Some Binary Quantum Codes with Good Burst-Error-Correcting Capabilities

Kin-ichiroh Tokiwa, Kazutaka Kiyama and Takahiro Yamasaki

Abstract

Quantum error-correcting codes have been developed as one of the promising tools for protecting quantum information against quantum errors. A great deal of effort has been made mainly to construct efficient quantum random-error-correcting codes. In this article, we investigate a class of quantum codes capable of correcting quantum burst errors, and present a list of some new good quantum burst-error-correcting codes of length less than or equal to 51.

keywords: quantum error-correcting codes, CSS codes, burst error correction.

1 Introduction

The first quantum error-correcting code was discovered by Shor [1]. Since then, the theory of quantum error-correcting codes has progressed rapidly, and various code constructions have been proposed on the assumption that quantum errors occur independently. One of the most important families of quantum error-correcting codes has been provided by Steane [2] and Calderbank and Shor [3]. These codes are commonly referred to as Calderbank-Shor-Steane (CSS) codes. On the other hand, Vatan, Roychowdhury, and Anantram [4] have explored the design of quantum error-correcting codes for the case when quantum errors occur predominantly in bursts. However, few quantum burst-error-correcting codes have been known so far.

The main purpose of our work is to find out many good quantum codes capable of correcting quantum burst errors. In this article, we consider the subject from the following points of view:

- focusing our attention on a class of CSS type nondegenerate binary quantum error-correcting codes,
- utilizing an algorithm [5] which can efficiently search a basis of any CSS type quantum error-correcting code, and
- specifying good quantum burst-error-correcting codes in terms of computer search.

As a result, we present a list of some new good quantum burst-error-correcting codes of length up to 51.

---

* Received November, 1, 2004.
Department of Electrical Engineering and Electronics, Osaka Sangyo University

2 CSS Type Quantum Codes

For $n > k$, an $[[n, k]]$ binary quantum error-correcting code can be regarded as a mapping of k qubits (i.e., a Hilbert space of dimension 2^k) into n qubits (i.e., a Hilbert space of dimension 2^n). Therefore, this code can be uniquely specified with 2^k orthonormal basis $|\boldsymbol{v}_1\rangle, |\boldsymbol{v}_2\rangle, \ldots, |\boldsymbol{v}_{2^k}\rangle$, where $\boldsymbol{v}_i$ are binary vectors of length n and $|\boldsymbol{v}_i\rangle$ denote quantum states of n qubits. Note here that, to simplify notation, the normalization factors are deleted throughout this article. In general, the kind of quantum errors to be considered are bit-flip errors, phase errors, and their combinations. Thus the CSS code construction [1]–[4] for burst-error correction is summarized as follows:

For $i = 1, 2$, let $\mathcal{C}_i$ be an $[n, k_i]$ binary classical linear code capable of correcting all burst errors of length b_i or less. Suppose that the dual of $\mathcal{C}_2$ is a subcode of $\mathcal{C}_1$ (i.e., $\mathcal{C}_2^\perp \subseteq \mathcal{C}_1$) and $k_1 + k_2 > n$. Then we have an $[[n, k_1 + k_2 - n]]$ CSS type quantum code $\mathcal{Q}$ which can correct all quantum burst errors of length $b = \min(b_1, b_2)$ or less. Basis vectors of $\mathcal{Q}$ can be represented as

$$|\boldsymbol{v}_i\rangle = \sum_{\boldsymbol{c} \in \mathcal{C}_2^\perp} |\boldsymbol{c} + \boldsymbol{a}_i\rangle, \tag{1}$$

where $\boldsymbol{a}_i$ are chosen from cosets of $\mathcal{C}_2^\perp$ in $\mathcal{C}_1$, i.e., $\boldsymbol{a}_i \in \mathcal{C}_1/\mathcal{C}_2^\perp$.

