PAPER Special Section on Information Theory and Its Applications

Constructing Quantum Error-Correcting Codes for p^m-State Systems from Classical Error-Correcting Codes*

Ryutaroh MATSUMOTO†, *Student Member and* Tomohiko UYEMATSU†, *Regular Member*

SUMMARY We generalize the construction of quantum error-correcting codes from $\mathbf{F}_4$-linear codes by Calderbank et al. to p^m-state systems. Then we show how to determine the error from a syndrome. Finally we discuss a systematic construction of quantum codes with efficient decoding algorithms.

key words: *quantum codes, stabilizer codes, additive codes, self-orthogonal codes*

1. Introduction

Quantum error-correcting codes have attracted much attention. Among many research articles, the most general and systematic construction is the so called *stabilizer code construction* [6] or *additive code construction* [2], which constructs a quantum error-correcting code as an eigenspace of an Abelian subgroup S of the error group. Thereafter Calderbank et al. [3] proposed a construction of S from an additive code over the finite field $\mathbf{F}_4$ with 4 elements.

These constructions work for tensor products of 2-state quantum systems. However Knill [8], [9] and Rains [13] observed that the construction [2], [6] can be generalized to n-state systems by an appropriate choice of the error basis. Rains [13] also generalized the construction [3] using additive codes over $\mathbf{F}_4$ to p-state quantum systems, but his generalization does not relate the problem of quantum code construction to classical error-correcting codes. We propose a construction of quantum error-correcting codes for p^m-state systems from classical error-correcting codes which is a generalization of [3].

Throughout this paper, p denotes a prime number and m a positive integer. This paper is organized as follows. In Sect. 2, we review the construction of quantum codes for nonbinary systems. In Sect. 3, we propose a construction of quantum codes for p-state systems from classical codes over $\mathbf{F}_{p^2}$. In Sect. 4, we propose a construction of quantum codes for p^m-state systems from classical linear codes over $\mathbf{F}_{p^{2m}}$. In Sect. 5, we discuss a systematic construction of quantum codes with efficient decoding algorithms.

Manuscript received January 20, 2000.
Manuscript revised April 10, 2000.

†The authors are with the Department of Electrical and Electronic Engineering, Tokyo Institute of Technology, Tokyo, 152-8552 Japan. The first author is supported by JSPS Research Fellowships for Young Scientists.

*The results in this paper were partly presented at the 2000 IEICE General Conference, Hiroshima Univ., Japan, March 28–31, 2000 [12].

2. Stabilizer Coding for p^m-State Systems

2.1 Code Construction

We review the generalization [8], [9], [13] of the construction [2], [6]. First we consider p-state systems. We shall construct a quantum code Q encoding quantum information in p^k-dimensional linear space into $\mathbb{C}^{p^n}$. Q is said to have minimum distance d and said to be an $[[n,k,d]]_p$ quantum code if it can detect up to $d-1$ quantum local errors. Let λ be a primitive p-th root of unity, C_p, D_λ $p\times p$ unitary matrices defined by $(C_p)_{ij} = \delta_{j-1,i \bmod p}$, $(D_\lambda)_{ij} = \lambda^{i-1}\delta_{i,j}$. Notice that C_2 and D_{-1} are the Pauli spin matrices σ_x and σ_z. We consider the error group E consisting of $\lambda^j w_1 \otimes \cdots \otimes w_n$, where j is an integer, w_i is $C_p^a D_\lambda^b$ with some integers a, b.

For row vectors $\boldsymbol{a} = (a_1, \ldots, a_n)$, $\boldsymbol{b} = (b_1, \ldots, b_n)$, $(\boldsymbol{a}|\boldsymbol{b})$ denotes the concatenated vector $(a_1, \ldots, a_n, b_1, \ldots, b_n)$ as used in [3]. For vectors $(\boldsymbol{a}|\boldsymbol{b}), (\boldsymbol{a}'|\boldsymbol{b}') \in \mathbf{F}_p^{2n}$, we define the alternating inner product

$$((\boldsymbol{a}|\boldsymbol{b}), (\boldsymbol{a}'|\boldsymbol{b}')) = \langle \boldsymbol{a}, \boldsymbol{b}' \rangle - \langle \boldsymbol{a}', \boldsymbol{b} \rangle, \tag{1}$$

where $\langle , \rangle$ denotes the standard inner product in $\mathbf{F}_p^n$. For $\boldsymbol{a} = (a_1, \ldots, a_n) \in \mathbf{F}_p^n$, we define

$$X(\boldsymbol{a}) = C_p^{a_1} \otimes \cdots \otimes C_p^{a_n},$$

$$Z(\boldsymbol{a}) = D_\lambda^{a_1} \otimes \cdots \otimes D_\lambda^{a_n}.$$

Then we have

$$\begin{aligned} &X(\boldsymbol{a})Z(\boldsymbol{b})X(\boldsymbol{a}')Z(\boldsymbol{b}') \\ &\quad = \lambda^{\langle \boldsymbol{a},\boldsymbol{b}'\rangle - \langle \boldsymbol{a}',\boldsymbol{b}\rangle} X(\boldsymbol{a}')Z(\boldsymbol{b}')X(\boldsymbol{a})Z(\boldsymbol{b}). \end{aligned} \tag{2}$$

