ISSN 2186-6570

A Simple Method for Obtaining Expansions of Symplectic Codes Over an Extension Field for Quantum Error Correction

Mitsuru Hamada

Quantum ICT Research Institute, Tamagawa University
6-1-1 Tamagawa-gakuen, Machida, Tokyo 194-8610, Japan

Tamagawa University Quantum ICT Research Institute Bulletin, Vol.2, No.1, 1-4, 2012

Tamagawa University Quantum ICT Research Institute Bulletin
Vol.2 No.1 : 1-4 (2012)

A Simple Method for Obtaining Expansions of Symplectic Codes Over an Extension Field for Quantum Error Correction

Mitsuru Hamada
Quantum Information Science Research Center
Quantum ICT Research Institute
Tamagawa University
6-1-1 Tamagawa-gakuen, Machida, Tokyo 194-8610, Japan

***Abstract*—In this work, presented is a simple method for obtaining symplectic codes over a finite field $\mathbb{F}$ from symplectic codes over an extension field of $\mathbb{F}$. This task has been known to be accomplished by expanding elements of the extension field in terms of dual bases, but the proposed simpler method does not directly use dual bases. Here, symplectic codes, which resemble classical linear codes, stand for a general class of quantum error-correcting codes. This work may fall in the area of coding theory, but are directly related to quantum error correction.**

I. Introduction

Most known quantum error-correcting codes (QECCs), explicitly or implicitly, use the structure of symplectic geometry in a vector space over a finite filed [1], [2]. As a result, naturally, such quantum error-correcting codes can be represented as error-correcting codes over a finite filed, which will be called symplectic codes.

This work presents a simple method for obtaining symplectic codes over $\mathbb{F}_q$ from symplectic codes over $\mathbb{F}_{q^k}$, the extension field of $\mathbb{F}_q$. Here and throughout, $\mathbb{F}_q$ denotes the finite field consisting of q elements.

The topic treated in this work is coding-theoretic while it is motivated by issues on constructing quantum error-correcting codes [3], [4]. Note it is known how to obtain a quantum error-correcting code that corresponds to a given symplectic code [3], [2]. It may be said that a symplectic code over a finite field represents the essential structure of the corresponding quantum error-correcting codes that are expressed in terms of Hilbert spaces.

II. Preliminaries on Symplectic Codes

First, we fix some notation. The juxtaposition of vectors x and z is denoted by $(x|z)$. We write $B \le C$ if B is a subspace of C. We use the dot product defined by $(x_1, \dots, x_n) \cdot (y_1, \dots, y_n) = \sum_{i=1}^{n} x_i y_i$ on $\mathbb{F}^n$, where $\mathbb{F}$ is a finite field. While $C^{\perp}$ denotes the usual dual $\{y \in \mathbb{F}^n \mid \forall x \in C,\ x \cdot y = 0\}$ of $C \le \mathbb{F}^n$, $C^{\perp_{\mathrm{s}}}$ denotes the symplectic dual, i.e., the dual $\{y \in \mathbb{F}^{2n} \mid \forall x \in C,\ \mathsf{f}_{\mathrm{s}}(x, y) = 0\}$ with respect to the standard symplectic bilinear form f_{s} defined by

$$\mathsf{f}_{\mathrm{s}}\big((u_x|u_z), (v_x|v_z)\big) = u_x \cdot v_z - u_z \cdot v_x.$$

We let $\mathsf{span}_{\mathbb{F}} M$ denote the space spanned by the rows of a matrix M, i.e., the space consisting of vectors of the form $a_1 v_1 + \cdots + a_m v_m$, where $v_1, \dots, v_m$ are the rows of M, and $a_i \in \mathbb{F}$ for $i \in \{1, \dots, m\}$. If $\mathbb{F}$ is clear from the context, we write $\mathsf{span}\, M$ instead of $\mathsf{span}_{\mathbb{F}} M$.