According to the well-known Reiger bound [6], it is easily verified that an upper bound on the quantum burst-error-correcting capability b holds:

$$b \leq \left\lfloor \frac{n - \max(k_1, k_2)}{2} \right\rfloor. \tag{2}$$

Hereinafter, quantum codes that meet the bound (2) with equality will be called *good*. It should be noted that there may exist more powerful codes among the other kind of quantum codes (e.g., degenerate quantum codes). In this article, however, only CSS type nondegenerate binary quantum codes will be considered. This is because such codes can be handled easily. Moreover, note that in this article we exclude a burst error defined with cyclic boundary conditions, that is to say, *an end-around burst error* [6].

3 Search Algorithm

As mentioned above, if any suitable classical linear codes $\mathcal{C}_1$ and $\mathcal{C}_2$ could be obtained, then a CSS type quantum burst-error-correcting code $\mathcal{Q}$ can be constructed. However, it is not easy to find such codes $\mathcal{C}_1$ and $\mathcal{C}_2$ constructively. Hence we take a way to search for an appropriate code $\mathcal{C}_1$ for a given code $\mathcal{C}_2$ (equivalently, $\mathcal{C}_2^\perp$). The outline of our search procedure is summarized as follows:

Step 1: Choose an $[n, k_2]$ classical cyclic code $\mathcal{C}_2$ and its $[n, n-k_2]$ dual code $\mathcal{C}_2^\perp$, and determine their burst-error-correcting capabilities b_2 and $b_2^\perp$, respectively.

Step 2: Search for an $[n, k_1]$ classical linear code $\mathcal{C}_1$ with burst-error-correcting capability b_1 which includes $\mathcal{C}_2^\perp$ as a subcode, where $b_1 = \min(b_2, b_2^\perp)$.

Step 3: Set $b = \min(b_1, b_2)$. If the value of b meets the bound (2) with equality, then an $[[n, k_1 + k_2 - n]]$ good quantum burst-error-correcting code Q is obtained. Otherwise, return to **Step 1** and change the initial codes.

In **Step 1**, we investigate burst-error-correcting capabilities of $\mathcal{C}_2$ and $\mathcal{C}_2^{\perp}$ by checking whether all syndromes of the possible burst error patterns are distinct. Clearly, the computational complexity of such method grows exponentially as burst length to be considered becomes longer. Thus it would be necessary to adopt more efficient schemes (e.g., [7]) in order to search more powerful codes.

In **Step 2**, we take advantage of a slightly modified version of the search algorithm proposed in [5]. In the following, it will be called *T-algorithm*, and will be described briefly. See [5] for more details.

Let us provide some definitions and notations. For a vector $\boldsymbol{x} = (x_1, x_2, \ldots, x_L)$ of any length L and for any integer ℓ $(1 \leq \ell \leq L)$, two kinds of functions $\Phi_\ell(\boldsymbol{x})$ and $\Psi_\ell(\boldsymbol{x})$ are defined as

$$\Phi_\ell(\boldsymbol{x}) = x_\ell \tag{3}$$

and

$$\Psi_\ell(\boldsymbol{x}) = (x_1, \ldots, x_{\ell-1}, x_{\ell+1}, \ldots, x_L). \tag{4}$$

The former is a function that takes out the ℓ-th component of $\boldsymbol{x}$, and the latter is a function that deletes the ℓ-th component from $\boldsymbol{x}$. Moreover, let $\left(\mathbf{0}^k; \boldsymbol{x}\right)$ denote a concatenation of a string of k zeros and a vector $\boldsymbol{x}$.