For $(\boldsymbol{a}|\boldsymbol{b}) = (a_1, \ldots, a_n, b_1, \ldots, b_n) \in \mathbf{F}_p^{2n}$, we define the weight of $(\boldsymbol{a}|\boldsymbol{b})$ to be

$$\sharp\{i \mid a_i \neq 0 \text{ or } b_i \neq 0\}. \tag{3}$$

Theorem 1: Let C be an $(n-k)$-dimensional $\mathbf{F}_p$-linear subspace of $\mathbf{F}_p^{2n}$ with the basis $\{(\boldsymbol{a}_1|\boldsymbol{b}_1), \ldots, (\boldsymbol{a}_{n-k}|\boldsymbol{b}_{n-k})\}$, $C^\perp$ the orthogonal space of C with respect to the inner product (1). Suppose that $C \subseteq C^\perp$ and the minimum weight (3) of $C^\perp \setminus C$ is d. Then the subgroup S of E generated by $\{X(\boldsymbol{a}_1)Z(\boldsymbol{b}_1), \ldots, X(\boldsymbol{a}_{n-k})Z(\boldsymbol{b}_{n-k})\}$ is Abelian, and an eigenspace of S is an $[[n,k,d]]_p$ quantum code.

Next we consider quantum codes for p^m-state systems, where m is a positive integer. But the code construction for p^m-state systems is almost the same as that for p-state systems, because the state space of a p^m-state system can be regarded as the m-fold tensor products of that of a p-state system. We shall construct a quantum code encoding quantum information in p^{mk}-dimensional linear space into $\mathbb{C}^{p^{mn}}$. For $(\boldsymbol{a}|\boldsymbol{b}) = (a_{1,1}, a_{1,2}, \ldots, a_{1,m}, a_{2,1}, \ldots, a_{n,m}, b_{1,1}, \ldots, b_{n,m}) \in \mathbf{F}_p^{2mn}$, we define the weight of $(\boldsymbol{a}|\boldsymbol{b})$ to be

$$\sharp\{i \mid \text{there exists nonzero element in } \{a_{i,1}, \ldots, a_{i,m}, b_{i,1}, \ldots, b_{i,m}\}\}. \tag{4}$$

Corollary 2: Let C be an $(mn-mk)$-dimensional $\mathbf{F}_p$-linear subspace of $\mathbf{F}_p^{2mn}$ with the basis $\{(\boldsymbol{a}_1|\boldsymbol{b}_1), \ldots, (\boldsymbol{a}_{mn-mk}|\boldsymbol{b}_{mn-mk})\}$, $C^\perp$ the orthogonal space of C with respect to the inner product (1). Suppose that $C \subseteq C^\perp$ and the minimum weight (4) of $C^\perp \setminus C$ is d. Then the subgroup S of E generated by $\{X(\boldsymbol{a}_1)Z(\boldsymbol{b}_1), \ldots, X(\boldsymbol{a}_{mn-mk})Z(\boldsymbol{b}_{mn-mk})\}$ is Abelian, and an eigenspace of S is an $[[n,k,d]]_{p^m}$ quantum code.

2.2 Error Correction Procedure

In this subsection we review the process of correcting errors. Let $H = \mathbb{C}^p$, $H^{\otimes n} \supset Q$ the quantum code constructed by Theorem 1, and H_{env} the Hilbert space representing the environment. Suppose that we send a codeword $|\psi\rangle \in Q$, that the state of the environment is initially $|\psi_{\mathrm{env}}\rangle \in H_{\mathrm{env}}$, and that we receive $|\psi'\rangle \in H^{\otimes n} \otimes H_{\mathrm{env}}$. Then there exists a unitary operator U such that

$$|\psi'\rangle = U(|\psi\rangle \otimes |\psi_{\mathrm{env}}\rangle).$$

If U acts nontrivially τ $(0 \le \tau \le n)$ subsystems among n tensor product space $H^{\otimes n}$, then τ is said to be *the number of errors.*

We assume that $2\tau + 1 \le d$, where d is as in Theorem 1. If we measure each observable in $H^{\otimes n}$ whose eigenspaces are the same as those of $X(\boldsymbol{a}_i)Z(\boldsymbol{b}_i)$ for $i = 1, \ldots, n-k$, where $X(\boldsymbol{a}_i)Z(\boldsymbol{b}_i)$ is as defined in Theorem 1, then the entangled state $|\psi'\rangle$ is projected to $A|\psi\rangle \otimes |\psi'_{\mathrm{env}}\rangle$, for some $A \in E$ and $|\psi'_{\mathrm{env}}\rangle \in H_{\mathrm{env}}$, by the measurements. By the measurement outcomes we can find a unitary operator $A' \in E$ such that $A'A|\psi\rangle = |\psi\rangle$.

The determination of A' requires exhaustive search in general. Thus the computational cost finding A' from the measurement outcomes is large when both n and d are large. However, in certain special cases we can efficiently determine A'. An efficient method finding A' is presented in Sect. 3.2.

Remark 3: The error correction method presented in this subsection is not explicitly mentioned in the papers [2], [3], [6]. Still, it can be derived from general facts on quantum error correction presented in [1], [5], [10]. A readable exposition on the error correction procedure is provided by Preskill [16].

3. Construction of Quantum Codes for p-State Systems from Classical Codes

3.1 Codes for p-State Systems

In this subsection we describe how to construct quantum codes for p-state systems from additive codes over $\mathbf{F}_{p^2}$. Let ω be a primitive element in $\mathbf{F}_{p^2}$.

