

# (4, 1)-Quantum Random Access Coding Does Not Exist

MASAHITO HAYASHI<sup>1</sup>

KAZUO IWAMA<sup>2</sup>

HARUMICHI NISHIMURA<sup>3</sup>

RUDY RAYMOND<sup>2</sup>

SHIGERU YAMASHITA<sup>4</sup>

<sup>1</sup>ERATO-SORST Quantum Computation and Information Project,  
Japan Science and Technology Agency  
masahito@qci.jst.go.jp

<sup>2</sup>Graduate School of Informatics, Kyoto University  
{iwama, raymond}@kuis.kyoto-u.ac.jp

<sup>3</sup>Graduate School of Science, Osaka Prefecture University<sup>1</sup>  
hnishimura@mi.s.osakafu-u.ac.jp

<sup>4</sup>Graduate School of Information Science, Nara Institute of Science and Technology  
ger@is.naist.jp

**Abstract.** An  $(n, 1, p)$ -Quantum Random Access (QRA) coding, introduced by Ambainis, Nayak, Ta-shma and Vazirani in *ACM Symp. on Theory of Computing* 1999, 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 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.

## 1 Introduction

The state of  $n$  quantum bits (qubits) is given by a vector of length  $2^n$  and seems to hold much more information than (classical)  $n$  bits. However, due to the famous Holevo bound [10], 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, Nayak, Ta-shma and Vazirani introduced the notion of *quantum random access (QRA) coding* [4]. (The paper [5] includes the contents of [4] and their improvement in [17].) They explored the possibility of using much less 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 [4]) 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.

**Our Contribution** 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 idea is to use the well-known geometric fact that a three-dimensional ball cannot be divided into 16 nonempty

---

<sup>1</sup>This work was done while HN was in Graduate School of Informatics, Kyoto university.

regions by four planes. (Interestingly, the proof for the non-existence of a classical counterpart of  $(2, 1, p)$ -QRA coding in [4] uses a similar geometric fact, i.e., a straight line cannot stab all insides of the four quarters of a two-dimensional square.) Our result has nice applications to the analysis of *quantum network coding* which was introduced very recently [9].

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  $(2^{2m}, m, p)$ -QRA coding with  $p > 1/2$  does not exist.

**Related Work** For the relation among these three parameters of  $(n, m, p)$ -QRA coding, the following bound is known [17]:  $m \geq (1 - H(p))n$ , where  $H$  is the binary entropy function, and it is also known [4] 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 [4, 17], analyzing quantum communication complexity [6, 14], designing locally decodable code [12, 19], 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, Maurer and Renner [15] 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 [1], who explored the QRA coding in the setting of the Merlin-Arthur games.

## 2 Quantum Random Access Coding

The following definition is due to [4].

**Definition.** 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  $i \in \{1, 2, \dots, n\}$  there exists a positive operator-valued measure (POVM)  $E^i = \{E_0^i, E_1^i\}$  such that  $\text{Tr}(E_{x_i}^i \rho_x) \geq p$  for all  $x \in \{0, 1\}^n$ , where  $x_i$  is the  $i$ -th bit of  $x$ .

Recall that a POVM  $\{E_0^i, E_1^i\}$  has to satisfy the following conditions: (i)  $E_0^i$  and  $E_1^i$  are both nonnegative Hermitian and (ii)  $E_0^i + E_1^i = I$ . It is well-known, since  $E_0^i$  and  $E_1^i$  are of rank at most 2, that  $E_0^i$  can be written as  $E_0^i = \alpha_1 |u_1\rangle\langle u_1| + \alpha_2 |u_2\rangle\langle u_2|$  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),  $E_1^i = I - E_0^i = (1 - \alpha_1) |u_1\rangle\langle u_1| + (1 - \alpha_2) |u_2\rangle\langle u_2|$ . If  $E_0^i$  and  $E_1^i$  can be written as  $E_0^i = |u_1\rangle\langle u_1|$  and  $E_1^i = |u_2\rangle\langle u_2|$ , then the measurement by the POVM  $\{E_0^i, E_1^i\}$  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.

