Application of Classical Codes over GF(4) on Quantum Error Correction Codes

Duc Manh Nguyen and Sunghwan Kim(✉)

CIT Lab, University of Ulsan, Ulsan 44610, South Korea
nguyenmanhduc18@gmail.com, sungkim@ulsan.ac.kr

Abstract. This research studies the construction of classical linear code over Galois field 4. This classical code is self-orthogonal with Hermitian product. In addition, quantum stabilizer codes are investigated from the classical codes. Finally, quantum stabilizer codes, which are able to correct one error and detect two errors in quantum information channel, have been explained in detail to show the practicality of this construction.

Keywords: Quantum information · Quantum stabilizer codes · Galois field 4

1 Introduction

Quantum processing devices have proved to have the possibility for difficult tasks in factorizing in RSA algorithm, in searching from unordered sets, and in security of cryptography problem [1]. The algorithms based on quantum computing devices have a better efficiency than the best algorithm in classical computing devices [2]. Since the quantum noise and imperfect quantum operations have affected the performance of quantum algorithm, we use the quantum error correction code (QECC) to remove or detect the quantum noise in quantum channel. The invention of Shor code for nine qubits [3] and Calderbank–Shor–Steane code for seven qubits (a perfect CSS code) [4] showed the way quantum information could be extended by using the redundancy qubit for encoding in quantum systems. Quantum stabilizer codes are proposed by Gottesman [5]. The codes are proved to be the most important method of QECC and they are very useful for the construction of encoding and decoding circuits for quantum computation [6]. In addition, a quantum stabilizer code can be specified by classical binary code where its parity-check matrix respects to the symplectic inner product (SIP) [7]. As a consequence, a lot of quantum stabilizer codes are proposed and their construction is from linear binary codes [8]. It also turns out that the classical error correction codes can be given by the elements of Galois field. So we consider the idea of Calderbank et al. [9] about the relationship between the classical codes,

S. C. Satapathy et al. (Eds.): FICTA 2018, AISC 1013, pp. 116–122, 2020.
https://doi.org/10.1007/978-981-32-9186-7_13

which are self-orthogonal with Hermitian product and the quantum stabilizer codes.

This research aims to design new classical codes over Galois field 4 which are self-orthogonal code with Hermitian product. The quantum stabilizer codes are considered afterward where their lengths are ranging from five to ten. The paper begins with the review of the quantum mechanic and the role of quantum error correction code. After that, the construction of classical self-orthogonal code with Hermitian product is proposed. Then, we show the result of quantum stabilizer codes which is transformed from classical GF(4) codes. Finally, we present the conclusion.

2 Quantum Error Correction Codes

2.1 Quantum Mechanism

Bit or binary digit is the basic unit of information used in classical computing and digital communication. The basic unit of quantum information is the quantum bit (*qubit*). But if *bit* has two basic states of 0 or 1, the qubit applied the superposition principle of two basic states. It is necessary to use the mathematical model of quantum information. For this purpose, we use the two-dimensional Hilbert space (H) of complex number. The basic state is indicated as

$$|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \ |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \tag{1}$$

the superposition state is denoted as

$$|\psi\rangle = \begin{bmatrix} a \\ b \end{bmatrix} = a\,|0\rangle + b\,|1\rangle\,, \tag{2}$$

whereas the norm condition for basic state complex numbers a, b satisfy $|a|^2 + |b|^2 = 1$. As a consequence, the information which are represented in quantum state are unlimited. Generally, the quantum registers are n qubits physical system and the n times tensor product of two-dimensional Hilbert space.

Quantum system requires the unitary transformations on quantum states. Each transformation operator is a combination of the Pauli matrices:

$$\mathbf{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \ \mathbf{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \ \mathbf{Z} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \ \mathbf{Y} = \mathbf{XZ}. \tag{3}$$

Pauli matrices includes $\mathbf{X}$ (bit flip), $\mathbf{Z}$ (phase flip), and $\mathbf{Y}$ (the combination of bit and phase flips). The Pauli group P_1 for one qubit is closed under multiplication, which are formed by $\mathbf{X}$, $\mathbf{Z}$ and $\mathbf{Y}$. We have, $P_1 = \{\mathbf{I}, \mathbf{X}, \mathbf{Y}, \mathbf{Z}\}$. Generally, in the n-qubit Pauli group, P_n is the n times tensor product of Pauli group P_1. P_n has the most important property: any two vectors in P_n are either commutative or anti-commutative.