Lemma 4: $\{\omega, \omega^p\}$ is a basis of $\mathbf{F}_{p^2}$ over $\mathbf{F}_p$.

Proof: When $p = 2$ the assertion is obvious. We assume that $p \ge 3$. Suppose that $\omega^p = a\omega$ for some $a \in \mathbf{F}_p$. Then $\omega = \omega^{p^2} = (a\omega)^p = a^2\omega$, and a is either 1 or -1. If $a = 1$, then $\omega \in \mathbf{F}_p$ and ω is not a primitive element. If $a = -1$, then $\omega^{2p} = \omega^2$. This is a contradiction, because ω is a primitive element and $2p \not\equiv 2 \pmod{p^2-1}$. □

For $(\boldsymbol{a}|\boldsymbol{b}) \in \mathbf{F}_p^{2n}$ we define $\phi(\boldsymbol{a}|\boldsymbol{b}) = \omega\boldsymbol{a} + \omega^p\boldsymbol{b}$. Then the weight (3) of $(\boldsymbol{a}|\boldsymbol{b})$ is equal to the Hamming weight of $\phi(\boldsymbol{a}|\boldsymbol{b})$. For $\boldsymbol{c} = (c_1, \ldots, c_n), \boldsymbol{d} \in \mathbf{F}_{p^2}^n$, we define the inner product† of $\boldsymbol{c}$ and $\boldsymbol{d}$ by

$$\langle \boldsymbol{c}, \boldsymbol{d}^p\rangle - \langle \boldsymbol{c}^p, \boldsymbol{d}\rangle = \langle \boldsymbol{c}, \boldsymbol{d}^p\rangle - \langle \boldsymbol{c}, \boldsymbol{d}^p\rangle^p \tag{5}$$

where $\langle , \rangle$ denotes the standard inner product in $\mathbf{F}_{p^2}^n$ and $\boldsymbol{c}^p = (c_1^p, \ldots, c_n^p)$. For $(\boldsymbol{a}|\boldsymbol{b}), (\boldsymbol{a}'|\boldsymbol{b}') \in \mathbf{F}_p^{2n}$ the inner product (5) of $\phi(\boldsymbol{a}|\boldsymbol{b})$ and $\phi(\boldsymbol{a}'|\boldsymbol{b}')$ is

$$\begin{aligned}
&\langle \phi(\boldsymbol{a}|\boldsymbol{b}), \phi(\boldsymbol{a}'|\boldsymbol{b}')^p\rangle - \langle \phi(\boldsymbol{a}|\boldsymbol{b})^p, \phi(\boldsymbol{a}'|\boldsymbol{b}')\rangle \\
&\quad = \langle \omega\boldsymbol{a} + \omega^p\boldsymbol{b}, \omega^p\boldsymbol{a}'^p + \omega\boldsymbol{b}'^p\rangle \\
&-\langle \omega^p\boldsymbol{a}^p + \omega\boldsymbol{b}^p, \omega\boldsymbol{a}' + \omega^p\boldsymbol{b}'\rangle \\
&\quad = (\omega^2 - \omega^{2p})(\langle \boldsymbol{a}, \boldsymbol{b}'\rangle - \langle \boldsymbol{a}', \boldsymbol{b}\rangle).
\end{aligned}$$

Since ω is a primitive element, $\omega^2 \ne \omega^{2p}$. Thus the inner product (1) of $(\boldsymbol{a}|\boldsymbol{b})$ and $(\boldsymbol{a}'|\boldsymbol{b}')$ is zero iff the inner product (5) of $\phi(\boldsymbol{a}|\boldsymbol{b})$ and $\phi(\boldsymbol{a}'|\boldsymbol{b}')$ is zero. Thus we have

Theorem 5: Let C be an additive subgroup of $\mathbf{F}_{p^2}^n$ containing p^{n-k} elements, C' its orthogonal space with respect to the inner product (5). Suppose that $C' \supseteq C$ and the minimum Hamming weight of $C' \setminus C$ is d. By identifying $\phi^{-1}(C)$ with an Abelian subgroup of E via $X(\cdot)Z(\cdot)$, any eigenspace of $\phi^{-1}(C)$ is an $[[n,k,d]]_p$ quantum code.

†The map (5) is $\mathbf{F}_p$-bilinear but does not take values in $\mathbf{F}_p$. It is neither $\mathbf{F}_{p^2}$-bilinear nor $\mathbf{F}_{p^2}$-sesquilinear. Thus calling the map (5) "inner product" is a little abusive. But the map (5) can be converted to an $\mathbf{F}_p$-bilinear form by dividing it by $\omega^2 - \omega^{2p}$. For this reason we call the map (5) "inner product."

We next clarify the self-orthogonality of a linear code over $\mathbf{F}_{p^2}$ with respect to (5).

Lemma 6: Let C be a linear code over $\mathbf{F}_{p^2}$, and C' the orthogonal space of C with respect to (5). We define $C^p = \{\boldsymbol{x}^p \mid \boldsymbol{x} \in C\}$ and $(C^p)^\perp$ the orthogonal space of C^p with respect to the standard inner product. Then we have $C' = (C^p)^\perp$.