**Example 1.** The  $(2, 1, 0.85)$ -QRA coding [4] 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

$$\begin{aligned} |\varphi(00)\rangle &= \cos(\pi/8)|0\rangle + \sin(\pi/8)|1\rangle, & |\varphi(10)\rangle &= \cos(3\pi/8)|0\rangle + \sin(3\pi/8)|1\rangle, \\ |\varphi(11)\rangle &= \cos(5\pi/8)|0\rangle + \sin(5\pi/8)|1\rangle, & |\varphi(01)\rangle &= \cos(7\pi/8)|0\rangle + \sin(7\pi/8)|1\rangle. \end{aligned}$$

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 Fig.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., [18]): (i) let  $\rho$  be any one-qubit quantum state,  $\vec{r} = (r_x, r_y, r_z)$  be a

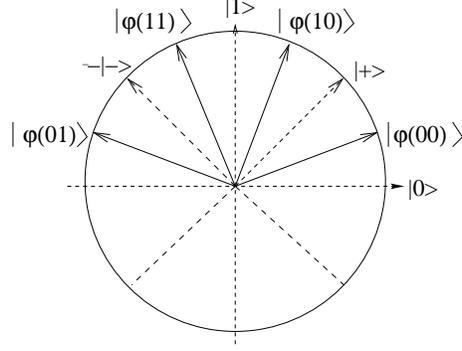


Figure 1: The (2, 1, 0.85)-QRA coding in  $|0\rangle$ - $|1\rangle$  plane representation

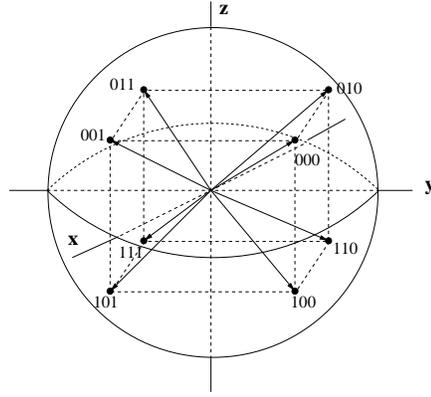


Figure 2: The (3, 1, 0.79)-QRA coding in Bloch vector representation

(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  $\boldsymbol{\rho} = \frac{1}{2}(I + r_x X + r_y Y + r_z Z)$  defines a one-to-one mapping between  $\boldsymbol{\rho}$  and  $\vec{r}$ . The vector  $\vec{r}$  is called the *Bloch vector* of  $\boldsymbol{\rho}$ . It is well-known that  $\boldsymbol{\rho}$  is pure iff  $|\vec{r}| = 1$ . (ii) Let  $\vec{s}$  be the Bloch vector of a pure state  $|\psi\rangle\langle\psi|$ . Then  $\langle\psi|\boldsymbol{\rho}|\psi\rangle = \frac{1}{2}(1 + \vec{r} \cdot \vec{s})$ . 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 [4]) maps  $x_1 x_2 x_3 \in \{0, 1\}^3$  to  $\boldsymbol{\rho}_{x_1 x_2 x_3} = |\varphi(x_1 x_2 x_3)\rangle\langle\varphi(x_1 x_2 x_3)|$ , where

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

such that  $\tilde{\theta}$  satisfies  $\cos^2 \tilde{\theta} = 1/2 + \sqrt{3}/6 > 0.79$ .

