}{\sqrt{2}} |0\rangle \otimes \frac{1}{2^{\frac{n-1}{2}}} (|0\rangle + (-1)^{x_{n-2}} |1\rangle) \otimes \cdots \otimes (|0\rangle + (-1)^{x_0} |1\rangle) +$$

$$+ \frac{1}{\sqrt{2}} (-1)^{x_{n-1}} |1\rangle \otimes \frac{1}{2^{\frac{n-1}{2}}} (|0\rangle + (-1)^{x_{n-2}} |1\rangle) \otimes \cdots \otimes (|0\rangle + (-1)^{x_0} |1\rangle) =$$

$$= \frac{1}{\sqrt{2}} |0\rangle \otimes H_{n-1} |x_{n-2} \cdots x_0\rangle + \frac{1}{\sqrt{2}} (-1)^{x_{n-1}} |1\rangle \otimes H_{n-1} |x_{n-2} \cdots x_0\rangle =$$

$$= \frac{1}{2^{n/2}} \Bigg(|0\rangle \otimes \sum_{y=0}^{2^{n-1}-1} (-1)^{x_0 y_0 \oplus x_1 y_1 \oplus \cdots \oplus x_{n-2} y_{n-2}} |y\rangle +$$

$$+ (-1)^{x_{n-1}} |1\rangle \otimes \sum_{y=0}^{2^{n-1}-1} (-1)^{x_0 y_0 \oplus x_1 y_1 \oplus \cdots \oplus x_{n-2} y_{n-2}} |y\rangle \Bigg) =$$

$$= \frac{1}{2^{n/2}} \Bigg(\sum_{y=0}^{2^{n-1}-1} (-1)^{x_0 y_0 \oplus x_1 y_1 \oplus \cdots \oplus x_{n-2} y_{n-2} \oplus x_{n-1} \cdot 0} |0\rangle |y\rangle +$$

$$+ \sum_{y=0}^{2^{n-1}-1} (-1)^{x_0 y_0 \oplus x_1 y_1 \oplus \cdots \oplus x_{n-2} y_{n-2} \oplus x_{n-1} \cdot 1} |1\rangle |y\rangle \Bigg) =$$

$$= \frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} (-1)^{x \bullet y} |y\rangle .$$