Proof: It is clear that $C' \supseteq (C^p)^\perp$. Suppose that $\boldsymbol{x} \in C'$. Then for all $\boldsymbol{y} \in C$, $\langle \boldsymbol{x}, \boldsymbol{y}^p \rangle - \langle \boldsymbol{x}, \boldsymbol{y}^p \rangle^p = 0$. Thus $\langle \boldsymbol{x}, \boldsymbol{y}^p \rangle \in \mathbf{F}_p$. Since $\langle \boldsymbol{x}, \omega^p \boldsymbol{y}^p \rangle - \langle \boldsymbol{x}, \omega^p \boldsymbol{y}^p \rangle^p = 0$, $\omega^p \langle \boldsymbol{x}, \boldsymbol{y}^p \rangle \in \mathbf{F}_p$. Since $\omega^p \in \mathbf{F}_{p^2} \setminus \mathbf{F}_p$, we conclude that $\langle \boldsymbol{x}, \boldsymbol{y}^p \rangle = 0$. □

Theorem 7: Let C be an $[n, (n-k)/2]$ linear code over $\mathbf{F}_{p^2}$ such that $C \subseteq (C^p)^\perp$. Suppose that the minimum Hamming weight of $(C^p)^\perp \setminus C$ is d. Then any eigenspace of $\phi^{-1}(C)$ is an $[[n,k,d]]_p$ quantum code.

3.2 Error Correction for p-State Systems

In this subsection we consider how to determine the error from measurements with quantum codes obtained via Theorem 7. We retain notations from Theorem 7. Suppose that $\boldsymbol{g}_1, \ldots, \boldsymbol{g}_r$ is an $\mathbf{F}_{p^2}$-basis of C. Then $\mathbf{F}_p$-basis of $\phi^{-1}(C)$ is $(\boldsymbol{a}_1|\boldsymbol{b}_1) = \phi^{-1}(\boldsymbol{g}_1), (\boldsymbol{a}_2|\boldsymbol{b}_2) = \phi^{-1}(\omega \boldsymbol{g}_1), \ldots, (\boldsymbol{a}_{2r}|\boldsymbol{b}_{2r}) = \phi^{-1}(\omega \boldsymbol{g}_r)$. Suppose that by the procedure in Sect. 2.2, the error is converted to $A \in E$ that corresponds to $\phi^{-1}(\boldsymbol{e})$ for some $\boldsymbol{e} \in \mathbf{F}_{p^2}^n$ via $X(\cdot)Z(\cdot)$, and the original quantum state is $|\psi\rangle$. We know which eigenspace of $X(\boldsymbol{a}_i)Z(\boldsymbol{b}_i)$ the vector $A|\psi\rangle$ belongs to. By Eq. (2)

$$X(\boldsymbol{a}_i)Z(\boldsymbol{b}_i)A|\psi\rangle = \lambda^\ell A|\psi\rangle,$$

where ℓ is the alternating inner product (1) of $(\boldsymbol{a}_i|\boldsymbol{b}_i)$ and $\phi^{-1}(\boldsymbol{e})$, which is denoted by $s_i \in \mathbf{F}_p$. Then we have

$$\langle \boldsymbol{g}_i, \boldsymbol{e}^p \rangle - \langle \boldsymbol{g}_i^p, \boldsymbol{e} \rangle = (\omega^2 - \omega^{2p}) s_{2i-1},$$

$$\langle \omega \boldsymbol{g}_i, \boldsymbol{e}^p \rangle - \langle \omega^p \boldsymbol{g}_i^p, \boldsymbol{e} \rangle = (\omega^2 - \omega^{2p}) s_{2i}.$$

It follows that $\langle \boldsymbol{g}_i^p, \boldsymbol{e} \rangle = (\omega^2 - \omega^{2p})(\omega s_{2i-1} - s_{2i})/(\omega^p - \omega)$. $\{\boldsymbol{g}_1^p, \ldots, \boldsymbol{g}_r^p\}$ can be used as rows of the check matrix of $(C^p)^\perp$. If we have a classical decoding algorithm for $(C^p)^\perp$ finding the error $\boldsymbol{e}$ from a classical syndrome $\langle \boldsymbol{g}_1^p, \boldsymbol{e} \rangle, \ldots, \langle \boldsymbol{g}_r^p, \boldsymbol{e} \rangle$, then we can find the quantum error $A \in E$.

Remark 8: In this section we assumed that ω is a primitive element in $\mathbf{F}_{p^2}$. It is enough to assume that ω belongs to $\mathbf{F}_{p^2}$ and ω^p, ω are linearly independent over $\mathbf{F}_p$.

4. Construction of Quantum Codes for p^m-State Systems from Classical Codes

4.1 Codes for p^m-State Systems

In this subsection we show a construction of quantum codes for p^m-state systems from classical linear codes over $\mathbf{F}_{p^{2m}}$. Our construction is based on the construction [4] by Chen which constructs quantum codes for 2-state systems from linear codes over $\mathbf{F}_{2^{2m}}$. We modify his construction so that we can estimate the minimum weight (4) from the original code over $\mathbf{F}_{p^{2m}}$.