As shown in Fig.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  $\{|0\rangle, |1\rangle\}$ ,  $\{|+\rangle, |-\rangle\}$  and  $\{|+\prime\rangle, |-\prime\rangle\}$  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,  $|+\prime\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$  and

$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ . Thus, for example, if we measure  $|\varphi(001)\rangle$  by  $\{|+\rangle, |-\rangle\}$ , 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, [5] 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  $|\varphi(0x_1x_2)\rangle$  and  $|\varphi(1x_3x_4)\rangle$  uniformly at random, where  $|\varphi(z_1z_2z_3)\rangle$  is the same state as the one used in the (3, 1, 0.79)-QRA coding. For decoding, we first apply the universal cloning [7] to the qubit ( $|\varphi(0x_1x_2)\rangle$  or  $|\varphi(1x_3x_4)\rangle$ ) and let  $\rho_1$  and  $\rho_2$  be the first and the second clones, respectively. If we want to get  $x_1$  ( $x_2$ , resp.), 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  $|\varphi(0x_1x_2)\rangle$ , we recover the second (third, resp.) 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  $|\varphi(1x_3x_4)\rangle$ , 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 the definition of the QRA coding: The encoding process maps  $x_1x_2x_3x_4$  to a mixed state. The decoding process is a bit complicated, but it is well-known (e.g., [18]) 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, then the outcome is completely random. Thus the total success probability is  $(p_0 + 1/2)/2 > 1/2$ . Why is this argument wrong?

### 3 Main Result

**Theorem 3.1** *There exists no (4, 1,  $p$ )-QRA coding with  $p > 1/2$ .*

First let us return to Fig. 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 three-dimensional 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 its potential image of POVM, it seems unlikely that there exists a simple extension of this argument to the case of POVMs. A little surprisingly, there does.

**Lemma 3.2** *If there exists (4, 1,  $p$ )-QRA coding with  $p > 1/2$ , then the three-dimensional ball can*

be divided into 16 distinct regions by 4 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  $\text{Tr}(E_0^i \rho_w) \leq 1 - p$  if  $w_i = 1$ . As shown in the previous section,  $E_0^i$  and  $E_1^i$  can be written as:

$$\begin{aligned} E_0^i &= \alpha_1^i |u_i\rangle\langle u_i| + \alpha_2^i |u_i^\perp\rangle\langle u_i^\perp| \\ E_1^i &= (1 - \alpha_1^i) |u_i\rangle\langle u_i| + (1 - \alpha_2^i) |u_i^\perp\rangle\langle u_i^\perp|, \end{aligned}$$

for  $0 \leq \alpha_2^i \leq \alpha_1^i \leq 1$  and orthogonal states  $|u_i\rangle$  and  $|u_i^\perp\rangle$ . Thus, for all  $i$ ,  $\text{Tr}(E_0^i \rho_w)$  can be written as:

$$\forall i \left[ \alpha_1^i \langle u_i | \rho_w | u_i \rangle + \alpha_2^i \langle u_i^\perp | \rho_w | u_i^\perp \rangle \begin{cases} > 1/2 & \text{if } w_i = 0, \\ < 1/2 & \text{if } w_i = 1 \end{cases} \right]. \quad (1)$$

Denoting the Bloch vectors of  $\rho_w$  and  $|u_i\rangle\langle u_i|$  as  $\vec{r}_w$  and  $\vec{u}_i$ , respectively, (1) is rewritten as

$$\forall i \left[ \frac{\alpha_1^i + \alpha_2^i}{2} + \frac{\alpha_1^i - \alpha_2^i}{2} \cdot \vec{r}_w \cdot \vec{u}_i \begin{cases} > 1/2 & \text{if } w_i = 0, \\ < 1/2 & \text{if } w_i = 1 \end{cases} \right], \quad (2)$$

by Fact (ii) on the Bloch sphere. (Note that the Bloch vector for  $|u_i^\perp\rangle\langle u_i^\perp|$  is  $-\vec{u}_i$ .) If we let  $c_i = 1 - (\alpha_1^i + \alpha_2^i)$  and  $\vec{s}_i = (\alpha_1^i - \alpha_2^i) \cdot \vec{u}_i$ , (2) becomes the following simple linear inequalities for the fixed  $\vec{s}_i$ s.

$$\forall i \left[ \vec{r}_w \cdot \vec{s}_i \begin{cases} > c_i & \text{if } w_i = 0, \\ < c_i & \text{if } w_i = 1 \end{cases} \right]. \quad (3)$$

