(4,1)-Quantum random access coding does not exist—one qubit is not enough to recover one of four bits

M Hayashi¹,⁶, K Iwama², H Nishimura³,⁷, R Raymond⁴ and S Yamashita⁵

¹ ERATO-SORST Quantum Computation and Information Project, Japan Science Technology Agency, 5-28-3 Hongo, Bunkyo-ku, Tokyo 113-0033, Japan
² School of Informatics, Kyoto University, Yoshida-Honmachi, Sakyo-ku, Kyoto 606-8501, Japan
³ School of Science, Osaka Prefecture University, 1-1 Gakuen-cho, Sakai 599-8531, Japan
⁴ Tokyo Research Laboratory, IBM Japan, 1623-14 Shimotsuruma, Yamato 242-8502, Japan
⁵ Graduate School of Information Science, Nara Institute of Science and Technology, 8916-5 Takayama-cho, Ikoma 630-0192, Japan

E-mail: masahito@qci.jst.go.jp, iwama@kuis.kyoto-u.ac.jp, hnishimura@mi.s.osakafu-u.ac.jp, raymond@jp.ibm.com and ger@is.naist.jp

New Journal of Physics 8 (2006) 129
Received 7 June 2006
Published 4 August 2006
Online at http://www.njp.org/
doi:10.1088/1367-2630/8/8/129

Abstract. An \((n, 1, p)\)-quantum random access (QRA) coding, introduced by Ambainis et al (1999 ACM Symp. Theory of Computing p 376), is the following communication system: the sender which has \(n\)-bit information encodes his/her information into one qubit, which is sent to the receiver. The receiver can recover any one bit of the original \(n\) bits correctly with probability at least \(p\), through a certain decoding process based on positive operator-valued measures. Actually, Ambainis et al shows the existence of a \((2, 1, 0.85)\)-QRA coding and also proves

---

6 Also, Superrobust Computation Project, Information Science and Technology Strategic Core (21st Century COE by MEXT), Graduate School of Information Science and Technology, The University of Tokyo, Japan.
7 Author to whom any correspondence should be addressed.
the impossibility of its classical counterpart. Chuang immediately extends it to a $(3, 1, 0.79)$-QRA coding and whether or not a $(4, 1, p)$-QRA coding such that $p > 1/2$ exists has been open since then. This paper gives a negative answer to this open question. Moreover, we generalize its negative answer for one-qubit encoding to the case of multiple-qubit encoding.

### Contents

1. Introduction .................................... 3
   1.1. Related work ........................................ 3
2. Quantum random access coding 3
3. Main results 6
4. Applications to network coding 8
5. Concluding remarks 10
Acknowledgments 10
References 11

1. Introduction

The state of $n$ quantum bits (qubits) is represented by a $2^n$-dimensional complex-valued unit vector and seems to hold much more information than (classical) $n$ bits. However, due to the famous Holevo bound [1], this is not true information theoretically, i.e., we need $n$ qubits to transmit $n$-bit information faithfully. As an interesting challenge to this most basic fact in quantum information theory, Ambainis et al introduced the notion of quantum random access (QRA) coding [2]. (The paper [3] includes the contents of [2] and their improvement in [4].) They explored the possibility of using much fewer qubits if the receiver has to recover only partial bits, say one bit out of the $n$ original ones, which are not known by the sender in advance.

As a concrete example, they give $(2, 1, 0.85)$-QRA coding; the sender having two-bit information sends one qubit and the receiver can recover any one of the two bits with probability at least 0.85. It is also proved that this is not possible classically, i.e., if the sender can transmit one classical bit, then the success probability is at most 1/2. This $(2, 1, 0.85)$-QRA coding is immediately extended to $(3, 1, 0.79)$-QRA coding by Chuang (as mentioned in [2]) and it has been open whether we can make a further extension (i.e., whether there is an $(n, 1, p)$-QRA coding such that $n \geq 4$ and $p > 1/2$) since then.

This paper gives a negative answer to this open question, namely, we prove there is no $(4, 1, p)$-QRA coding such that $p$ is strictly greater than $1/2$. Our proof is a reduction to the well-known geometric fact that a three-dimensional (3D) ball cannot be divided into 16 nonempty regions by four planes. (Interestingly, the proof for the non-existence of a classical counterpart of $(2, 1, p)$-QRA coding in [2] uses a similar geometric fact, i.e., a straight line cannot stab all insides of the four quarters of a 2D square.) Our result has nice applications to the analysis of quantum network coding which was introduced very recently [5].

In general, the sender is allowed to send $m \geq 1$ qubits; such a system is denoted by $(n, m, p)$-QRA coding. Our result can be extended to this general case, namely we can show that $(2^m, m, p)$-QRA coding with $p > 1/2$ does not exist. This is quite tight since we can see that a
Thus, this bound is asymptotically tight and has many applications such as proving the limit of \((n, m, p)\) \((n, m, p)\)-QRA coding exists by reducing a communication complexity upper bound to the QRA coding [6, 7].