We fix a normal basis $\{\theta, \theta^p, \ldots, \theta^{p^{2m-1}}\}$ of $\mathbf{F}_{p^{2m}}$ over $\mathbf{F}_p$. There always exists a normal basis of $\mathbf{F}_{p^{2m}}$ over $\mathbf{F}_p$ [11, Sect. VI,§13]. For $\boldsymbol{a} = (a_1, \ldots, a_m, b_1, \ldots, b_m), \boldsymbol{a}' = (a_1', \ldots, a_m', b_1', \ldots, b_m') \in \mathbf{F}_p^{2m}$, we define $\phi(\boldsymbol{a}) = a_1\theta + a_2\theta^p + \cdots + a_m\theta^{p^{m-1}} + b_1\theta^{p^m} + \cdots + b_m\theta^{p^{2m-1}}$, and $T(\boldsymbol{a}, \boldsymbol{a}') = c_{m+1} - c_1 \in \mathbf{F}_p$, where $\phi(\boldsymbol{a})\phi(\boldsymbol{a}')^{p^m} = c_1\theta + \cdots + c_{2m}\theta^{p^{2m-1}}$ and $c_i \in \mathbf{F}_p$. Then T is a bilinear form.

Lemma 9: T is alternating and nondegenerate.

Proof: First we show that T is alternating, that is, $T(\boldsymbol{a}, \boldsymbol{a}) = 0$ for all $\boldsymbol{a} \in \mathbf{F}_p^{2m}$. Let $x = \phi(\boldsymbol{a}) \in \mathbf{F}_{p^{2m}}$, and $xx^{p^m} = c_1\theta + \cdots + c_{2m}\theta^{p^{2m-1}}$ for $c_i \in \mathbf{F}_p$. Then $(xx^{p^m})^{p^m} = c_{m+1}\theta + c_{m+2}\theta^p + \cdots + c_{2m}\theta^{p^{m-1}} + c_1\theta^{p^m} + \cdots + c_m\theta^{p^{2m-1}}$. Since $(xx^{p^m})^{p^m} = x^{p^m}x$, $c_i = c_{i+m}$ for $i = 1, \ldots, m$. Hence $T(\boldsymbol{a}, \boldsymbol{a}) = 0$.

We assume that $x \neq 0$, which implies that $\boldsymbol{a} \neq 0$. Since $x(\theta/x^{p^m})^{p^m} = \theta^{p^m}$, $T(\boldsymbol{a}, \phi^{-1}(\theta/x^{p^m})) = 1$, which shows the nondegeneracy. □

Lemma 10: By abuse of notation, we denote by T the representation matrix of the bilinear form T with respect to the standard basis of $\mathbf{F}_p^{2m}$, that is, for $\boldsymbol{a}, \boldsymbol{b} \in \mathbf{F}_p^{2m}$, we have $T(\boldsymbol{a}, \boldsymbol{b}) = \boldsymbol{a} T \boldsymbol{b}^t$. Let I_m be the $m \times m$ unit matrix and $S = \begin{pmatrix} 0 & I_m \\ -I_m & 0 \end{pmatrix}$. There exists a nonsingular $2m \times 2m$ matrix D such that $DTD^t = S$.

Proof: See [11, Chapter XV] and use the previous lemma. □

For $\boldsymbol{c} = (c_1, \ldots, c_n) \in \mathbf{F}_{p^{2m}}^n$, let $(a_{i,1}, \ldots, a_{i,m}, b_{i,1}, \ldots, b_{i,m}) = \phi^{-1}(c_i)D^{-1} \in \mathbf{F}_p^{2m}$. We define $\Phi(\boldsymbol{c}) = (a_{1,1}, a_{1,2}, \ldots, a_{1,n}, a_{2,1}, \ldots, a_{n,m}, b_{1,1}, \ldots, b_{n,m})$. Then it is clear that the Hamming weight of $\boldsymbol{c}$ is equal to the weight (4) of $\Phi(\boldsymbol{c})$, since D is a nonsingular matrix. For $\boldsymbol{a}, \boldsymbol{b} \in \mathbf{F}_{p^{2m}}^n$ we consider the inner product

$$\langle \boldsymbol{a}, \boldsymbol{b}^{p^m} \rangle, \tag{6}$$

where $\langle , \rangle$ denotes the standard inner product in $\mathbf{F}_{p^{2m}}^n$.

Proposition 11: Let $C \subset \mathbf{F}_{p^{2m}}^n$ be a linear code over $\mathbf{F}_{p^{2m}}$, and C' the orthogonal space of C with respect to (6). Then the orthogonal space of $\Phi(C)$ with respect to (1) is $\Phi(C')$.

Proof: For $\boldsymbol{e} = (e_1, \ldots, e_n), \boldsymbol{e}' = (e'_1, \ldots, e'_n) \in \mathbf{F}_{p^{2m}}^n$, the inner product (1) of $\Phi(\boldsymbol{e}) = (a_{1,1}, \ldots, a_{n,m}, b_{1,1}, \ldots, b_{n,m})$ and $\Phi(\boldsymbol{e}') = (a'_{1,1}, \ldots, a'_{n,m}, b'_{1,1}, \ldots, b'_{n,m})$ is equal to

$$\begin{aligned}\sum_{i=1}^{n}\sum_{j=1}^{m}&(a_{i,j}b'_{i,j} - a'_{i,j}b_{i,j})\\ &= \sum_{i=1}^{n} \phi^{-1}(e_i)D^{-1}S(D^{-1})^t\phi^{-1}(e'_i)^t\\ &= \sum_{i=1}^{n} T(\phi^{-1}(e_i), \phi^{-1}(e'_i)).\end{aligned}$$