Now, let  $B$  be the set of all Bloch vectors. Let also  $D_{s_i}^{(0)}$  and  $D_{s_i}^{(1)}$  be the subsets of  $\mathbb{R}^3$  defined by  $D_{s_i}^{(0)} = \{\vec{r} \in B \mid \vec{r} \cdot \vec{s}_i > c_i\}$  and  $D_{s_i}^{(1)} = \{\vec{r} \in B \mid \vec{r} \cdot \vec{s}_i < c_i\}$ , respectively. By (3), all 16 subsets  $D_w = D_{s_1}^{(w_1)} \cap D_{s_2}^{(w_2)} \cap D_{s_3}^{(w_3)} \cap D_{s_4}^{(w_4)}$  must not be empty. These subsets are the 16 non-empty regions of the ball divided by the 4 planes  $\{\vec{r} \mid \vec{r} \cdot \vec{s}_i = c_i\}$ .  $\square$

Lemma 3.2 contradicts the following well-known geometric fact, which completes the proof of Theorem 3.1.

**Lemma 3.3** *A ball cannot be divided into 16 non-empty regions by 4 planes.*

By using the notion of Bloch vectors of  $n$ -qubit states, we have the following generalization.

**Theorem 3.4** *There is no  $(2^{2m}, m, p)$ -QRA coding with  $p > 1/2$ .*

The proof of Theorem 3.4 proceeds similarly to Theorem 3.1 except for the generalization of Bloch vectors and Lemma 3.3. For completeness we repeat such a similar argument. First, we review the Bloch vectors of  $N$ -level quantum states [3, 11, 13, 16]. Let  $\lambda_1, \dots, \lambda_{N^2-1}$  be orthogonal generators of  $SU(N)$  satisfying: (i)  $\lambda_i^\dagger = \lambda_i$ ; (ii)  $\text{Tr}(\lambda_i) = 0$ ; (iii)  $\text{Tr}(\lambda_i \lambda_j) = 2$  if  $i = j$  and 0 if  $i \neq j$ . Then, any  $N$ -level quantum state  $\rho$  can be represented as an  $(N^2 - 1)$ -dimensional real vector  $\vec{r} = (r_1, \dots, r_{N^2-1})$ , 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  $\vec{s}$ ,

$$\text{Tr}(\rho\sigma) = \frac{1}{N} + \frac{1}{2} \cdot \vec{r} \cdot \vec{s}. \quad (4)$$

Second, we give the following lemma.

**Lemma 3.5** *If there exists a  $(2^{2m}, m, p)$ -QRA coding with  $p > 1/2$ , then  $\mathbb{R}^{2^{2m}-1}$  can be divided into  $2^{2^{2m}}$  distinct regions by  $2^{2m}$  hyperplanes.*

**Proof.** Suppose that  $(2^{2m}, m, p)$ -QRA coding with  $p > 1/2$  exists. Then, by definition there are  $2^{2^{2m}}$  encoding states  $\{\rho_w\}_{w \in \{0,1\}^{2^{2m}}}$  and  $2^{2m}$  POVMs  $\{E_0^i, E_1^i\}_{i \in \{1,2,\dots,2^{2m}\}}$  such that  $\text{Tr}(E_0^i \rho_w) > 1/2$  if  $w_i = 0$  and  $\text{Tr}(E_0^i \rho_w) < 1/2$  if  $w_i = 1$ . Since  $E_0^i$  and  $E_1^i$  are  $2^m$ -dimensional nonnegative Hermitian, they can be written as:

$$\begin{aligned} E_0^i &= \sum_{j=1}^{2^m} \alpha_j^i |u_j^i\rangle\langle u_j^i| \\ E_1^i &= \sum_{j=1}^{2^m} (1 - \alpha_j^i) |u_j^i\rangle\langle u_j^i|, \end{aligned}$$

such that  $\{|u_j^i\rangle\}_{j=1}^{2^m}$  is an orthonormal basis. Thus, for all  $i \in \{1, \dots, 2^{2m}\}$ , the following must be satisfied:

$$\forall i \left[ \sum_{j=1}^{2^m} \alpha_j^i \langle u_j^i | \rho_w | u_j^i \rangle \begin{cases} > 1/2 & \text{if } w_i = 0, \\ < 1/2 & \text{if } w_i = 1 \end{cases} \right]. \quad (5)$$

