Helstrom theorem from the no-signaling condition

Won-Young Hwang*
Department of Physics Education, Chonnam National University, Kwangjoo 500-757, Republic of Korea
(Received 15 February 2005; published 14 June 2005)

We prove a special case of the Helstrom theorem by using the no-signaling condition in the special theory of relativity that faster-than-light communication is impossible.

DOI: 10.1103/PhysRevA.71.062315 PACS number(s): 03.67.Hk, 03.65.Wj

Quantum bits (qubits) are fundamentally different from classical bits in that unknown qubits cannot be copied with unit efficiency [1–3] (the no-cloning theorem). Another related property of qubits is that nonorthogonal qubits cannot be distinguished with certainty [4].

Interestingly, however, it has been found that the no-signaling condition is entangled with other impossibility proofs [5–8]. In particular, it has been shown that the no-signaling condition gives the same tight bound on probability of conclusive measurement as obtained by quantum mechanical formula [7].

In this paper, we add one in the list of theorems that can be proven by the no-signaling condition. We prove a special case of the Helstrom theorem [9]. The result in this paper is closely related to other's works but different. In particular, our argument is quite similar to the one in Ref. [5]. Our contribution is an observation that violation of the Helstrom theorem implies that two appropriately chosen (different) decompositions of the same density operator can be discriminated. This paper is organized as follows. We describe the proposition that we will prove. We prove it by the no-signaling condition and then we conclude.

Roughly speaking, the Helstrom theorem means that the more nonorthogonal two qubits are, the more difficult it is to discriminate them by positive operator valued measurement [4]. Let us consider a special case of the Helstrom theorem.

Proposition 1. Consider two nonorthogonal qubits, $|\alpha\rangle$ and $|\beta\rangle$, whose overlap, $|\langle\alpha|\beta\rangle|^2$, is between 0 and 1. We are given a qubit that is either $|\alpha\rangle$ or $|\beta\rangle$ with equal a priori probability, $1/2$. We want to identify the qubit quantum mechanically. Identifier of the qubit gives either an output, 0, or the other output, 1. P_E is the probability of making error in the identification. Minimal value of P_E is given by $P_E^m = (1/2)[1-\sqrt{1-|\langle\alpha|\beta\rangle|^2}]$ [4].

(Proposition 1 has interesting applications in quantum cryptography, e.g., the Bennett 1992 quantum key distribution protocol [10] and quantum remote gambling protocol [11].) Before we prove Proposition 1, let us introduce the following. Any pure qubit $|i\rangle\langle i|$ can be represented by a three-dimensional Euclidean Bloch vector $\hat{r}_i$ as $|i\rangle\langle i| = (1/2)(\mathbf{1}+\hat{r}_i\cdot\vec{\sigma})$ [12]. Here $\mathbf{1}$ is the identity operator, $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$, and $\sigma_x, \sigma_y, \sigma_z$ are Pauli operators. Two Bloch vectors corresponding to $|\alpha\rangle$ and $|\beta\rangle$ are $\hat{r}_\alpha$ and $\hat{r}_\beta$, respectively. We define an angle between $\hat{r}_\alpha$ and $\hat{r}_\beta$ to be 2θ. That is, $|\langle\alpha|\beta\rangle|^2 = \cos^2\theta$. A pure state $|\gamma\rangle$ is defined as that its Bloch vector $\hat{r}_\gamma$ bisects the two Bloch vectors $\hat{r}_\alpha$ and $\hat{r}_\beta$ in the same plane, namely, $\hat{r}_\gamma = C(\hat{r}_\alpha + \hat{r}_\beta)$ where C is a constant for normalization. A pure state $|\delta\rangle$ is defined as its Bloch vector $\hat{r}_\delta$ makes an angle $\pi/2$ and $\pi/2+\theta$ with the Bloch vector $\hat{r}_\gamma$ and $\hat{r}_\alpha$, in the same plane, respectively. A pure state $|-\delta\rangle$ is defined as its Bloch vector $\hat{r}_{-\delta}$ is the negative of that of $|\delta\rangle$, namely $-\hat{r}_\delta$. Note that all Bloch vectors here are in the same plane.