This paper is organized as follows. In the rest of section 1, we discuss the related work. Section 2 gives the formal definition of \((n, 1, p)\)-QRA coding and the optimal codings for cases \(n = 2\) and \(3\). Also, we discuss a possible strategy for \(n \geq 4\). In section 3, we show the non-existence of \((4, 1, p)\)-QRA coding with \(p > 1/2\) and also the limit of \((n, m, >1/2)\)-QRA coding for general \(m\), extending the geometric proof argument for \(n = 4\). Section 4 includes applications of our results to quantum network coding. Finally, section 5 concludes the paper.

1.1. Related work

For the relation among these three parameters of \((n, m, p)\)-QRA coding, the following bound is known [4]: \(m \geq (1 - H(p))n\), where \(H\) is the binary entropy function, and it is also known [2] that \((n, m, p)\)-QRA coding with \(m = (1 - H(p))n + O(\log n)\) exists (which is actually classical). Thus, this bound is asymptotically tight and has many applications such as proving the limit of quantum finite automata [2, 4], analysing quantum communication complexity [6, 8, 9], designing locally decodable code [10, 11], and so on. However, it says almost nothing for small \(n\) and \(m\); if we set \(n = 4\) and \(p > 1/2\), for example, the bound implies only \(m > 0\). This bound neither implies the limit of \(n\) for a given \(m\) if \(\epsilon = p - 1/2\) is very small, say \(\epsilon = 1/g(n)\) for rapidly increasing \(g(n)\). Our second result says that there does exist a limit of \(n\) for any small \(\epsilon\).

König et al [12] extended the concept of QRA coding to the situation that the receiver wants to compute a (randomly selected) function on the bits the sender has, and applied their limit of its extended concept to the security of the privacy amplification, a primitive of quantum key distribution. The study on QRA coding for more than two parties was done by Aaronson [13], who explored the QRA coding in the setting of the Merlin-Arthur games.

2. Quantum random access coding

First, we review the notion of QRA coding given in [2]. The \((n, m, p)\)-QRA coding is an \(m\)-qubit coding of the sender with \(n\) bits so that the receiver can recover any one bit of the \(n\) bits with probability at least \(p\). We give the formal definition for \(m = 1\) since we deal with examples of \((n, 1, p)\)-QRA coding in this section (and the definition for general \(m\) is similarly given).

**Defnition 1.** An \((n, 1, p)\)-QRA coding is a function that maps \(n\)-bit strings \(x \in \{0, 1\}^n\) to \(1\)-qubit states \(\rho_x\), satisfying the following: For every \(i \in \{1, 2, \ldots, n\}\) there exists a positive operator–valued measure (POVM) \(E^i = \{E^i_0, E^i_1\}\) such that \(\text{Tr}(E^i_\alpha \rho_x) \geq p\) for all \(x \in \{0, 1\}^n\), where \(x_i\) is the \(i\)-th bit of \(x\).

Recall that a POVM \(\{E^i_0, E^i_1\}\) has to satisfy the following conditions: (i) \(E^i_0\) and \(E^i_1\) are both nonnegative Hermitian and (ii) \(E^i_0 + E^i_1 = I\). It is well-known, since \(E^i_0\) and \(E^i_1\) are of rank at most 2, that \(E^i_0\) can be written as \(E^i_0 = \alpha_1|u_1\rangle \langle u_1| + \alpha_2|u_2\rangle \langle u_2|\) for some orthonormal basis \(|u_1\rangle, |u_2\rangle\), \(0 \leq \alpha_1 \leq 1\) and \(0 \leq \alpha_2 \leq 1\). Hence, by (ii), \(E^i_1 = I - E^i_0 = (1 - \alpha_1)|u_1\rangle \langle u_1| + (1 - \alpha_2)|u_2\rangle \langle u_2|\). If \(E^0_0\) and \(E^1_1\) can be written as \(E^0_0 = |u_1\rangle \langle u_1|\) and \(E^1_1 = |u_2\rangle \langle u_2|\), then the measurement by the POVM \(\{E^0_0, E^1_1\}\) is called a projective measurement (in the basis \(|u_1\rangle, |u_2\rangle\)).

We next review \((2, 1, 0.85)\)- and \((3, 1, 0.79)\)-QRA codings.
Then the vector of a pure state is the Bloch vector \( \vec{\rho} \) such that \( \rho_{xx} \) is a (real) vector such that

Example 2. The following POVM can be done by using Bloch vectors.