Let $H^{\otimes n}$ be a state space of n qubits. Quantum stabilizer group S is an Abelian subgroup of P_n, it is closed under multiplication and there is no trivial subspace, C_S of $H^{\otimes n}$ which is fixed (or stabilized) by S. The stabilized C_S defines a codeword such that

$$C_S = \{\ |\psi\rangle \in H^{\otimes n} :\ \ \mathbf{g}|\psi\rangle = |\psi\rangle,\ \ \forall \mathbf{g} \in S\}. \tag{4}$$

If group S has its generators: $g = \{\mathbf{g}_1, \mathbf{g}_2, .., \mathbf{g}_{m=n-k}\}$, the C_S is code space or the codeword for a quantum stabilizer code with parameters $[[n, k, d_{min}]]$. $[[n, k, d_{min}]]$ encodes k qubits into n qubits and it can correct $\lfloor \frac{d_{min}-1}{2} \rfloor$ errors. Then, there is the constraint for the generators of g where two elements have to be commutative to each other. Let $nor(S)$ be the normalizer of S in P_n,

$$nor(S) = \{\mathbf{A} \in P_n \ \mid\ \mathbf{A}^\dagger \mathbf{E} \mathbf{A} \in S,\ \forall \mathbf{E} \in S\}. \tag{5}$$

$nor(S)$ is all operators from P_n which are commutative with S. Hence, minimum distance parameter of quantum stabilizer code is calculated as

$$d_{min} = min\{wei(\mathbf{E})\},\ s.t\ \ \mathbf{E} \in nor(S) \setminus S, \tag{6}$$

where $wei(\mathbf{E})$ is the number of positions not equal to $\mathbf{I}$ in vector $\mathbf{E}$.

We can express the generator of quantum stabilizer code as the binary field due to any n-qubit Pauli operator can be expressed as multiplication of $\mathbf{X}$-containing operator and a $\mathbf{Z}$-containing operator. We define the mapping as $\mathbf{I} \leftrightarrow (0, 0)$, $\mathbf{X} \leftrightarrow (1, 0)$, $\mathbf{Z} \leftrightarrow (0, 1)$, and $\mathbf{Y} \leftrightarrow (1, 1)$. As a consequence, the m generators of an $[[n, k]]$ is formed in binary field as $\mathbf{H} = [\mathbf{H_X}|\mathbf{H_Z}]$ where $\mathbf{H_X}, \mathbf{H_Z}$ are $(n-k) \times n$ binary matrices. The commutative constraint between generators must change to the symplectic product constraint as

$$\mathbf{H_Z} \times \mathbf{H_X}^T \ +\ \mathbf{H_X} \times \mathbf{H_Z}^T \ =\ \mathbf{0}_{n-k}.$$

0_m is the matrix of all zero elements with size $m \times m$. We can uniquely transform the parity-check matrix $\mathbf{H}$ into standard form using Gaussian elimination as

$$\begin{bmatrix} \overbrace{\mathbf{I}}^{l} & \overbrace{\mathbf{A}}^{n-k-l} & \overbrace{\mathbf{B}}^{k} & \overbrace{\mathbf{C}_1}^{l} & \overbrace{\mathbf{D}}^{n-k-l} & \overbrace{\mathbf{C}_2}^{k} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{F}_1 & \mathbf{I} & \mathbf{F}_2 \end{bmatrix} \begin{matrix} \} & l \\ \} & n-k-l. \end{matrix}$$

2.2 Classical Codes over GF(4)

Quantum stabilizer codes are considered as classical code over the Galois field by mapping the four Pauli operators with four elements of Galois field. We define Galois field 4 as set of four elements $\{0,\ 1,\ \omega,\ \omega^2 = \omega + 1\}$. The mapping between Pauli operators, binary form, and GF(4) elements are given in Table 1. We define the products for GF(4) as

- The conjugation of element in GF(4): $\overline{u}\ :=\ u^2$.
- The trace function of element in GF(4): $tr(u)\ :=\ u + \overline{u}$.