Let us start the proof. Consider an entangled state for Alice and Bob, who are supposed to be remotely separated usually,

$$|\psi\rangle = \sqrt{p}|0\rangle_A|\alpha\rangle_B + \sqrt{1-p}|1\rangle_A|\delta\rangle_B. \tag{1}$$

Here, $|0\rangle$ and $|1\rangle$ are two orthogonal qubits, A and B denote Alice and Bob, and $p = 1/(1+\sin\theta)$ and $1-p = \sin\theta/(1+\sin\theta)$. If Alice performs a measurement in the $\{|0\rangle, |1\rangle\}$ basis, therefore, Bob is given a mixture of $|\alpha\rangle\langle\alpha|$ and $|\gamma\rangle\langle\gamma|$ with respective probabilities p and $1-p$. Then Bob's density operator ρ_B is given by $\rho_B = p|\alpha\rangle\langle\alpha| + (1-p)|\gamma\rangle\langle\gamma| = (1/2)\{\mathbf{1} + \hat{r}_B\cdot\vec{\sigma}\}$, where $\hat{r}_B = p\hat{r}_\alpha + (1-p)\hat{r}_\gamma$. Note that the Bloch vector of a mixture is given by sum of Bloch vectors of pure states constituting the mixture with corresponding probabilities as weighting factors. However, the theorem of Gisin-Hughston-Jozsa-Wootters says that, with the state in Eq. (1), Alice can generate any decomposition of Bob's mixture [5,12,13] by the appropriate choice of her measurement basis. (Usually this theorem is known as that of the latter three authors. However, the theorem had been already demonstrated by Gisin [5].) However, we have a relation that $\hat{r}_B = p\hat{r}_\alpha + (1-p)\hat{r}_\gamma = p\hat{r}_\beta + (1-p)\hat{r}_{-\gamma}$, which means that the density operator ρ_B can also be decomposed as

$$\rho_B = p|\beta\rangle\langle\beta| + (1-p)|-\gamma\rangle\langle-\gamma|.$$

Thus the state in Eq. (1) can also be written as

$$|\psi\rangle = \sqrt{p}|0'\rangle_A|\beta\rangle_B + \sqrt{1-p}|1'\rangle_A|-\delta\rangle_B, \tag{2}$$

where $\{|0'\rangle, |1'\rangle\}$ is another orthogonal basis.

Now let us assume that there exists a binary detector of any kind whose probability of error P_E is less than P_E^m for the two nonorthogonal states $|\alpha\rangle$ and $|\beta\rangle$. That is, the detector gives the outcomes 0 and 1 for $|\alpha\rangle$ and $|\beta\rangle$, respectively, with a probability $1-P_E$. Then Alice and Bob can do faster-than-light communication in the following way. First Alice and Bob prepare many copies of the state in Eq. (1). If Alice wants to send a bit 0 (bit 1) then Alice performs measure-

*Electronic address: wyhwang@chonnam.ac.kr

ments on her qubits in the $\{|0\rangle,|1\rangle\}(\{|0'\rangle,|1'\rangle\})$ basis. Bob can discriminate the two cases by performing measurements on his qubits using the detector: In the case of bit 0 (bit 1), $|\alpha\rangle(|\beta\rangle)$ is generated with probability p at Bob's site. Then $p(1-P_E)>1/2$ because $P_E<P_E^m$ and $p(1-P_E^m)=1/2$. That is, in the case of bit 0 (bit 1), the detector gives outcome 0 (outcome 1) with a probability larger than $1/2$. Therefore, whatever outcomes are given for the other state, Bob can discriminate the two cases.

We proved a special case of Helstrom theorem, Proposition 1, by using no-signaling condition in special theory of relativity that faster-than-light communication is impossible.

I thank Marco Piani very much for a helpful correction.

[1] D. Dieks, Phys. Lett. **92A**, 271 (1982).
[2] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982).
[3] H. P. Yuen, Phys. Lett. **113A**, 405 (1986).
[4] A. Chefles, Contemp. Phys. **41**, 401 (2000), and references therein.
[5] N. Gisin, Helv. Phys. Acta **62**, 363 (1989).
[6] N. Gisin, Phys. Lett. A **242**, 1 (1998).
[7] S. M. Barnett and E. Andersson, Phys. Rev. A **65**, 044307 (2002).
[8] A. K. Pati and S. L. Braunstein, Phys. Lett. A **315**, 208 (2003).
[9] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic, New York, 1976).
[10] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[11] W.-Y. Hwang, D. Ahn, and S.-W. Hwang, Phys. Rev. A **64**, 064302 (2001).
[12] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, (Cambridge University Press, Cambridge, U.K., 2000).
[13] L. P. Hughston, R. Jozsa, and W. K. Wootters, Phys. Lett. A **183**, 14 (1993).