From the viewpoint of coding theory [5], a symplectic QECC (additive code [1]) can be viewed as a subspace of $\mathbb{F}_q^{2n}$ that contains its symplectic dual, i.e., a subspace $\mathcal{D}$ with

$$\mathcal{D}^{\perp_{\mathrm{s}}} \le \mathcal{D}. \tag{1}$$

Such an $(n+k)$-dimensional subspace may be called an f_{s}-dual-containing code, but will be called a *symplectic code* or an $[[n, k]]$ symplectic code (over $\mathbb{F}_q$) for simplicity in this work. It will be also called a q-ary $[[n, k]]$ symplectic code.

Note a symplectic code can be rephrased as the symplectic dual of a subspace $\mathcal{C} \le \mathbb{F}_q^{2n}$ with

$$\mathcal{C} \le \mathcal{C}^{\perp_{\mathrm{s}}}, \tag{2}$$

and (2) is equivalent to

$$\forall x, y \in \mathcal{C},\ \mathsf{f}_{\mathrm{s}}(x, y) = 0.$$

A matrix $\mathcal{G}$ is called a generator matrix of a symplectic code $\mathcal{D} \le \mathbb{F}_q^{2n}$ if $\mathcal{D} = \mathsf{span}\, \mathcal{G}$; a matrix $\mathcal{H}$ is called a *check matrix* or symplectic check matrix of $\mathcal{D}$ if $\mathcal{D}^{\perp_{\mathrm{s}}} = \mathsf{span}\, \mathcal{H}$.

When we say ‘obtaining $\mathcal{D}$,’ as will be natural for coding theorists, it may be understood as obtaining a generator matrix of $\mathcal{D}$. However, it may also be understood as obtaining a check matrix, $\mathcal{H}$, of $\mathcal{D}$ since $\mathcal{D}$ is expressed as

$$\mathcal{D} = \{y \in \mathbb{F}_q^{2n} \mid \forall x \in \mathsf{span}\, \mathcal{H},\ \mathsf{f}_{\mathrm{s}}(x, y) = 0\}.$$

In fact, the check matrix $\mathcal{H}$ is more important than a generator matrix in the context of quantum error correction. For example, known encoders and decoders of the quantum error-correcting code corresponding to the symplectic code $\mathcal{D}$ can be described, in the framework of quantum theory, in terms of operators associated with the check matrix $\mathcal{H}$. Hence, we primarily pay attention to obtaining $\mathcal{H}$. (Obtaining a generator matrix of $\mathcal{D}$ from $\mathcal{H}$ is easy in case a generator matrix is needed.)

III. Expansions of Codes

It will be shown that q-ary codes can be obtained from q^k-ary codes by means of dual bases in this section. This fact seems to have been known for long in the literature [6].

It is known that a q^k-ary $[[N, K]]$ symplectic code $\mathcal{D} \leq \mathbb{F}_{q^k}^{2N}$ or its symplectic dual $\mathcal{D}^{\perp_{\rm s}}$ can be used as a q-ary $[[kN, kK]]$ symplectic code by expanding the coordinates of $(x_1, \dots, x_N,\, z_1, \cdots, z_N)$ in $\mathcal{D}$ or in $\mathcal{D}^{\perp_{\rm s}}$ to obtain

$$\begin{aligned}(&x_1^{(1)}, \dots, x_k^{(1)}, \dots, x_1^{(N)}, \dots, x_k^{(N)},\\ &\quad z_1^{(1)}, \dots, z_k^{(1)}, \dots, z_1^{(N)}, \dots, z_k^{(N)}) \in \mathbb{F}_q^{2kN}\end{aligned} \qquad (3)$$

where

$$x_i = x_1^{(i)}\beta_1 + \cdots + x_k^{(i)}\beta_k \text{ and } z_i = z_1^{(i)}\beta'_1 + \cdots + z_k^{(i)}\beta'_k$$

with some dual bases $(\beta_i)_{i=1}^k$ and $(\beta'_i)_{i=1}^k$ of $\mathbb{F}_{q^k}$, which satisfy $\mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q} \beta_i\beta'_i = \delta_{ij}$ (the Kronecker delta) by definition.[1] In particular, it is trivially true that the q-ary expansions, as in (3), of vectors in $\mathcal{D}^{\perp_{\rm s}}$ are orthogonal to each other with respect to the symplectic bilinear form $\mathrm{f_s}$.[2] Hence, those expansions form the symplectic dual of some symplectic codes over $\mathbb{F}_q$, which is, in fact, the q-ary expansion of $\mathcal{D}$. Here, when obtaining a q-ary $[[kN, kK]]$ symplectic code $\widetilde{\mathcal{D}}$ from a q^k-ary $[[N, K]]$ symplectic code $\mathcal{D}$ in this way, we call $\widetilde{\mathcal{D}}$ a q-ary expansion of $\mathcal{D}$.