If $e_i e_i'^{p^m} = c_1\theta + \cdots + c_{2m}\theta^{p^{2m-1}}$, then $T(\phi^{-1}(e_i), \phi^{-1}(e'_i)) = c_{m+1} - c_1$. Thus if $\langle \boldsymbol{e}, \boldsymbol{e}'^{p^m}\rangle = 0$ then the inner product (1) of $\Phi(\boldsymbol{e})$ and $\Phi(\boldsymbol{e}')$ is zero, which implies $\Phi(C')$ is contained in the orthogonal space of $\Phi(C)$ with respect to (1). Comparing their dimensions as $\mathbf{F}_p$-spaces we see that they are equal. □

Theorem 12: Let $C \subset \mathbf{F}_{p^{2m}}^n$ be an $[n, (n-k)/2]$ linear code over $\mathbf{F}_{p^{2m}}$, $C^{p^m} = \{\boldsymbol{x}^{p^m} \mid \boldsymbol{x} \in C\}$, and $(C^{p^m})^\perp$ the orthogonal space of C^{p^m} with respect to the standard inner product. Suppose that $C \subseteq (C^{p^m})^\perp$, and the minimum Hamming weight of $(C^{p^m})^\perp \setminus C$ is d. Then the minimum weight (4) of $\Phi(C)$ is d, and $\Phi(C)$ is self-orthogonal with respect to the inner product (1). Any eigenspace of $\Phi(C)$ is an $[[n, k, d]]_{p^m}$ quantum code.

4.2 Error Correction for p^m-State Systems

In this subsection we consider how to determine the error from measurements with quantum codes obtained via Theorem 12. We retain notations from Theorem 12. Suppose that $\boldsymbol{g}_1, \ldots, \boldsymbol{g}_r$ is an $\mathbf{F}_{p^{2m}}$-basis of C.

Suppose that by a similar procedure to Sect. 2.2, the error is converted to a unitary matrix corresponding to $\Phi(\boldsymbol{e})$ for $\boldsymbol{e} \in \mathbf{F}_{p^{2m}}^n$. We fix a basis $\{\alpha_1, \ldots, \alpha_{2m}\}$ of $\mathbf{F}_{p^{2m}}$ over $\mathbf{F}_p$. Then $\mathbf{F}_p$-basis of $\Phi(C)$ is $\{\Phi(\alpha_j \boldsymbol{g}_i) \mid i = 1, \ldots, r, j = 1, \ldots, 2m\}$. First we shall show how to calculate $\langle \boldsymbol{e}, \boldsymbol{g}_i^{p^m}\rangle$ for each i. For $j = 1, \ldots, 2m$, let $(\boldsymbol{a}_j|\boldsymbol{b}_j) = \Phi(\alpha_j \boldsymbol{g}_i)$. As in Sect. 3.2, by the measurement outcomes we can know the inner product (1) of $\Phi(\boldsymbol{e})$ and $\Phi(\alpha_j \boldsymbol{g}_i)$, denoted by s_j, for $j = 1, \ldots, 2m$.

For $x = c_1\theta + \cdots + c_{2m}\theta^{p^{2m-1}} \in \mathbf{F}_{p^{2m}}$, $c_1, \ldots, c_{2m} \in \mathbf{F}_p$, we define $P(x) = c_{m+1} - c_1$. Then P is a nonzero $\mathbf{F}_p$-linear map. As discussed in the proof of Proposition 11, $s_j = P(\langle \boldsymbol{e}, \alpha_j^{p^m} \boldsymbol{g}_i^{p^m}\rangle) = P(\alpha_j^{p^m}\langle \boldsymbol{e}, \boldsymbol{g}_i^{p^m}\rangle)$. We define the map $P_{2m} : \mathbf{F}_{p^{2m}} \to \mathbf{F}_p^{2m}$, $x \mapsto (P(\alpha_1^{p^m} x), \ldots, P(\alpha_{2m}^{p^m} x))$. Then P_{2m} is an $\mathbf{F}_p$-linear map, and $P_{2m}(\langle \boldsymbol{e}, \boldsymbol{g}_i^{p^m}\rangle) = (s_1, \ldots, s_{2m})$. If P_{2m} is an isomorphism, then finding $\langle \boldsymbol{e}, \boldsymbol{g}_i^{p^m}\rangle$ from $(s_1, \ldots, s_{2m})$ is a trivial task, merely a matrix multiplication. We shall show that P_{2m} is an isomorphism.

Lemma 13: [11, Theorem 6.1, Chapter III] Let W be a $2m$-dimensional vector space over a field K with a basis $\{x_1, \ldots, x_{2m}\}$, and $\widehat{W}$ the dual of W, that is, the K-linear space consisting of linear maps from W to K. Then there exists a basis $\{f_1, \ldots, f_{2m}\}$ of $\widehat{W}$ such that $f_k(x_j) = \delta_{jk}$. $\{f_1, \ldots, f_{2m}\}$ is called the *dual basis.*

Lemma 14: There exist $\beta_1, \ldots, \beta_{2m} \in \mathbf{F}_{p^{2m}}$ such that $P(\alpha_j^{p^m}\beta_k) = \delta_{jk}$.