Example 1. The \((2, 1, 0.85)\)-QRA coding [2] maps \( x_1 x_2 \in \{0, 1\}^2 \) to \( \rho_{x_1 x_2} = |\varphi(x_1 x_2)\rangle \langle \varphi(x_1 x_2)| \) where

For decoding, we use the measurements by the following POVMs (projective measurements, in fact): \( E^1 = \{ |0\rangle \langle 0|, |1\rangle \langle 1| \} \), and \( E^2 = \{ |+\rangle \langle +|, |−\rangle \langle −| \} \), where \( |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \) and \( |−\rangle = \frac{1}{\sqrt{2}}(|0\rangle − |1\rangle) \). See figure 1. To decode the second bit, for example, we measure the encoding state in the basis \{\( |+\rangle, |−\rangle \}\). The angle between \( |\varphi(00)\rangle \) and \( |+\rangle \) (and also between \( |\varphi(10)\rangle \) and \( |+\rangle \)) is \( \pi/8 \) and hence the success probability of decoding the value 0 is \( \cos^2 (\pi/8) > 0.85 \).

To explain \((3, 1, 0.79)\)-QRA coding, the Bloch sphere is convenient, which is based on the following two facts (see, e.g., [14]): (i) let \( \rho \) be any one-qubit quantum state, \( \vec{r} = (r_x, r_y, r_z) \) be a (real) vector such that \( |\vec{r}| \leq 1 \), and \( X, Y, Z \) be \( 2 \times 2 \) Pauli matrices such that

\[
X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.
\]

Then \( \rho = \frac{1}{2}(I + r_x X + r_y Y + r_z Z) \) defines a one-to-one mapping between \( \rho \) and \( \vec{r} \). The vector \( \vec{r} \) is called the Bloch vector of \( \rho \). It is well-known that \( \rho \) is pure iff \( |\vec{r}| = 1 \). (ii) Let \( \vec{s} \) be the Bloch vector of a pure state \( |\psi\rangle \langle \psi| \). Then \( \langle \psi| \rho |\psi\rangle = \frac{1}{2}(1 + \vec{r} \cdot \vec{s}) \). Namely, the probability calculation for a POVM can be done by using Bloch vectors.

Example 2. The \((3, 1, 0.79)\)-QRA coding (attributed to Chuang in [2]) maps \( x_1 x_2 x_3 \in \{0, 1\}^3 \) to \( \rho_{x_1 x_2 x_3} = |\varphi(x_1 x_2 x_3)\rangle \langle \varphi(x_1 x_2 x_3)| \), where

\[
|\varphi(000)\rangle = \cos \tilde{\theta} |0\rangle + e^{-\pi i/4} \sin \tilde{\theta} |1\rangle, \quad |\varphi(001)\rangle = \cos \tilde{\theta} |0\rangle + e^{-\pi i/4} \sin \tilde{\theta} |1\rangle,
\]
\[
|\varphi(010)\rangle = \cos \tilde{\theta} |0\rangle + e^{3\pi i/4} \sin \tilde{\theta} |1\rangle, \quad |\varphi(011)\rangle = \cos \tilde{\theta} |0\rangle + e^{-3\pi i/4} \sin \tilde{\theta} |1\rangle,
\]
\[
|\varphi(100)\rangle = \sin \tilde{\theta} |0\rangle + e^{\pi i/4} \cos \tilde{\theta} |1\rangle, \quad |\varphi(101)\rangle = \sin \tilde{\theta} |0\rangle + e^{-\pi i/4} \cos \tilde{\theta} |1\rangle,
\]
\[
|\varphi(110)\rangle = \sin \tilde{\theta} |0\rangle + e^{3\pi i/4} \cos \tilde{\theta} |1\rangle, \quad |\varphi(111)\rangle = \sin \tilde{\theta} |0\rangle + e^{-3\pi i/4} \cos \tilde{\theta} |1\rangle,
\]

such that \( \tilde{\theta} \) satisfies \( \cos^2 \tilde{\theta} = 1/2 + \sqrt{3}/6 > 0.79 \).
As shown in figure 2, Bloch vectors for those eight states are $(\pm 1/\sqrt{3}, \pm 1/\sqrt{3}, \pm 1/\sqrt{3})$. For decoding, we use projective measurements in the bases $\{|0\rangle, |1\rangle\}$, $\{|+, |\rangle\}$ and $\{|+, |\rangle\}$ for recovering the first, second and third bits, respectively, whose Bloch vectors are $\pm (0, 0, 1)$ (z-axis), $\pm (1, 0, 0)$ (x-axis), and $\pm (0, 1, 0)$ (y-axis), respectively. Here, $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$. Thus, for example, if we measure $|\psi(001)\rangle$ by $\{|+, |\rangle\}$, then the probability of getting the correct value 0 for the second bit is $1/2 + \sqrt{3}/6 > 0.79$.

Note that the success probability of the $(3, 1, 0.79)$-QRA coding is worse than that of the $(2, 1, 0.85)$-QRA coding, but is still quite high. Thus, it might be natural to conjecture that we still have room to encode four bits into one qubit. In fact, [3] gives a statement of positive flavour. Before disproving this conjecture, let us look at the third example, which might seem to work as a $(4, 1, >1/2)$-QRA coding.