– The trace product of two elements $\mathbf{x}$ and $\mathbf{y}$ in Galois field: $\mathbf{x} * \mathbf{y} := \sum_i tr(\mathbf{x}_i\overline{\mathbf{y}_i})$.
– The Hermitian product "." of two elements $\mathbf{x}$ and $\mathbf{y}$ in Galois field: $\mathbf{x}.\mathbf{y} := \sum_i \mathbf{x}_i\overline{\mathbf{y}_i}$.

We have the trivial equations, $tr(0) = tr(1) = 0$, $tr(\omega) = tr(\omega^2) = 1$, $\overline{0} = 0$, $\overline{1} = 1$, and $\overline{\omega} = \omega^2$. As a consequence, the relationship has been shown in Table 1. Addition of two vectors in GF(4) maps to multiplication of two corresponding Pauli operators. For one-qubit case, two operators are commutative if and only if one of them is $\mathbf{I}$ or if they are equal to each other. Since $tr(0) = 0$, for $u \neq 0, u^3 = 1$, and $tr(u^3) = tr(1) = 0$, the trace product of two operators is always 0. Otherwise, the trace product of single Pauli operators is 1. Generally, for n qubits case, Pauli operators which arise from vector $\mathbf{u}$, $\mathbf{v}$ are commutative when the trace product is zero (the component-wise n time is even or $\mathbf{u} * \mathbf{v} = \sum tr(\mathbf{u}_i\overline{\mathbf{v}_i}) = 0$).

We sum up the relationship between quantum stabilizer code and classical code over GF(4) as shown in the following study:

Theory 1. C is a classical code $[n, k]$ with elements in Galois field 4, Hermitian self-orthogonal and no codewords has weight $< d$ in $C^{\perp}\backslash C$ ($C^{\perp}$ denotes the dual code with Hermitian product of C). So, the corresponding $[[n, n-2k, d]]$ exists.

From Theory 1, we can have the quantum stabilizer code from classical code over GF(4). They must be additive code over GF(4) and two following conditions must be satisfied, (let $\mathbf{x}_1$, $\mathbf{x}_2$ be two generators):

1. They are orthogonal to each other: $\mathbf{x}_i.\overline{\mathbf{x}_j} = 0$ for any i, j from $\{1, 2\}$.
2. They are orthogonal itself: number of difference 0 elements of $\mathbf{x}_1$, $\mathbf{x}_2$ are even.

Table 1. Galois field elements, Pauli operators, and binary mapping table

Single Pauli matrices	Galois field	Binary
$\mathbf{I}$	0	(0,0)
$\mathbf{X}$	1	(1,0)
$\mathbf{Y}$	ω^2	(1,1)
$\mathbf{Z}$	ω	(0,1)

3 Proposed Construction

3.1 Construction of Generator Matrix

We assume that $\mathbf{G}$ is the matrix with elements from Galois field 4 as $\mathbf{G} = [\mathbf{I}_m|\mathbf{G}^0]$ and the size $m \times l$. We construct two new matrices $\mathbf{G}^1$ and $\mathbf{G}^2$ with size $(m+1) \times (l+2)$ and $(m+2) \times (l+2)$, respectively, as

$$\mathbf{G}^1 = \begin{bmatrix} \mathbf{A}\ \mathbf{X}^1 \\ \mathbf{Y}\ \mathbf{G}^0 \end{bmatrix}, \mathbf{G}^2 = \begin{bmatrix} \mathbf{I}_2\ \mathbf{X}^2 \\ \mathbf{Y}\ \mathbf{G}^0 \end{bmatrix}, \tag{7}$$