Proof: Notice that $\{\alpha_1^{p^m}, \ldots, \alpha_{2m}^{p^m}\}$ is an $\mathbf{F}_p$-basis of $\mathbf{F}_{p^{2m}}$. The dual space $\widehat{\mathbf{F}}_{p^{2m}}$ can be regarded as $\mathbf{F}_{p^{2m}}$-linear space by defining $xf : u \mapsto f(xu)$ for $x \in \mathbf{F}_{p^{2m}}$ and $f \in \widehat{\mathbf{F}}_{p^{2m}}$. Let $f_1, \ldots, f_{2m}$ be the dual basis of $\{\alpha_1^{p^m}, \ldots, \alpha_{2m}^{p^m}\}$. Since $\widehat{\mathbf{F}}_{p^{2m}}$ is one-dimensional $\mathbf{F}_{p^{2m}}$-linear space and $0 \neq P \in \widehat{\mathbf{F}}_{p^{2m}}$, f_k can be written as $\beta_k P$ for some $\beta_k \in \mathbf{F}_{p^{2m}}$. It is clear that $P(\alpha_j^{p^m}\beta_k) = \delta_{jk}$. □

Proposition 15: P_{2m} is an isomorphism.

Proof: It suffices to show that P_{2m} is surjective. For $(a_1, \ldots, a_{2m}) \in \mathbf{F}_p^{2m}$, $P_{2m}(a_1\beta_1 + \cdots + a_{2m}\beta_{2m}) = (a_1, \ldots, a_{2m})$, where β_k is as in the previous lemma. □

As in Sect. 3.2, the error $\boldsymbol{e}$ can be determined by a classical error-correcting algorithm for $(C^{p^m})^\perp$ from $\langle \boldsymbol{g}_1^{p^m}, \boldsymbol{e}\rangle, \ldots, \langle \boldsymbol{g}_r^{p^m}, \boldsymbol{e}\rangle$.

5. Notes on the Construction of Codes with Efficient Decoding Algorithms

It is desirable to have a systematic construction of quantum codes with efficient decoding algorithms. Calderbank et al. [3, Sect. V] showed a construction of cyclic linear quantum codes using the BCH bound for the minimum distance. With their construction we can correct errors up to the BCH bound using the Berlekamp-Massey algorithm.

If we use the Hartmann-Tzeng bound [7] or the restricted shift bound [14] then we get a better estimation of the minimum distance, and we can correct more errors using modified versions of the Feng-Rao decoding algorithm in [14, Theorem 6.8 and Remark 6.12]. The algorithms [14, Theorem 6.8 and Remark 6.12] correct errors up to the Hartmann-Tzeng bound or the restricted shift bound.

We cannot construct good cyclic codes of arbitrary code length. So we have to often puncture a cyclic code as in [3, Theorem 6 b)] to get a quantum code with efficient decoding algorithms. In classical error correction, we correct errors of a punctured code by applying an error-and-erasure decoding algorithm for the original code to the received word. But there is no (classical) received word in quantum error correction. So we decode a quantum punctured code as follows: Let $C' \subset \mathbf{F}_q^n$ be a (classical) linear code, $\boldsymbol{h}'_1, \ldots, \boldsymbol{h}'_r$ the rows of a check matrix for C', C the punctured code of C' obtained by discarding the first coordinate, $\boldsymbol{h}_1, \ldots, \boldsymbol{h}_{r-1}$ the rows of a check matrix for C, and $0\boldsymbol{h}_i$ the concatenation of 0 and $\boldsymbol{h}_i$ for $i = 1, \ldots, r-1$. We can express $0\boldsymbol{h}_i$ as

$$0\boldsymbol{h}_i = \sum_{j=1}^{r} a_{ij}\boldsymbol{h}'_j,$$

where $a_{ij} \in \mathbf{F}_q$ [15, Lemma 10.1]. Suppose that an error $\boldsymbol{e} = (e_2, \ldots, e_n) \in \mathbf{F}_q^{n-1}$ occurs and that we have the syndrome $s_1 = \langle \boldsymbol{h}_1, \boldsymbol{e}\rangle, \ldots, s_{r-1} = \langle \boldsymbol{h}_{r-1}, \boldsymbol{e}\rangle$. We want to find $\boldsymbol{e}$ from $s_1, \ldots, s_{r-1}$ using an error-and-erasure decoding algorithm for C'. We can find $s'_1, \ldots, s'_r \in \mathbf{F}_q$ such that

$$s_i = \sum_{j=1}^{r} a_{ij}s'_j$$

for $i = 1, \ldots, r-1$. Then there exists $\boldsymbol{e}' = (e_1, \ldots, e_n) \in \mathbf{F}_q^n$ such that

$$\langle \boldsymbol{h}'_j, \boldsymbol{e}'\rangle = s'_j \text{ for } j = 1, \ldots, r, \tag{7}$$

because the condition (7) implies that $\langle 0\boldsymbol{h}_i, \boldsymbol{e}'\rangle = s_i$ for $i = 1, \ldots, r-1$. If we apply an error-and-erasure decoding algorithm to the syndrome $s'_1, \ldots, s'_r$ with the erasure in the first coordinate, then we find $\boldsymbol{e}'$.

Note that the algorithms [14, Theorem 6.8 and Remark 6.12] are error-only decoding algorithms but we can modify them to error-and-erasure algorithms along the same line as [17, Sect. VI].

Acknowledgment

We would like to thank Prof. Hao Chen, Department of Mathematics, Zhongshan University, People's Republic of China, for providing his paper [4], without which our paper might not be in the present form. We would also like to thank Prof. Tetsuro Nishino, Department of Information and Communication Engineering, University of Electro-Communications, for teaching us quantum computing. We would also like to thank the anonymous reviewer for the critical comments that improved the presentation of our paper. We would also like to thank Dr. Shinji Miura, SONY Corporation, and Prof. Masaaki Homma, Department of Mathematics, Kanagawa University, for pointing out Remark 8.