**Example 3.** For encoding $x_1x_2x_3x_4 \in \{0, 1\}^4$, we select $|\psi(0x_1x_2)\rangle$ and $|\psi(1x_3x_4)\rangle$ uniformly at random, where $|\psi(z_1z_2z_3)\rangle$ is the same state as the one used in the $(3, 1, 0.79)$-QRA coding. For decoding, we first apply the universal cloning [15] to the qubit ($|\psi(0x_1x_2)\rangle$ or $|\psi(1x_3x_4)\rangle$) and let $\rho_1$ and $\rho_2$ be the first and the second clones, respectively. If we want to get $x_1$ ($x_2$, respectively), we apply the decoding process of $(3, 1, 0.79)$-QRA coding to recover the first bit of $\rho_1$. If the result is 0, then by assuming that the transmitted qubit was $|\psi(0x_1x_2)\rangle$, we recover the second (third, respectively) bit of $\rho_2$ again by $(3, 1, 0.79)$-QRA decoding process. Otherwise, i.e., if the result is 1, then by assuming that the transmitted qubit was $|\psi(1x_3x_4)\rangle$, we output the random bit (0 or 1 with equal probability). Decoding $x_3$ or $x_4$ is similar and omitted.

First of all, one should see that the above protocol completely follows Definition 1: the encoding process maps $x_1x_2x_3x_4$ to a mixed state. The decoding process is a little complicated, but it is well-known (e.g., [14]) that such a physically realizable procedure can be expressed by...
a single POVM. Suppose that the receiver wants to get $x_1$ or $x_2$. Then note that $|\varphi(0x_1x_2)\rangle$ is sent with probability 1/2 and if that is the case, the receiver can get a correct result with probability $p_0$ which is strictly greater than 1/2. Otherwise, i.e., if $|\varphi(1x_3x_4)\rangle$ is sent, it seems that we only get a result independent of $x_1$ or $x_2$. (Say, if the first measurement yields the correct answer 1, then the outcome is completely random.) Thus the total success probability might appear to be more than a half. Why is this argument wrong?

3. Main results

In this section, we give two results on the impossibility of QRA coding. First, we show the non-existence of $(4, 1, >1/2)$-QRA coding, which means that the $(3, 1, 0.79)$-QRA coding is the best we can do for the $(n, 1, >1/2)$-QRA coding.

**Theorem 1.** There exists no $(4, 1, p)$-QRA coding with $p > 1/2$.

First let us return to figure 2 to see how $(3, 1, 0.79)$-QRA coding works. Recall that the measurements for recovering $x_1$, $x_2$ and $x_3$ are all projective measurements. Now one should observe that each measurement corresponds to a plane in the Bloch sphere which acts as a ‘boundary’ for the encoding states. For example, the measurement in the basis $\{|0\rangle, |1\rangle\}$ corresponds to the $xy$-plane (states $|0\rangle$ and $|1\rangle$ correspond to $+z$ and $-z$ axes, respectively, on the sphere, which means that the measurement determines whether the encoding state lies above or under the $xy$-plane). Thus, the three planes corresponding to projective measurements of $(3, 1, 0.79)$-QRA coding divide the Bloch sphere into eight disjoint regions, each of which includes exactly one encoding state.

Now suppose that there is a $(4, 1, p)$-QRA coding whose decoding process is four projective measurements. Then, by a simple extension of the above argument, each measurement corresponds to a plane and the four planes divide the sphere into, say, $m$ regions. On the other hand, by definition we have 16 encoding states and hence $m \geq 16$. (Otherwise, some two states fall into the same region, meaning the same outcome for those states, a contradiction.) However, it is well-known that a 3D ball cannot be divided into 16 (or more) regions by four planes. Thus, we are done if the decoding process is restricted to projective measurements. Due to the generality of POVMs, one might expect that the above argument does not hold for the case of POVMs. However, as shown in the hereafter, a similar argument applies.

**Lemma 1.** If there exists $(4, 1, p)$-QRA coding with $p > 1/2$, then the 3D ball can be divided into 16 distinct regions by four planes.

**Proof.** Suppose that $(4, 1, p)$-QRA coding with $p > 1/2$ exists. Then by definition there are 16 encoding states $\{\rho_w\}_{w \in \{0,1\}^4}$ and 4 POVMs $\{E_0^i, E_1^i\}_{i \in \{1,2,3,4\}}$ such that $\text{Tr}(E_0^i\rho_w) \geq p$ if $w_i = 0$ and $\text{Tr}(E_1^i\rho_w) \leq 1 - p$ if $w_i = 1$. As shown in the previous section, $E_0^i$ and $E_1^i$ can be written as:

$$E_0^i = \alpha'_1|u_i\rangle\langle u_i| + \alpha'_2|u_i^+\rangle\langle u_i^+|,$$

$$E_1^i = (1 - \alpha'_1)|u_i\rangle\langle u_i| + (1 - \alpha'_2)|u_i^+\rangle\langle u_i^+|$$

for $0 \leq \alpha'_2 \leq \alpha'_1 \leq 1$ and orthogonal states $|u_i\rangle$ and $|u_i^+\rangle$. Thus, for all $i$, $\text{Tr}(E_0^i\rho_w)$ can be written as:

$$\alpha'_1\langle u_i|\rho_w|u_i\rangle + \alpha'_2\langle u_i^+|\rho_w|u_i^+\rangle \begin{cases} 
>1/2 & \text{if } w_i = 0, \\
<1/2 & \text{if } w_i = 1.
\end{cases}$$