IV. Main Result

A. Homomorphism of Extension Field Into Space of Matrices

We use the following known lemma.

Lemma 1: There exists a one-to-one map $\Phi : \mathbb{F}_{q^k} \to \mathbb{F}_q^{k\times k}$ (the set of $k \times k$ matrices over $\mathbb{F}_q$) with the following property:

$$\Phi(\xi)\Phi(\xi') = \Phi(\xi\xi'),\ \ \Phi(\xi) + \Phi(\xi') = \Phi(\xi + \xi')$$

for any $\xi, \xi' \in \mathbb{F}_{q^k}$.

Note that the map Φ is called a homomorphism by definition.

We can construct such a map concretely as follows.

Construction of Φ. Take a root α of a monic primitive polynomial f of degree k over $\mathbb{F}_q$.[3] We set $\Phi(\alpha^i) = T^i$ for $i = 0, \dots, q^k - 2$, where T is the companion matrix of f, and put $\Phi(0) = O_k$, where O_k denotes the $k \times k$ zero matrix.

Here, the companion matrix of a monic polynomial f is defined as follows. Let us write $f(x)$ as $f(x) = x^k - f_{k-1}x^{k-1} - \cdots - f_1 x - f_0$. The companion matrix of f is

$$T = \begin{bmatrix} 0_{k-1} & f_0 \\ & f_1 \\ I_{k-1} & \vdots \\ & f_{k-1} \end{bmatrix} \qquad (4)$$

where 0_{k-1} is the zero vector in $\mathbb{F}_q^{k-1}$, and I_{k-1} is the $(k-1) \times (k-1)$ identity matrix.

Example. Let $q = 2$ and $k = 3$. The companion matrix of a primitive polynomial $f(x) = x^3 + x + 1$ is

$$T = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}.$$

A proof that the above constructed map Φ has the property in the lemma can be found in [3]. In [3], one can also find the following useful fact with a proof. Noticing $(\alpha^{j-1})_{j=1}^k$ is a basis of the $\mathbb{F}_q$-linear vector space $\mathbb{F}_{q^k}$, let us write α^i as

$$\alpha^i = x_1 + x_2\alpha + \cdots + x_k\alpha^{k-1}.$$

The vector $(x_1, \dots, x_k)^{\rm T}$ obtained in this way is denoted by

$$\begin{matrix} | \\ \alpha^i. \\ | \end{matrix}$$

Namely,

$$\begin{matrix} | \\ \alpha^i \\ | \end{matrix} = \begin{bmatrix} x_1 \\ \vdots \\ x_k \end{bmatrix}.$$

Then, we have

$$T^i = \begin{bmatrix} | & & | \\ \alpha^i & \cdots & \alpha^{i+k-1} \\ | & & | \end{bmatrix}, \quad 0 \leq i \leq q^k - 2. \qquad (5)$$

B. Main Result

In this section, we present a simple method for obtaining a check matrix of a q-ary expansion of an arbitrary q^k-ary symplectic code $\mathcal{D}$ from a check matrix of $\mathcal{D}$.

Note that given an $m \times 2n$ matrix $\mathcal{H} = [H_x H_z]$ consisting of a pair of $m\times n$ matrices H_x and H_z over $\mathbb{F}_q$, the rows of $\mathcal{H}$ are orthogonal to each other with respect to the symplectic form $\mathrm{f_s}$ if and only if

$$H_x {H_z}^{\rm T} - H_z {H_x}^{\rm T} = O_m. \qquad (6)$$

Hence, (6) is a condition that $\mathcal{H}$ is a check matrix of some symplectic code.