where $\mathbf{I}_m = \begin{bmatrix} 1\ 0\ \ldots\ 0 \\ 0\ 1\ \ldots\ 0 \\ \vdots\ \vdots\ \ddots\ \vdots \\ 0\ 0\ \ldots\ 1 \end{bmatrix}, \mathbf{G}^0 = \begin{bmatrix} \mathbf{g}_1 \\ \mathbf{g}_2 \\ \vdots \\ \mathbf{g}_m \end{bmatrix}, \mathbf{A} = [0\ \ 1]$, $\mathbf{X}^1 = [x_1\ \ x_2\ \ \ldots\ \ x_n]$ is the vector over GF(4) with a number of positions which are different to 0 are even, $\mathbf{X}^2 = \begin{bmatrix} \mathbf{X}^1 \\ \mathbf{X}^1 \end{bmatrix}$, $\mathbf{Y} = \begin{bmatrix} y_1\ \ y_1 \\ y_2\ \ y_2 \\ \cdots \\ y_m\ \ y_m \end{bmatrix}$ where $\overline{y_i} := \mathbf{X}^1.\mathbf{g}_i$.

Hence, $\mathbf{G}$ is the generator matrix of classical code over Galois field and a self-orthogonal code with Hermitian product. And $\mathbf{G}^1$ and $\mathbf{G}^2$ can be used as $\mathbf{G}^0$ in the generators matrix $\mathbf{G}$ of a new classical code over Galois field with Hermitian self-orthogonal.

Proof. Since vector $[x_1\ \ x_2\ \ \ldots\ \ x_n]$ has even weight, and $\mathbf{g}_i$ (i is from 1 to m) have odd weight, the weight of each vector in $\mathbf{G}^1$ and $\mathbf{G}^2$ is odd. So, they are orthogonal itself. In addition, as the pre-definition of y_i:

$$\overline{y_i} := [x_1\ \ x_2\ \ \ldots\ \ x_n].\mathbf{g}_i \tag{8}$$

$$\Rightarrow 1\overline{y_i} + [x_1\ \ x_2\ \ \ldots\ \ x_n].\mathbf{g}_i = 1\overline{y_i} + 1\overline{y_i} = 0. \tag{9}$$

So, they are orthogonal to each other.

We have proved that $\mathbf{G}^1$ and $\mathbf{G}^2$ satisfy two constraints, they can be used for construction of the generator matrix $\mathbf{G}$ with elements in Galois field which is self-orthogonal with Hermitian product.

3.2 Optimal Quantum Error Correction Codes

We consider the construction of classical code over GF(4) with respect to Hermitian self-orthogonal product and the corresponding results of quantum stabilizer codes whose code lengths are ranging from five to ten.

Example 1. The shortest length for QECC is five with $[[5, 1, 3]]$ code. As the equation in Eq. 7, we need to find matrix $\mathbf{G}^0$ with two vectors which are having length 3. Since all elements of $\mathbf{G}^0$ are from Galois field, it is easy to get a vector length 3 for $\mathbf{G}^0$ as

$$\mathbf{G}^0 = \begin{bmatrix} 1\ \ \omega\ \omega^2 \\ \omega^2\ \omega\ \ 1 \end{bmatrix}. \tag{10}$$

From generator matrix $\mathbf{G} = [\mathbf{I}|\mathbf{G}^0]$, we have Hermitian self-orthogonal code $[5, 2, 4]$ and corresponding quantum stabilizer code in standard form as

$$\begin{cases} \mathbf{g}_1 = [1000011110] \\ \mathbf{g}_2 = [0100011011] \\ \mathbf{g}_3 = [0010111101] \\ \mathbf{g}_4 = [0001110110] \end{cases}. \tag{11}$$

They are generators in binary form for $[[5, 1, 3]]$.

Example 2. The optimal quantum stabilizer code length 7 is $[[7, 1, 3]]$. $[[7, 1, 3]]$ is first constructed based on Calderbank, Shor, and Steane construction in [5]. In this paper, we consider the classical code with $\mathbf{G}^0$ as

$$\mathbf{G}^0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}. \tag{12}$$

We get $\mathbf{G}^1$ from $\mathbf{G}^0$ as

$$\mathbf{G}^1 = \begin{bmatrix} 1 & 0 & \omega^2 & \omega^2 \\ \omega & \omega & 1 & 0 \\ \omega & \omega & 0 & 1 \end{bmatrix}. \tag{13}$$