(1)
Theorem 2. There is no \( N \) then, any \( \vec{r}_w \) and \( \vec{u}_i \), respectively, \((1)\) is rewritten as
\[
\frac{\alpha_i^1 + \alpha_i^2}{2} + \frac{\alpha_i^1 - \alpha_i^2}{2} \cdot \vec{r}_w \cdot \vec{u}_i \begin{cases} >1/2 & \text{if } w_i = 0, \\ <1/2 & \text{if } w_i = 1, \end{cases}
\]
by fact (ii) on the Bloch sphere described before example 2. (Note that the Bloch vector for \( |u_i^+\rangle \langle u_i^+| \) is \( -\vec{u}_i \).) If we let \( c_i = 1 - (\alpha_i^1 + \alpha_i^2) \) and \( \vec{s}_i = (\alpha_i^1 - \alpha_i^2) \cdot \vec{u}_i \), \((2)\) becomes the following simple linear inequalities for the fixed \( \vec{s}_i \) s.
\[
\vec{r}_w \cdot \vec{s}_i \begin{cases} >c_i & \text{if } w_i = 0, \\ <c_i & \text{if } w_i = 1. \end{cases}
\]

Now, let \( B \) be the set of all Bloch vectors. Let also \( D_i^{(0)} \) and \( D_i^{(1)} \) be the subsets of \( \mathbb{R}^3 \) defined by \( D_i^{(0)} = \{ \vec{r} \in B \mid \vec{r} \cdot \vec{s}_i > c_i \} \) and \( D_i^{(1)} = \{ \vec{r} \in B \mid \vec{r} \cdot \vec{s}_i < c_i \} \), respectively. By \((3)\), all 16 subsets \( D_w = D_{s_1}^{(0)} \cap D_{s_2}^{(0)} \cap D_{s_3}^{(0)} \cap D_{s_4}^{(0)} \) must not be empty. These subsets are the 16 non-empty regions of the ball divided by the four planes \( \{ \vec{r} \mid \vec{r} \cdot \vec{s}_i = c_i \} \).

Lemma 1 contradicts the following well-known geometric fact, which completes the proof of theorem 1.

**Lemma 2.** A ball cannot be divided into 16 non-empty regions by four planes.

Our second result is a generalization of theorem 1. By using the notion of Bloch vectors of \( n \)-qubit states, we have the following generalization.

**Theorem 2.** There is no \((2^m, m, p)\)-QRA coding with \( p > 1/2 \).

The proof of theorem 2 proceeds similarly to theorem 1 except for the generalization of Bloch vectors and lemma 2. For completeness we repeat such a similar argument. First, we review the Bloch vectors of \( N \)-level quantum states \([16]–[18]\). Let \( \lambda_1, \ldots, \lambda_{2^N-1} \) be orthogonal generators of \( SU(N) \) satisfying: (i) \( \lambda_i^+ = \lambda_i \); (ii) \( \text{Tr}(\lambda_i) = 0 \); (iii) \( \text{Tr}(\lambda_i \lambda_j) = 2 \) if \( i = j \) and \( 0 \) if \( i \neq j \). (We should note that the factor 2 of (iii) is just according to convention, not inevitable \([19]\).)

Then, any \( N \)-level quantum state \( \rho \) can be represented as an \((N^2 - 1)\)-dimensional real vector \( \vec{r} = (r_1, \ldots, r_{2^N-1}) \), called the Bloch vector of \( \rho \), such that \( \rho = \frac{1}{N} I_N + \frac{1}{2} \sum_{i=1}^{N^2-1} r_i \lambda_i \), where \( I_N \) is the \( N \)-dimensional identity matrix. Note that, by the properties of \( \lambda_i \) s, for any two \( N \)-level quantum states \( \rho \) and \( \sigma \) with their Bloch vectors \( \vec{r} \) and \( \vec{s} \),
\[
\text{Tr}(\rho \sigma) = \frac{1}{N} + \frac{1}{2} \cdot \vec{r} \cdot \vec{s}.
\]

Second, we give the following lemma.

**Lemma 3.** If there exists a \((2^m, m, p)\)-QRA coding with \( p > 1/2 \), then \( \mathbb{R}^{2^m-1} \) can be divided into \( 2^m \) distinct regions by \( 2^m \) hyperplanes.