T-algorithm: We consider an $[n, k_2]$ classical cyclic code $\mathcal{C}_2$ and its $[n, n-k_2]$ dual code $\mathcal{C}_2^{\perp}$ whose burst-error-correcting capabilities are b_2 and $b_2^{\perp}$, respectively. Also, we assume a parity-check matrix H of $\mathcal{C}_2^{\perp}$ is given in reduced-echelon canonical form [8]. In other words, suppose that the leftmost part of H is a $k_2 \times k_2$ identity matrix. Then the following steps are executed:

step i : Obtain a set of sums of syndromes in $\mathcal{C}_2^{\perp}$ as

$$\Sigma^{(1)} = \left\{ (\boldsymbol{e} + \boldsymbol{e}')H^T \mid \boldsymbol{e}, \boldsymbol{e}' \in \mathcal{E} \right\},$$

where $\mathcal{E}$ is a set of all patterns of possible burst errors of length b_1 $\left(= \min(b_2, b_2^{\perp})\right)$ or less.

step ii : Initialize a column permutation matrix ρ_1 as an $n \times n$ identity matrix.

step iii : Set $\kappa_1 = n - k_2$, $\boldsymbol{a}_1 = \mathbf{0}^n$, and $j = 1$.

step iv : If a set

$$F_2^{n-\kappa_j} \backslash \Sigma^{(j)} = \left\{ \boldsymbol{x} \mid \boldsymbol{x} \in F_2^{n-\kappa_j} \wedge \boldsymbol{x} \notin \Sigma^{(j)} \right\}$$

is empty, then go to step vi. Otherwise, select any vector $\boldsymbol{x}_j \in F_2^{n-\kappa_j} \backslash \Sigma^{(j)}$, and make up an auxiliary vector

$$\boldsymbol{u}_j = (\mathbf{0}^{\kappa_j}; \boldsymbol{x}_j)\rho_j^{-1}$$

and 2^{j-1} vectors

$$\boldsymbol{a}_{\ell+2^{j-1}} = \boldsymbol{a}_\ell + \boldsymbol{u}_j$$

for $1 \leq \ell \leq 2^{j-1}$.

step v : Using a value ν_j such that

$$\Phi_\ell(\boldsymbol{x}_j) = \begin{cases} 0 & \text{for } 1 \leq \ell < \nu_j \\ 1 & \text{for } \ell = \nu_j \end{cases},$$

update a set of sums of syndromes $\Sigma^{(j+1)}$ and a column permutation matrix ρ_{j+1} as

$$\Sigma^{(j+1)} = \left\{ \Psi_{\nu_j}(\boldsymbol{\sigma}) + \Phi_{\nu_j}(\boldsymbol{\sigma})\Psi_{\nu_j}(\boldsymbol{x}_j) \mid \boldsymbol{\sigma} \in \Sigma^{(j)} \right\}$$

and

$$\rho_{j+1} = \rho_j \pi_j,$$

where π_j is an $n \times n$ column permutation matrix by which the $(\kappa_j + \nu_j)$-th column is moved just before the $(\kappa_j + 1)$-st column. Then set $\kappa_{j+1} = \kappa_j + 1$ and $j = j + 1$, and go to step iv.

step vi : Set $k_1 = \kappa_j$ as the dimension of the desired code $\mathcal{C}_1$, and output auxiliary vectors $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_{j-1}$ and coset leaders $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_{2^{j-1}}$ in $\mathcal{C}_1/\mathcal{C}_2^{\perp}$.

In **Step 3**, in order to find out good codes, we require that the value of $b = \min(b_1, b_2)$ meets the bound (2) with equality. Clearly, however, this restriction can be relaxed. In any case, we are able to obtain an $[[n, k_1 + k_2 - n]]$ quantum code $\mathcal{Q}$ which can correct quantum burst errors of length b or less and whose basis vectors are represented as (1) by using vectors $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_{2^{j-1}}$ given in **step vi**.

4 Results

In our computer search, the initial codes $\mathcal{C}_2^{\perp}$ have been chosen from almost all of binary classical cyclic codes of length up to 64 whose generator polynomials have degree 35 or less. Some good quantum burst-error-correcting codes obtained by computer search are listed in Table 1, in which the following notations are used:

▷ in relation to quantum code $\mathcal{Q}$

$$n := \text{code length}$$
$$k := \text{dimension}$$
$$b := \text{maximum length of correctable burst errors}$$