Theorem 1: Let Φ be a one-to-one map having the property in Lemma 1, i.e., a homomorphism. Assume

[1] A widely known definition of the operation 'trace' $\mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}$ would be as follows: $\mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q} \gamma = \gamma + \gamma^q + \cdots + \gamma^{q^{k-1}}$.

[2] Of course, 'x is orthogonal to y with respect to $\mathrm{f_s}$' means $\mathrm{f_s}(x, y) = 0$.

[3] A monic polynomial is a polynomial the leading coefficient of which is one.

$\mu \times 2N$ matrix $\mathcal{H} = [H_x H_z]$ consisting of $\mu \times N$ matrices

$$H_x = \begin{bmatrix} h_{11} & \cdots & h_{1N} \\ \vdots & & \vdots \\ h_{\mu 1} & \cdots & h_{\mu N} \end{bmatrix}$$

and

$$H_z = \begin{bmatrix} h'_{11} & \cdots & h'_{1N} \\ \vdots & & \vdots \\ h'_{\mu 1} & \cdots & h'_{\mu N} \end{bmatrix}$$

satisfies

$$H_x {H_z}^{\mathrm{T}} - H_z {H_x}^{\mathrm{T}} = O_\mu .$$

Then, $k\mu \times 2kN$ matrix $\widetilde{\mathcal{H}} = [\widetilde{H}_x \widetilde{H}_z]$ consisting of

$$\widetilde{H}_x = \begin{bmatrix} \Phi(h_{11}) & \cdots & \Phi(h_{1N}) \\ \vdots & & \vdots \\ \Phi(h_{\mu 1}) & \cdots & \Phi(h_{\mu N}) \end{bmatrix}$$

and

$$\widetilde{H}_z = \begin{bmatrix} \Phi(h'_{11})^{\mathrm{T}} & \cdots & \Phi(h'_{1N})^{\mathrm{T}} \\ \vdots & & \vdots \\ \Phi(h'_{\mu 1})^{\mathrm{T}} & \cdots & \Phi(h'_{\mu N})^{\mathrm{T}} \end{bmatrix}$$

satisfies

$$\widetilde{H}_x {\widetilde{H}_z}^{\mathrm{T}} - \widetilde{H}_z {\widetilde{H}_x}^{\mathrm{T}} = O_{\widetilde{\mu}} .$$

where $\widetilde{\mu} = k\mu$.

Proof. The statement immediately follows from the fact that the map Φ is a homomorphism. □

Remark. One construction of the map Φ was given just below Lemma 1. Given a map Φ of the property in the lemma, the map $\Phi' : \xi \mapsto \Lambda^{-1}\Phi(\xi)\Lambda$, where Λ is an invertible matrix, also has the desirable property of being a homomorphism. □

By this theorem, we have obtained a method for producing a desirable check matrix $\widetilde{\mathcal{H}}$ from the original check matrix $\mathcal{H} = [H_x H_z]$. The method is simply replacing the entries of H_x with their images under Φ and replacing the entries of H_z with the transposes of their images under Φ.

V. Discussions

A. Advantage

As already mentioned in Section III, it has been known that we can obtain q-ary expansions of symplectic codes from q^k-ary symplectic codes using dual bases.

An advantage of this work's method would be that we need not explicitly obtain such a pair of dual bases.

B. Relation to Concatenations of Calderbank-Shor-Steane Codes

A symplectic code with check matrix of the form

$$\mathcal{H} = \left[\begin{array}{cc} H_2 & O \\ O & H_1 \end{array} \right], \tag{7}$$

where O is the matrix whose entries are all zero, is called a Calderbank-Shor-Steane (CSS) code.[4]