**Proof.** Suppose that \((2^m, m, p)\)-QRA coding with \( p > 1/2 \) exists. Then, by definition there are \( 2^{2m} \) encoding states \( \{\rho_w\}_{w \in \{0,1\}^{2^m}} \) and \( 2^m \) POVMs \( \{E_i^0, E_i^1\}_{i \in \{1,2,\ldots,2^m\}} \) such that \( \text{Tr}(E_i^1 \rho_w) > 1/2 \) if \( w_i = 0 \) and \( \text{Tr}(E_i^0 \rho_w) < 1/2 \) if \( w_i = 1 \). Since \( E_i^0 \) and \( E_i^1 \) are \( 2^m \)-dimensional nonnegative Hermitian, they can be written as:
\[
E_i^0 = \sum_{j=1}^{2^m} \alpha_j^i |u_j^i\rangle \langle u_j^i|, \quad E_i^1 = \sum_{j=1}^{2^m} (1 - \alpha_j^i) |u_j^i\rangle \langle u_j^i|,
\]
such that \( \{|u'_j\rangle\}_{j=1}^{2^m} \) is an orthonormal basis. Thus, for all \( i \in \{1, \ldots, 2^m\} \), the following must be satisfied:

\[
\sum_{j=1}^{2^m} \alpha'_j |u'_j\rangle \langle \rho_w |u'_j\rangle \begin{cases} >1/2 & \text{if } w_i = 0, \\ <1/2 & \text{if } w_i = 1. \end{cases}
\]

(5)

Denoting the Bloch vectors of \( \rho_w \) and \( |u'_j\rangle \langle u'_j| \) as \( \vec{r}_w \) and \( u'_j \) (which are \((2^m-1)\)-dimensional real vectors), respectively, (5) is rewritten as

\[
\sum_{j=1}^{2^m} \left( \frac{\alpha'_j}{2^m} + \frac{\alpha_j'}{2} \vec{r}_w \cdot \vec{u}_j \right) \begin{cases} >1/2 & \text{if } w_i = 0, \\ <1/2 & \text{if } w_i = 1, \end{cases}
\]

(6)

by (4). (Notice that an \( m \)-qubit state can be identified with a \( 2^m \)-level quantum state.) If we let

\[
c_i = 1/2 - \sum_{j=1}^{2^m} \frac{\alpha_j'}{2^m} \text{ and } \vec{s}_i = \sum_{j=1}^{2^m} \frac{\alpha_j'}{2} \vec{u}_j,
\]

(6) is simplified as follows:

\[
\vec{r}_w \cdot \vec{s}_i \begin{cases} >c_i & \text{if } w_i = 0, \\ <c_i & \text{if } w_i = 1. \end{cases}
\]

(7)

Now, the following geometric fact (see, e.g., [20]) completes the proof of theorem 2.

**Lemma 4.** \( \mathbb{R}^{2^m-1} \) cannot be divided into \( 2^{2^m} \) non-empty regions by \( 2^m \) hyperplanes.

### 4. Applications to network coding

Network coding, introduced in [21], is nicely explained by using the so-called Butterfly network as shown in figure 3. The capacity of each directed link is all one and there are two source-sink pairs \( s_1 \) to \( t_1 \) and \( s_2 \) to \( t_2 \). Notice that both paths have to use the single link from \( s_0 \) to \( t_0 \) and hence the total amount of flow in both paths is bounded by one, say, 1/2 for each. Interestingly, this max-flow min-cut theorem no longer applies for `digital information flow.' As shown in the figure, we can transmit two bits, \( x \) and \( y \), on the two paths simultaneously.

The paper [5] extends this network coding for quantum channels and quantum information. Their results include: (i) One can send any quantum state \( |\psi_1\rangle \) from \( s_1 \) to \( t_1 \) and \( |\psi_2\rangle \) from \( s_2 \) to \( t_2 \) simultaneously with a fidelity strictly greater than 1/2. (ii) If one of \( |\psi_1\rangle \) and \( |\psi_2\rangle \) is classical, then the fidelity can be improved to 2/3. (iii) Similar improvement is also possible if \( |\psi_1\rangle \) and \( |\psi_2\rangle \) are restricted to only a finite number of (previously known) states. This allows us to design a protocol which can send three classical bits from \( s_1 \) to \( t_1 \) (similarly from \( s_2 \) to \( t_2 \)) but only one of them should be recovered.
For completeness, we include the scheme $X3C3C$ for result (iii) whose success probability is $\approx 0.525$. Note that, for the case of two bits, the scheme $X2C2C$ has a better success probability $\approx 0.59$ [5]. The following two primitives are used for $X3C3C$.

**3D measurement (MM$_3$).** The 3D measurement, denoted by $MM_3$, is defined by the POVM described by $\{\frac{1}{4} |\psi(z_1z_2z_3)\rangle\langle\psi(z_1z_2z_3)| \mid z_1z_2z_3 \in \{0, 1\}^3\}$. 