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

$$\forall i \left[ \sum_{j=1}^{2^m} \left( \frac{\alpha_j^i}{2^m} + \frac{\alpha_j^i}{2} \vec{r}_w \cdot \vec{u}_j^i \right) \begin{cases} > 1/2 & \text{if } w_i = 0, \\ < 1/2 & \text{if } w_i = 1 \end{cases} \right] \quad (6)$$

by (4). (Notice that an  $m$ -qubit state can be identified with a  $2^m$ -level quantum state.) If we let  $c_i = 1/2 - \sum_{j=1}^{2^m} \frac{\alpha_j^i}{2^m}$  and  $\vec{s}_i = \sum_{j=1}^{2^m} \frac{\alpha_j^i}{2} \vec{u}_j^i$ , (6) is simplified as follows:

$$\forall i \left[ \vec{r}_w \cdot \vec{s}_i \begin{cases} > c_i & \text{if } w_i = 0, \\ < c_i & \text{if } w_i = 1 \end{cases} \right]. \quad (7)$$

Let  $B$  be the set of all Bloch vectors for  $m$ -qubit states. Note that  $B \subseteq \mathbb{R}^{2^{2m}-1}$ . Let also  $D_{s_i}^{(0)}$  and  $D_{s_i}^{(1)}$  be the subsets of  $\mathbb{R}^{2^{2m}-1}$  defined by  $D_{s_i}^{(0)} = \{\vec{r} \in B \mid \vec{r} \cdot \vec{s}_i > c_i\}$  and  $D_{s_i}^{(1)} = \{\vec{r} \in B \mid \vec{r} \cdot \vec{s}_i < c_i\}$ , respectively. By (7), all  $2^{2^{2m}}$  subsets  $D_w = \bigcap_{i=1}^{2^{2m}} D_{s_i}^{(w_i)}$  must not be empty. These subsets are included into non-empty regions of  $\mathbb{R}^{2^{2m}-1}$  divided by the  $2^{2m}$  hyperplanes  $\{\vec{r} \mid \vec{r} \cdot \vec{s}_i = c_i\}$ .  $\square$

Now, the following geometric fact (see, e.g., [8]) completes the proof of Theorem 3.4.

**Lemma 3.6**  *$\mathbb{R}^{2^{2m}-1}$  cannot be divided into  $2^{2^{2m}}$  non-empty regions by  $2^{2m}$  hyperplanes.*

## 4 Applications to Network Coding

Network coding, introduced in [2], is nicely explained by using the so-called Butterfly network as shown in Fig. 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.

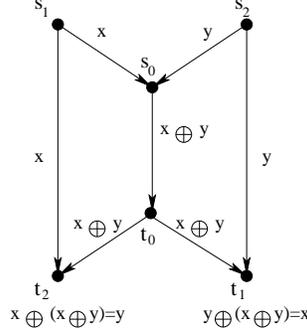


Figure 3: Butterfly network

The paper [9] 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.

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. 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, then the network can be viewed as a  $(4, 1, p)$ -QRA coding system, which cannot achieve  $p > 1/2$ .

## 5 Concluding Remarks

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  $x = x_1x_2x_3x_4x_5x_6x_7$ , the encoding state  $\rho(x)$  is

$$\alpha|\varphi(x_1x_2x_3)\rangle\langle\varphi(x_1x_2x_3)| \otimes |\varphi(x_4x_5x_6)\rangle\langle\varphi(x_4x_5x_6)| + (1 - \alpha)|\xi(x_7)\rangle\langle\xi(x_7)|$$

with  $\alpha = \frac{6}{7+\sqrt{3}}$ , where  $|\xi(0)\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$  and  $|\xi(1)\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ . To obtain any one of  $x_1, x_2$  and  $x_3$  (resp.  $x_4, x_5$  and  $x_6$ ) use the measurement of the  $(3, 1, 0.79)$ -QRA coding on the first qubit (resp. second qubit) of  $\rho(x)$ . To obtain  $x_7$ , use the projective measurement  $E^7 = \{E_0^7, E_1^7\}$  on  $\rho(x)$ , where  $E_0^7 = |00\rangle\langle 00| + |11\rangle\langle 11|$  and  $E_1^7 = |01\rangle\langle 01| + |10\rangle\langle 10|$ . Details are omitted.

