Possibility of upper-bounding dimension of quantum states device-independently

Won-Young Hwang *

1Department of Physics Education, Chonnam National University, Guwngju 500-757, Republic of Korea

We discuss possibility of upper-bounding dimension of quantum states device-independently. Provided that the states are pure, it is possible to generate certain four states whose dimension is bounded by two.

PACS numbers: 03.67.-a, 03.67.Dd

I. INTRODUCTION

Two-dimensional quantum state, or quantum bit (qubit), has been an important element in quantum information processing. Theoretically, qubit is the most simple one to deal with. In practice, however, it is difficult to generate perfect qubits because no-device is perfect. The difficulty is not a serious problem in most cases if degree of imperfection is small. However, in quantum key distribution (QKD) it is a serious problem because effect of the imperfection can be cleverly amplified by an eavesdropper [1, 2]. In fact, problems due to unavoidable imperfections have been major issues in practical QKD [2].

Recently, semi-device-independent QKD has been proposed, whose proviso is that dimension of source is bounded by two. That is, source is qubit [3]. Moreover, it has been shown [4, 5] that currently the most practicable one, the measurement-device-independent QKD gets full security provided that quantum states are two-dimensional. Thus an interesting issue is how to upper-bound dimension of quantum states device-independently. Recently studied “dimension witness” is a one which lower-bounds dimensions.

On the other hand, it has been shown with use of no-signaling principle that even with un-characterized devices it is possible to generate four quantum states for which the unambiguous state discrimination [7] is not possible [8]. The result implies that, if the states are pure, dimension of the states is bounded by three, because unambiguous state discrimination is always possible for linearly independent states [4]. In this paper, we describe the prescription to generate the four states. Then we show that dimension of the generated states is bounded by two if the states are pure.

II. TO GENERATE THE FOUR STATES

Let us recall a method to generate a set of qubits using Bell states. The set of qubits, \{ |0\rangle, |1\rangle, |+\rangle, |-\rangle \}, is the most widely used one in QKD. Here, |0\rangle and |1\rangle are orthonormal states and |±⟩ = (1/√2)(|0⟩ ± |1⟩). Assume that a sender, normally called Alice, wants to generate the states. If Alice has ideal Bell state and can perform ideal measurements, she can generate the ideal states; Alice has a Bell state

$$|φ^+⟩ = \frac{1}{\sqrt{2}}(|0⟩_A |0⟩_B + |1⟩_A |1⟩_B),$$

where $A_1$ and $A_2$ denote two separated boxes in which corresponding quantum states are kept. Assume that $M_0$ ($M_1$) is a measurement composed of $\{ |0⟩, |1⟩, 1⟩, 1⟩ \}$ ($\{ |+⟩, |−⟩, 1⟩, 1⟩ \}$). Alice chooses a value $i (i = 0, 1)$ with equal probability. She performs $M_i$ on quantum state in box $A_1$. Then, in box $A_2$, each one of the four qubit states are generated with equal probability. However, in practice, every component has unavoidable imperfections. Hence the actually generated state deviates from the ideal states. As a result, the dimension of the actual state also deviates from two.

However, it is possible to generate states whose dimension is strictly bounded by two even with un-characterized imperfect devices, provided that the states are pure. In brief, Alice follows the same procedures with imperfect real devices as she did with the ideal ones: She prepares a bipartite quantum state which we denote by $|φ⟩$. Then one part (the other one) of the state is kept into a box with a label $A_1$ (a label $A_2$). She randomly chooses a binary bit $i$. Alice performs a measurement $M_i$ on quantum state in box $A_1$ obtaining an outcome $j$ between 0 and 1. She attaches a label $(i, j)$ on box $A_2$. If $|φ⟩ = |φ^+⟩$ and $M_i = M_i$, the states in box $A_2$ with a label $(0, 0), (0, 1), (1, 0), (1, 1)$, are $|0⟩, |1⟩, |+⟩, |-⟩$, respectively. However, for any state $|φ⟩$ and any measurement $M_i$, our argument below for two-dimensionality is valid. However, in order that the generated states be close to the specified qubits, the state and measurement should be close to the Bell state and $M_i$.

III. BOUNDED BY TWO DIMENSION

Let $p(j|i)$ denote a probability that an outcome $j$ is obtained when Alice performed a measurement $M_i$. Here $\sum_j p(j|i) = 1$ for each $i$. Here the state in box $A_2$ with a label $(i, j)$ is supposed to be pure and denoted by $|i, j⟩$. Clearly, the density operator of the states in box $A_2$, 

*Email: wyhwang@jnu.ac.kr
which is $tr_{A_1}(|\phi^+\rangle\langle\phi^+|)$, must not depend on $i$ (see [10]).

\[
    p(0|0)\langle 0, 0| + p(1|0)\langle 0, 1| + p(1|1)\langle 0, 1| + p(0|1)\langle 0, 1|
\]
\[
    = p(0|1)(1 - |0, 1|1, 1|)^2|0, 1).
\]

Note that Eq. (2) is satisfied rigorously even if the states are prepared with un-characterized imperfect devices as long as Alice followed the procedures for preparation. Otherwise, superluminal communication become possible violating a fundamental principle in nature. The only case when Eq. (2) can be violated is that Alice fails to follow the procedure, e.g., an additional information carrier was delivered to the box-$A_2$ after measuring state in box-$A_1$. We assume that there was no such hidden signal-

\[
    p(0|0)(0, 0)\langle 0, 0| + p(1|0)\langle 0, 1| + p(1|1)\langle 0, 1| + p(0|1)\langle 0, 1|
\]
\[
    = p(0|1)(1 - |0, 1|1, 1|)^2|0, 1).
\]

In conclusion, we discussed a possibility to generate a set of four state whose dimension is bounded by two, provided that the states are pure. This might be a clue to find how to upper-bound a state without any proviso.

**Acknowledgement**

This study was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2010-0007208).

[1] H. P. Yuen, Quantum Semiclassical Opt. 8, 939 (1996).
[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lütkenhaus, M. Peev, Rev. Mod. Phys. 81, 1301 (2009).
[3] M. Pawlowski and N. Brunner, Phys. Rev. A 84, 010302 (2011).
[4] Z.-Q. Yin et al., Phys. Rev. A 88, 062322 (2013).
[5] Z.-Q. Yin et al., arXiv:1407.1921v3[quant-ph].
[6] N. Brunner et al., Phys. Rev. Lett. 100, 210503 (2008).
[7] I.D. Ivanovic, Phys. Lett. A 123, 257 (1987).
[8] W.-Y. Hwang, J. Korean Phys. Soc. 60, 1837 (2012).
[9] A. Chefles, Phys. Lett. A 239, 339 (1998).
[10] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information, (Cambridge Univ. Press, Cambridge, U.K., 2000.)
[11] A. Acín, N. Gisin, and L. Masanes, Phys. Rev. Lett. 97, 010503 (2006).
[12] H.-W. Li, Z.-Q. Yin, Y.-C. Wu, X.-B. Zou, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Phys. Rev. A 84, 034301 (2011).