**Approximated group operation (AG).** Before its definition, we introduce the operation Inv, which maps a pure state $|\psi\rangle = a|0\rangle + b|1\rangle$ to its 'opposite' state $b^*|0\rangle - a^*|1\rangle$ in the Bloch sphere (see e.g., [22, 23]). Note that the eight operations $\{I, X, Y, Z, Inv, InvX, InvY, InvZ\}$ form an abelian group operating on one-qubit states. Because Inv is not a physically allowable map, i.e., trace-preserving completely positive (TP-CP) map, we introduce its approximation $Inv'$, which maps $\rho$ to $Inv'\rho = \frac{1}{2}Inv\rho + \frac{3}{2} \cdot I$. We can check that $Inv'$ is a TP-CP map. The approximated group operation under a three-bit string $r_1r_2r_3$, denoted by $AG(\rho, r_1r_2r_3)$, is a transformation defined by $AG(\rho, 000) = \rho$, $AG(\rho, 011) = Z\rho$, $AG(\rho, 101) = X\rho$, $AG(\rho, 110) = Y\rho$ and, for any $r_1r_2r_3 \in \{001, 010, 100, 111\}$, $AG(\rho, r_1r_2r_3) = Inv'AG(\rho, \tilde{r}_1\tilde{r}_2\tilde{r}_3)$, where $\tilde{r}$ is the negation of $r \in \{0, 1\}$.

Now let us describe $X3C3C$. Here, $M[1], M[2]$ and $M[3]$ denotes the projective measurements in the bases $\{|0\rangle, |1\rangle\}, \{|+\rangle, |--\rangle\}$ and $\{|+\rangle, |--\rangle\}$, respectively, and $UC$ denotes the universal cloning [15].

**Protocol $X3C3C$:** Input $x_1x_2x_3$ at $s_1$, $y_1y_2y_3$ at $s_2$; Output Out$^1$ at $t_1$, Out$^2$ at $t_2$.

Step 1. $Q_1 = |\psi(x_1x_2x_3)\rangle$ (from $s_1$ to $t_2$), $Q_2 = |\psi(x_1x_2x_3)\rangle$ (from $s_1$ to $s_0$), $Q_3 = |\psi(y_1y_2y_3)\rangle$ (from $s_2$ to $s_0$), and $Q_4 = |\psi(y_1y_2y_3)\rangle$ (from $s_2$ to $t_1$).

Step 2. $Q_5 = AG(Q_2, MM_3(Q_3))$ from $s_0$ to $t_0$.

**Figure 3.** Butterfly network
Step 3. \((Q_6, Q_7) = UC(Q_5)\) from \(s_0\) to \(t_1\) and \(t_2\).

Step 4. (Decoding the \(j\)-th bit at \(t_1\) and \(t_2\)) \(\text{Out}^1 = M[j](Q_4) \oplus M[j](Q_7)\). \(\text{Out}^2 = M[j](Q_1) \oplus M[j](Q_6)\).

By our result in this paper, we can prove a kind of optimality of the result (iii). Firstly, we cannot extend the above three bits to four bits, that is, there exists no X4C4C. The reason is easy: if we could then we would get a \((4, 1, >1/2)\)-QRA coding for the \(s_1\)–\(t_1\) path by fixing the state at \(s_2\) to say \(|0\rangle\). Secondly, we can prove that the two side links (\(s_1\) to \(t_2\) and \(s_2\) to \(t_1\)) which are unusable in the conventional multicommodity flow are in fact useful; if we remove them even for the two bits case, then the network can be viewed as a \((4, 1, p)\)-QRA coding system, which cannot achieve \(p > 1/2\).

5. Concluding remarks

This paper showed the limit of \((n, m, >1/2)\)-QRA coding using the reduction to well-known geometric facts. In particular, our result is completely tight for \(m = 1\). The result for general \(m\) is quite good since we can observe that a \((2^{2m}, m, >1/2)\)-QRA coding exists by a reduction from a result of ‘unbounded-error’ communication complexity by Klauck [7] to the QRA coding (such a reduction can be done in a similar way to [6]). However, the case of general \(m\) is not completely tight: we have not shown whether \((2^{2m} - 1, m, >1/2)\)-QRA coding exists. An interesting open question is the possibility of \((n, 2, >1/2)\)-QRA coding. \((6, 2, 0.79)\)-QRA coding is obvious since we can use two \((3, 1, 0.79)\)-QRA codings independently. For \(n = 7\), there is the following simple construction.