## References

- [1] S. Aaronson, QMA/qpoly  $\subseteq$  PSPACE/poly: De-Merlinizing quantum protocols, to appear in *Proceedings of 21st IEEE Conference on Computational Complexity*, 2006. Also available at quant-ph/0510230.

- [2] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, Network information flow, *IEEE Transactions on Information Theory*, vol. 46, no. 4, pp. 1204–1216, 2000.
- [3] R. Alicki and K. Lendi, *Quantum Dynamical Semigroups and Applications, Lecture Notes in Physics*, vol. 286, Springer, 1987.
- [4] A. Ambainis, A. Nayak, A. Ta-shma, and U. Vazirani, Dense quantum coding and a lower bound for 1-way quantum automata, in *Proceedings of 31st ACM Symposium on Theory of Computing*, pp. 376–383, 1999.
- [5] A. Ambainis, A. Nayak, A. Ta-shma, and U. Vazirani, Dense quantum coding and quantum finite automata, *Journal of the ACM*, vol. 49, no. 4, pp. 496–511, 2002.
- [6] H. Buhrman and R. de Wolf, Communication complexity lower bounds by polynomials, in *Proceedings of 16th IEEE Conference on Computational Complexity*, pp. 120–130, 2001.
- [7] V. Bužek and M. Hillery, Quantum copying: Beyond the no-cloning theorem, *Physical Review A*, vol. 54, pp. 1844–1852, 1996.
- [8] H. Edelsbrunner, *Algorithms in Computational Geometry*, Springer-Verlag, 1987.
- [9] M. Hayashi, K. Iwama, H. Nishimura, R. Raymond, and S. Yamashita, Quantum network coding, preprint available at quant-ph/0601088.
- [10] A. S. Holevo, On capacity of a quantum communications channel, *Problems of Information Transmission*, vol. 15, no. 4, pp. 247–253, 1979.
- [11] L. Jakóbczyk and M. Siennicki, Geometry of Bloch vectors in two-qubit system, *Physics Letters A*, vol. 286, pp. 383–390, 2001.
- [12] I. Kerenidis and R. de Wolf, Exponential lower bound for 2-query locally decodable codes via a quantum argument, *Journal of Computer System and Science*, vol. 69, no. 3, pp. 395–420, 2004.
- [13] G. Kimura, The Bloch vector for N-level systems, *Physics Letters A*, vol. 314, pp. 339–349, 2003.
- [14] H. Klauck, On quantum and probabilistic communication: Las Vegas and one-way protocols, in *Proceedings of 32nd ACM Symposium on Theory of Computing*, pp. 644–651, 2000.
- [15] R. König, U. M. Maurer, and R. Renner, On the power of quantum memory, *IEEE Transactions on Information Theory*, vol. 51, no. 7, pp. 2391–2401, 2005.
- [16] G. Mahler and V. A. Weberruss, *Quantum Networks*, Springer-Verlag, 1995.
- [17] A. Nayak, Optimal lower bounds for quantum automata and random access codes, in *Proceedings of 40th IEEE Symposium on Foundations of Computer Science*, pp. 369–376, 1999.
- [18] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge, 2000.
- [19] S. Wehner and R. de Wolf, Improved lower bounds for locally decodable codes and private information retrieval, in *Proceedings of 32nd International Colloquium on Automata, Languages and Programming, Lecture Notes in Computer Science*, vol. 3580, pp.1424–1436, 2005.