▷ in relation to classical codes $\mathcal{C}_2$ and $\mathcal{C}_2^{\perp}$

$$b_2,\ b_2^{\perp} := \text{maximum length of correctable burst errors}$$
$$g(x) := \text{generator polynomial of } \mathcal{C}_2^{\perp}$$

▷ in relation to classical code $\mathcal{C}_1$

$$b_1 := \text{maximum length of correctable burst errors}$$
$$\boldsymbol{u}_j := \text{auxiliary vectors for constructing } \mathcal{C}_1$$

It should be noted that the generator polynomial $g(x)$ and the auxiliary vector $\boldsymbol{u}_j$ are both given in an octal representation. When the octal representation of $g(x)$ is expanded in binary, the binary digits are the coefficients of the polynomial, with the high-order coefficients at the left. In addition, when the octal representation of $\boldsymbol{u}_j$ is expanded in binary, the binary digits are assigned to the rightmost components of the vector of length n. On the other hand, it is easily verified that a generator polynomial of $\mathcal{C}_2$ can be derived from $g(x)$ as a reciprocal polynomial of $(x^n + 1)/g(x)$.

It should be also noted that the code $\mathcal{C}_1$ is not cyclic but linear. Thus the code can be uniquely represented in terms of its generator matrix. Let G_1 and $G_2^{\perp}$ denote generator matrices of the codes $\mathcal{C}_1$ and $\mathcal{C}_2^{\perp}$, respectively. Then the following relationship between these matrices holds:

$$G_1 = \begin{pmatrix} G_2^{\perp} \\ \hdashline \boldsymbol{u}_1 \\ \vdots \\ \boldsymbol{u}_k \end{pmatrix} \tag{5}$$

In Table 1, the symbol "a" means a good code which meets the bound (2) with equality, and the symbol "b" shows a code whose burst-error-correcting capability is only one smaller than the maximum value ensured by the bound (2). In addition, codes assigned the symbol "c" in Table 1 are worthy of attention. Calderbank, Rains, Shor, and Sloane [9] gave a useful table on the highest achievable minimum distance in any quantum random-error-correcting code of length up to 30, and Grassl [10] extended the table to codes of length up to 36. From these tables, it is possible to evaluate the limits of quantum random-error-correcting codes. It is clear that we can successfully correct quantum burst errors of length up to such evaluated limits by using those quantum random-error-correcting codes. However, quantum codes designated in Table 1 as the symbol"c" allow us to correct longer burst errors than any best quantum random-error-correcting code. Finally we also emphasize that the seven codes with the symbol "d" have the same correcting capabilities even if the end-around burst errors are included.

Table 1 Parameters of Good Binary Quantum Burst-Error-Correcting Codes (Length up to 51)

$\mathcal{Q}$			$\mathcal{C}_2$	$\mathcal{C}_2^{\perp}$		$\mathcal{C}_1$				
n	k	b	b_2	$b_2^{\perp}$	$g(x)$	b_1	$\boldsymbol{u}_j$ $(j = 1, 2, \ldots, k)$			
15	2	3	3	4	1163	3	257	433		a c
15	4	2	2	5	3545	2	25	52	211	a c d
							407			
21	3	4	4	6	13123	4	1467	2531	4605	a c d
21	6	3	3	7	61671	3	111	222	444	a c
							2061	4036	11062	
23	1	5	5	5	12237	5	6165			a c d
24	2	4	4	4	12105	4	467	5316		b c d
28	4	5	5	7	170377	5	2661	10513	20570	a c
							55420			
28	6	4	4	6	270547	4	421	1042	2104	b c
							4233	20176	50254	
30	5	6	6	8	1012405	6	23221	43762	155304	a c
							376727	777771		
30	6	5	5	8	1533407	5	2041	4102	10204	b c
							20456	41273	401403	
30	9	4	4	10	4202425	4	421	1042	2104	b c
							4210	20023	40041	
							100114	200205	410256	

Table 1 (*Continued*)