Example 4. The \((7, 2, 0.54)\)-QRA coding consists of encoding states and measurements as follows. For each seven bits \(x = x_1 x_2 x_3 x_4 x_5 x_6 x_7\), the encoding state \(\rho(x)\) is

\[
\alpha|\varphi(x_1 x_2 x_3)\rangle \langle \varphi(x_1 x_2 x_3)| \otimes |\varphi(x_4 x_5 x_6)\rangle \langle \varphi(x_4 x_5 x_6)| + (1 - \alpha)|\xi(x_7)\rangle \langle \xi(x_7)|
\]

with \(\alpha = 6/(7 + \sqrt{3})\), where \(|\xi(0)\rangle = 1/\sqrt{2}(|00\rangle + |11\rangle)\) and \(|\xi(1)\rangle = 1/\sqrt{2}(|01\rangle + |10\rangle)\). To obtain any one of \(x_1\), \(x_2\) and \(x_3\) (respectively \(x_4\), \(x_5\) and \(x_6\)) use the measurement of the \((3, 1, 0.79)\)-QRA coding on the first qubit (respectively second qubit) of \(\rho(x)\). To obtain \(x_7\), use the projective measurement \(E^j = [E^j_0, E^j_1]\) on \(\rho(x)\), where \(E^j_0 = |00\rangle\langle 00| + |11\rangle\langle 11|\) and \(E^j_1 = |01\rangle\langle 01| + |10\rangle\langle 10|\).

We can also regard the task of \((n, 1, >1/2)\)-QRA coding as a special case of the following task: the receiver is required to compute the inner product between the two \(n\) bits of the sender and the receiver by using one qubit from the sender. (In the QRA coding, the receiver has one of only \(n\) candidates \(100 \cdots 0, 010 \cdots 0,\) and \(000 \cdots 1\).) In case that the sender’s input is taken from \(\{0, 1\}^n\), we can show that \(n = 3\) is impossible by the reduction to a simple geometric fact again while \(n = 2\) is possible with success probability \(\approx 0.79\) using the four states that sit in the vertices of the tetrahedron inscribed in the Bloch sphere.

Acknowledgments

Most of this work was done while HN and RR were in Graduate School of Informatics, Kyoto University. KI was supported in part by Scientific Research Grant, Ministry of Japan, 16092101. SY was supported in part by Scientific Research Grant, Ministry of Japan, 16092218.
References

[1] Holevo A S 1979 Problems Inform. Trans. 15 247
[2] Ambainis A, Nayak A, Ta-shma A and Vazirani U 1999 Proc. 31st ACM Symp. on Theory of Computing (New York: ACM) p 376
[3] Ambainis A, Nayak A, Ta-shma A and Vazirani U 2002 J. ACM 49 496
[4] Nayak A 1999 Proc. 40th IEEE Symp. on Foundations of Computer Science (Los Alamitos, CA: IEEE) p 369
[5] Hayashi M, Iwama K, Nishimura H, Raymond R and Yamashita S 2006 Talk at 9th Workshop of Quantum Information Processing Preprint quant-ph/0601088
[6] Buhrman H and de Wolf R 2001 Proc. 16th IEEE Conf. on Computational Complexity (Los Alamitos, CA: IEEE) p 120
[7] Klauck H 2001 Proc. 42th IEEE Symp. on Foundations of Computer Science (Los Alamitos, CA: IEEE) p 288
[8] Gavinsky D, Kempe J, Regev O and de Wolf R 2006 Proc. 38th ACM Symp. on Theory of Computing (New York: ACM) Preprint quant-ph/0511013
[9] Klauck H 2000 Proc 32nd ACM Symp. on Theory of Computing (New York: ACM) p 644
[10] Kerenidis I and de Wolf R 2004 J. Comput. Syst. Sci. 69 395
[11] Wehner S and de Wolf R 2005 Proc. 32nd Int. Colloquium on Automata, Languages and Programming (Lecture Notes in Computer Science vol 3580) (New York: Springer) p 1424
[12] König R, Maurer U M and Renner R 2005 IEEE Trans. Inf. Theory 51 2391
[13] Aaronson S 2006 Proc. 21st IEEE Conf. on Computational Complexity (Los Alamitos, CA: IEEE) Preprint quant-ph/0510230
[14] Nielsen M A and Chuang I L 2000 Quantum Computation and Quantum Information (Cambridge: Cambridge University Press)
[15] Bužek V and Hillery M 1996 Phys. Rev. A 54 1844
[16] Alicki R and Lendi K 1987 Quantum Dynamical Semigroups and Applications (Lecture Notes in Physics vol 286) (New York: Springer)
[17] Jakóbczyk L and Siennicki M 2001 Phys. Lett. A 286 383
[18] Mahler G and Weberruss V A 1995 Quantum Networks (New York: Springer)
[19] Kimura G and Kossakowski A 2005 Open Syst. Inform. Dyn. 12 207 (Preprint quant-ph/0408014)
[20] Edelsbrunner H 1987 Algorithms in Computational Geometry (New York: Springer)
[21] Ahlswede R, Cai N, Li S-Y R and Yeung R W 2000 IEEE Trans. Inform. Theory 46 1204
[22] Bužek V, Hillery M and Werner R F 1999 Phys. Rev. A 60 2626
[23] Gisin N and Popescu S 1999 Phys. Rev. Lett. 83 432