Then, the generator matrix $\mathbf{G} = [\mathbf{I}|\mathbf{G}^1]$ corresponds to $[7, 3, 4]$. The standard form for generator matrix of $[[7, 1, 3]]$ is

$$\begin{cases} \mathbf{g}_1 = [10001001010110] \\ \mathbf{g}_2 = [01000011000100] \\ \mathbf{g}_3 = [00100010001100] \\ \mathbf{g}_4 = [00011000011101] \\ \mathbf{g}_5 = [00000111001000] \\ \mathbf{g}_6 = [00000000110011] \end{cases}. \tag{14}$$

Example 3. The optimal QECC length 9 is $[[9, 1, 3]]$ as reported as Shor code in [4]. In this paper, we consider the Hermitian self-orthogonal code with $\mathbf{G}^0$

$$\mathbf{G}^0 = \begin{bmatrix} 1 & \omega & \omega \\ \omega & 1 & \omega \\ \omega & \omega & 1 \end{bmatrix}. \tag{15}$$

We get $\mathbf{G}^1$ from $\mathbf{G}^0$ as

$$\mathbf{G}^1 = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & \omega & \omega \\ \omega^2 & \omega^2 & \omega & 1 & \omega \\ \omega^2 & \omega^2 & \omega & \omega & 1 \end{bmatrix}. \tag{16}$$

Then, the generator matrix $\mathbf{G} = [\mathbf{I}|\mathbf{G}^1]$ corresponds to classical code $[9, 4, 4]$. The standard form of generator matrix for $[[9, 1, 3]]$ is

$$\begin{cases} \mathbf{g}_1 = [100001101000100111] \\ \mathbf{g}_2 = [010000100000000011] \\ \mathbf{g}_3 = [001000100000111010] \\ \mathbf{g}_4 = [000100100001011001] \\ \mathbf{g}_5 = [000011101001000111] \\ \mathbf{g}_6 = [000000011001100000] \\ \mathbf{g}_7 = [000000000100010011] \\ \mathbf{g}_8 = [000000000011100111] \end{cases}. \tag{17}$$

4 Conclusion

This paper has proposed the design method for classical codes in Galois field, and they are self-orthogonal with Hermitian product. In addition, the investigation of quantum stabilizer codes from the classical codes is also mentioned. The optimal QECC with the length ranging from five to ten and minimum distance three is given to show the practicality of the proposed construction.

Acknowledgements. This work was supported by the Research Program through the National Research Foundation of Korea (NRF-2016R1D1A1B03934653, NRF-2019R1A2C1005920).

References

1. Nguyen, D.M., Kim, S.: Quantum key distribution protocol based on modified generalization of Deutsch-Jozsa Algorithm in d-level quantum system. Int. J. Theor. Phys (2017). https://doi.org/10.1007/s10773-018-3910-4
2. Grover, L.: Quantum mechanics helps in searching for a needle in a haystack. Phys. Rev. Lett. **79**, 325 (1997)
3. Shor, P.W.: Scheme for reducing decoherence in quantum computer memory. Phys. Rev. A. **52**, 2493 (1995)
4. Calderbank, A.R., Shor, P.W.: Good quantum error-correcting codes exist. Phys. Rev. A. **54**, 1098–1106 (1996)
5. Gottesman, D.: California Institute of Technology, Ph.D. thesis (1997)
6. Penrose, R.: Quantum Error Correction and Fault Tolerant Quantum Computing. CRC Press Inc., Boca Raton (2007)
7. Nguyen, D.M., Kim, S.: Minimal-entanglement entanglement-assisted quantum error correction codes from modified circulant matrices. Symmetry **9**(7), 122 (2017)
8. Nguyen, D.M., Kim, S.: Construction and complement circuit of a quantum stabilizer code with length 7. In: Proceedings of Eighth International Conference on Ubiquitous and Future Networks (2016)
9. Calderbank, A.R., Rains, E.M., Shor, P.W., Sloane, N.J.A.: Quantum error correction via codes over GF(4). IEEE Trans. Inform. Theory **44**, 1369–1387 (1998)