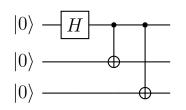


Problem 6. «Quantum entanglement»

The Nobel Prize in Physics in 2022 was awarded to researchers who experimentally investigated quantum entanglement. One of their studies was devoted to a Greenberger-Horne–Zeilinger state $|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$, which is an entangled state of three qubits. This state can be created using the following quantum circuit:



After the measurement, the probability to find the system described by $|GHZ\rangle$ in the state $|000\rangle$ or in the state $|111\rangle$ is equal to 1/2.

When we make measurements in quantum physics, we are able to make *post-selection*. For example, if we post-select the events when the first qubit was in state $|0\rangle$, the second and the third qubits will also be found in the state $|0\rangle$ for sure, this is actually what entanglement means. We also see that the post-selection destroys entanglement of two remaining qubits.

- Q1 But what will happen, if we post-select the events when the 1rst qubit is in the Hadamard state $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$? How can we perform this kind of post-selection if the result of each measurement of a qubit state can be only 0 or 1 and we can only post-select these events? Will the two remaining qubits be entangled after postselection? Design the circuit which will provide an answer.
- Q2 Problem for a special prize! There are two different classes of three-qubit entanglement. One of them is

$$|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle),$$

and the other is

$$|W\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle).$$

Discuss the possible ideas how the difference between these states can be found with the usage of post-selection and measurement. Don't forget that you need to verify entanglement for both types of states!

Turn to the next page.



Page 7 from 13

nsucrypto.nsu.ru

International Olympiad in Cryptography NSUCRYPTO'2022 Second round October 17-24 General, Teams

Remark. Let us briefly formulate the key points of quantum circuits. A qubit is a two-level quantum mechanical system whose state $|\psi\rangle$ is the superposition of basis quantum states $|0\rangle$ and $|1\rangle$. The superposition is written as $|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$, where α_0 and α_1 are complex numbers, called amplitudes, that possess $|\alpha_0|^2 + |\alpha_1|^2 = 1$. The amplitudes α_0 and α_1 have the following physical meaning: after the measurement of a qubit which has the state $|\psi\rangle$, it will be found in the state $|0\rangle$ with probability $|\alpha_0|^2$ and in the state $|1\rangle$ with probability $|\alpha_1|^2$. Note that we can measure qubit, initially given in the state $|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$, in other basis, for example Hadamard basis $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. In order to do this, we consider the state in the form $|\psi\rangle = \alpha'_0 |+\rangle + \alpha'_1 |-\rangle$, where complex amplitudes α'_0, α'_1 have the same physical meaning as α_0 and α_1 . Then we can calculate the probability that the qubit will be in the state $|+\rangle$ or $|-\rangle$ after the measurement and consider the process of post-selection in this case. In order to operate with multi-qubit systems, we consider the bilinear operation $\otimes : |x\rangle, |y\rangle \to |x\rangle \otimes |y\rangle$ on $x, y \in \{0, 1\}$ which is defined on pairs $|x\rangle, |y\rangle$, and by bilinearity is expanded on the space of all linear combinations of $|0\rangle$ and $|1\rangle$. When we have two qubits in states $|\psi\rangle$ and $|\varphi\rangle$ correspondingly, the state of the whole system of these two qubits is $|\psi\rangle \otimes |\varphi\rangle$. In general, for two qubits we have $|\psi\rangle = \alpha_{00}|0\rangle \otimes |0\rangle + \alpha_{01}|0\rangle \otimes |1\rangle + \alpha_{10}|1\rangle \otimes |0\rangle + \alpha_{11}|1\rangle \otimes |1\rangle$. The physical meaning of complex numbers α_{ij} is the same as for one qubit, so we have the essential restriction $|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$. We use more brief notation $|a\rangle \otimes |b\rangle \equiv |ab\rangle$. By induction, this process is expanded on the case of three qubits and more. Mathematically, the entanglement of n-qubits state means that we can not consider this state in the form $|\psi\rangle = |\varphi_1\rangle \otimes |\varphi_2\rangle$, where $|\varphi_1\rangle$ and $|\varphi_2\rangle$ are some states of m and n - m qubits, correspondingly. In order to verify your circuits, you can use different quantum circuit simulators, for example https://algassert.com/quirk.



Page 8 from 13

nsucrypto@nsu.ru