$\mathcal{Q}$			$\mathcal{C}_2$	$\mathcal{C}_2^{\perp}$		$\mathcal{C}_1$				
n	k	b	b_2	$b_2^{\perp}$	$g(x)$	b_1	$\boldsymbol{u}_j$ $(j = 1, 2, \ldots, k)$			
31	1	7	7	8	200427	7	177415			a c d
31	3	6	7	6	312017	6	12565	63307	104233	a c
31	8	5	5	10	5203467	5	2041	4102	10204	a c
							20410	41020	200117	
							400252	2101764		
31	11	4	4	10	11223653	4	421	1042	2104	b c
							4210	20023	40041	
							100114	200224	410004	
							1000141	6010332		
33	8	5	5	9	7142147	5	2041	4102	10204	b c
							20410	41021	200101	
							400053	1000405		
34	4	6	6	6	1012501	6	10313	20115	41454	b c
							502036			
35	4	7	7	8	6215517	7	40603	100221	201357	a c
							407046			
35	7	6	6	10	23766233	6	10101	20202	40404	a c
							101010	202020	404047	
							2000117			
35	11	5	5	11	55326013	5	2041	4102	10204	a c
							20453	41121	200051	
							400103	1000217	2000424	
							4100264	10101722		
35	14	4	4	10	244303045	4	421	1042	2104	b c
							4210	20023	40041	
							100114	200204	410001	
							1000045	2000106	10000174	
							20010004	40000235		
39	11	6	6	13	663364621	6	10101	20202	40404	a
							101010	202020	404040	
							2000103	4000205	10000411	
							20001021	40002260		
45	2	10	10	11	107767117	10	4023003	40124201		a
45	6	9	9	12	777070007	9	1003005	2005017	4011033	a
							10021243	20310350	40740522	
47	1	11	11	11	106331123	11	75667061			a d
51	1	12	12	12	246527647	12	142315235			a d

5 Conclusion

We have investigated a class of CSS type nondegenerate binary quantum codes capable of correcting quantum burst errors. As a result, we have given a list of some new good quantum burst-error-correcting codes of length up to 51 in terms of computer search. These codes are very efficient and attractive for correcting quantum burst errors excluding end-around burst errors.

Acknowledgment

This work was supported by Grant-in-Aid for Scientific Research (C)(2) (No.14550387) from Japan Society for the Promotion of Science.

References

[1] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," *Phys. Rev. A,* vol.52, pp.R2493–R2496, Oct. 1995.

[2] A. M. Steane, "Error correcting codes in quantum theory," *Phys. Rev. Lett.,* vol.77, pp.793–797, July 1996.

[3] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Phys. Rev. A,* vol.54, pp.1098–1105, Aug. 1996.

[4] F. Vatan, V. P. Roychowdhury, and M. P. Anantram, "Spatially correlated qubit errors and burst-correcting quantum codes," *IEEE Trans. Inform. Theory,* vol.45, pp.1703–1708, July 1999.

[5] K. Tokiwa and H. Tanaka, "A search algorithm for bases of Calderbank-Shor-Steane type quantum error-correcting codes," *IEICE Trans. Fundamentals,* vol.E84-A, pp.860–865, March 2001.

[6] S. Lin and D. J. Costello, Jr., *Error Control Coding: Fundamentals and Applications*, Prentice Hall, 1983.

[7] K. Tokiwa, M. Kasahara, and T. Namekawa, "Burst-error-correction capability of cyclic codes," *Trans. of IECE A,* vol.J66-A, pp.993–999, Oct. 1983. (In Japanese)

[8] W. W. Peterson and E. J. Weldon, Jr., *Error-Correcting Codes*, 2nd ed., The MIT Press, 1972.

[9] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction via codes over $GF(4)$," *IEEE Trans. Inform. Theory,* vol.44, pp.1369–1387, July 1998.

[10] M. Grassl, "Bounds on $d_{\min}$ for additive $[[n,k,d]]$ QECC (extended version of Table III of the above paper [9])," [Online]. Available: http://iaks-www.ira.uka.de/home/grassl/QECC/TableIII.html.