A single quantum cannot be cloned

Reading Report

Nisim Hurst A01012491

Friday 19 October 2018

Abstract

The article was written by Wootters and Zurek[1] and published on the Nature magazine back in 1982. The article presents a proof that due to the nature of quantum mechanical systems, there is no possible cloning or amplification device that can be applied to qubits.

Hypothesis and Evidence

The author states there is no cloning of quantum states. That means that the complex components from a qubit cannot be copied to a second qubit without affecting the first one.

The evidence stems from the fact that transformations in quantum mechanics should be representable by a unitary linear operator, i.e. by the principle of superposition and solving the Schrödinger equation. Thus, the author presents a proof whose origin lies in the unsatisfiability of the superposition principle.

Contribution

The article provides a generalized no-cloning theorem for any quantum system initially articulated by Park. The authors demonstrate that the equation for a perfect amplifier that produces identical pure states than the original qubit is impossible. However, if the qubit is in one of the eigenstates of the Hilbert space then it would be possible to copy it, i.e. pure states would be produced.

The authors explore mainly the photons quantum system, that considers angular momentum and polarization. In those systems angular momentum is not a problem. Thus, the authors use the linearity of quantum systems to provide their proof.

The no-cloning theorem imply many logical consequences, e.g. the impossibility of using error correction techniques on quantum states. Another consequence is the impossibility of accurately measure a qubit to teleport its state to a classical bit state and back into another quantum system without modifying it. Superluminal communication is also opted out.

Limitations and Weaknesses

The article is overwhelmingly focused on producing a copy of a photon conserving the angular momentum. All this analysis miss the principal point that was already proven. The article is unbalanced on this area, other quantum systems should be taken into consideration.

Future Work

Wooter's and Zurek's theorem is the base of quantum cryptography distribution protocols.

References

[1] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," $\it Nature, vol. 299, no. 5886, pp. 802–803, 1982.$