References

[1] C.H. Bennett, D.P. DiVicenzo, J.A. Smolin, and W.K. Wootters, "Mixed-state entanglement and quantum error correction," Phys. Rev. A, vol.54, no.5, pp.3824–3851, Nov. 1996. LANL eprint† quant-ph/9604024.

[2] A.R. Calderbank, E.M. Rains, P.W. Shor, and N.J.A. Sloane, "Quantum error correction and orthogonal geometry," Phys. Rev. Lett., vol.78, no.3, pp.405–408, Jan. 1997. LANL eprint quant-ph/9605005.

[3] A.R. Calderbank, E.M. Rains, P.W. Shor, and N.J.A. Sloane, "Quantum error correction via codes over GF(4)," IEEE Trans. Inf. Theory, vol.44, no.4, pp.1369–1387, July 1998. LANL eprint quant-ph/9608006.

[4] H. Chen, "Construction of quantum error-correcting codes via algebraic-geometric codes," preprint, April 1999.

[5] A. Ekert and C. Macchiavello, "Quantum error correction for communication," Phys. Rev. Lett., vol.77, no.12, pp.2585–2588, Sept. 1996. LANL eprint quant-ph/9602022.

[6] D. Gottesman, "Class of quantum error-correcting codes saturating the quantum Hamming bound," Phys. Rev. A, vol.54, no.3, pp.1862–1868, Sept. 1996. LANL eprint quant-ph/9604038.

[7] C.R.P. Hartmann and K.K. Tzeng, "Generalizations of the BCH bound," Inf. Control, vol.20, pp.489–498, 1972.

[8] E. Knill, "Non-binary unitary error bases and quantum codes," LANL eprint quant-ph/9608048, Aug. 1996.

[9] E. Knill, "Group representations, error bases and quantum codes," LANL eprint quant-ph/9608049, Aug. 1996.

[10] E. Knill and R. Laflamme, "Theory of quantum error-correcting codes," Phys. Rev. A, vol.55, no.2, pp.900–911, Feb. 1997. LANL eprint quant-ph/9604034.

[11] S. Lang, Algebra, Third ed., Addison-Wesley, 1993.

[12] R. Matsumoto and T. Uyematsu, "Constructing quantum error-correcting codes for p^m-state systems from classical error-correcting codes," Proc. 2000 IEICE General Conf., SA-5-5, March 2000.

[13] E.M. Rains, "Nonbinary quantum codes," IEEE Trans. Inf. Theory, vol.45, no.6, pp.1827–1832, Sept. 1999. LANL eprint quant-ph/9703048.

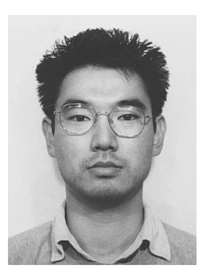
[14] R. Pellikaan, "The shift bound for cyclic, Reed-Muller and geometric Goppa codes," in Arithmetic, Geometry and Coding Theory, ed. R. Pellikaan, M. Perret, and S.G. Vlăduţ, pp.155–174, Walter de Gruyter, 1996.

[15] V.S. Pless, W.C. Huffman, and R.A. Brualdi, "An introduction to algebraic codes," in Handbook of Coding Theory, ed. V.S. Pless and W.C. Huffman, vol.1, pp.3–139, 1998.

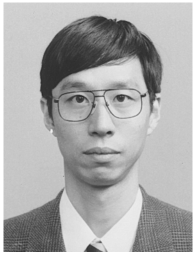
[16] J. Preskill, "Lecture Notes for Physics 229: Quantum Information and Computation," Chapter 7, available from `http://www.theory.caltech.edu/people/preskill/ph229`, Feb. 1999.

[17] B.-Z. Shen and K.K. Tzeng, "A code decomposition approach for decoding cyclic and algebraic-geometric codes," IEEE Trans. Inf. Theory, vol.41, no.6, pp.1969–1987, Nov. 1995.

†The LANL eprints can be obtained from `http://xxx.lanl.gov/`.



Ryutaroh Matsumoto was born in Nagoya, Japan, on November 29, 1973. He received the B.E. degree in computer science and M.E. degree in information processing from Tokyo Institute of Technology in 1996 and 1998 respectively. He is currently a Ph.D. student at the Department of Electrical and Electronic Engineering, Tokyo Institute of Technology. He is also a Research Fellow of the Japan Society for the Promotion of Science. E-mail: `ryutaroh@ss.titech.ac.jp`.



Tomohiko Uyematsu received the B.E., M.E. and D.E. degrees from Tokyo Institute of Technology in 1982, 1984 and 1988, respectively. From 1984 to 1992, he was with the Department of Electrical and Electronic Engineering of Tokyo Institute of Technology, first as research associate, next as lecturer, and lastly as associate professor. From 1992 to 1997, he was with School of Information Science of Japan Advanced Institute of Science and Technology as associate professor. Since 1997, he returned to the Department of Electrical and Electronic Engineering of Tokyo Institute of Technology as associate professor. In 1992, he was a visiting researcher at the Centre National de la Recherche Scientifique, France. He received Shinohara Memorial Young Engineer Award in 1989, and the Best Paper Award in 1993 and 1996, both from IEICE. His current research interests are in the areas of information theory, especially Shannon theory and multi-terminal information theory. Dr. Uyematsu is a member of IEEE.