This is consistent with saying [5] that the CSS code construction [7], [8] is to take classical codes C_1 and C_2 with $C_1^{\perp} \leq C_2$, and form

$$\mathcal{G} = \left[\begin{array}{cc} G_1 & O \\ O & G_2 \end{array} \right], \quad \mathcal{H} = \left[\begin{array}{cc} H_2 & O \\ O & H_1 \end{array} \right] \tag{8}$$

where G_i and H_i are the classical generator and parity check matrices of C_i. Following this, in [3], we have called a pair of linear codes (C_1, C_2), where $C_1, C_2 \leq \mathbb{F}_q^n$, satisfying the constraint

$$C_2^{\perp} \leq C_1 \tag{9}$$

and

$$k = \dim_{\mathbb{F}_q} C_1 + \dim_{\mathbb{F}_q} C_2 - n \tag{10}$$

an $[[n,k]]$ *code pair* over $\mathbb{F}_q$. Since an $[[n,k]]$ code pair, also referred to as a CSS code pair, is a succinct representation of the corresponding CSS code, the pair sometimes means the corresponding CSS code, and vice versa in what follows.

In [3], we have applied the present work's approach to the problem of obtaining check matrices of check matrices of 'concatenations' of CSS codes.[5] We remark that q-ary expansions of q^k-ary CSS codes can be viewed as an extreme case of the 'concatenations' of CSS codes. Specifically, 'Procedure for Creating $G'_{j,i}$' (consisting of Step 1 and Step 2) in [3, p. 2693, right column] is the method for obtaining check matrices. For the purpose of obtaining q-ary expansions of q^k-ary CSS codes, not the general 'concatenations,' in Step 2 thereof, we can set $(g_m{}^{2)})$ equal to the standard basis of $\mathbb{F}_q^k$ since the q-ary expansion of a q^k-ary CSS code pair (D_1, D_2) is the 'concatenation' of $(\mathbb{F}_q^k, \mathbb{F}_q^k)$ and (D_1, D_2).

C. The Term q-ary Expansion

In Section III, the author has written that when obtaining a q-ary $[[kN, kK]]$ symplectic code $\widetilde{\mathcal{D}}$ from a q^k-ary $[[N, K]]$ symplectic code $\mathcal{D}$ in the manner described there (using dual basis), we call $\widetilde{\mathcal{D}}$ a q-ary expansion of $\mathcal{D}$. The fact that codes obtained with this work's method using the explicitly constructed homomorphisms $\Phi(\xi)$ and $\Lambda^{-1}\Phi(\xi)\Lambda$ are, in fact, such q-ary expansions, has been checked with developments in [3]. (For CSS codes,

[4] For consistency, CSS codes mean the indicated class of symplectic codes, which are subspaces of discrete vector spaces. Of course, a CSS code represents a quantum error-correcting code, which is a subspace of a Hilbert space, as an arbitrary symplectic code does.

[5] The usage of the term 'concatenation' in [3] is different from the original usage of Forney.

this fact is known [3].) The main theorem does not rely on this fact.

VI. Conclusion

We have presented a simple method for obtaining a check matrix of a q-ary expansion of an arbitrary q^k-ary symplectic code $\mathcal{D}$ from a check matrix of $\mathcal{D}$.

References

[1] 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, no. 4, pp. 1369–1387, Jul. 1998.

[2] M. Hamada, "Information rates achievable with algebraic codes on quantum discrete memoryless channels," *IEEE Trans. Information Theory*, vol. 51, no. 12, pp. 4263–4277, Dec. 2005.

[3] ——, "Concatenated quantum codes constructible in polynomial time: Efficient decoding and error correction," *IEEE Trans. Information Theory*, vol. 54, no. 12, pp. 5689–5704, Dec. 2008.

[4] ——, "A polynomial-time construction of self-orthogonal codes and applications to quantum error correction," *Proc. IEEE International Symposium on Information Theory (ISIT)*, pp. 794–798, 2009.

[5] A. M. Steane, "Enlargement of Calderbank-Shor-Steane quantum codes," *IEEE Trans. Information Theory*, vol. 45, pp. 2492–2495, Nov. 1999.

[6] A. Ashikhmin and E. Knill, "Nonbinary quantum stabilizer codes," *IEEE Trans. Information Theory*, vol. 47, no. 5, pp. 3065–3072, Nov. 2001.

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

[8] A. M. Steane, "Multiple particle interference and quantum error correction," *Proc. Roy. Soc. Lond. A*, vol. 452, pp. 2551–2577, 1996.

This work was supported by JSPS KAKENHI Grant Numbers 22540150 and 21244007.