New Quantum Error-Correcting Codes from Hermitian Self-Orthogonal Codes over GF(4)

Jon-Lark Kim

Department of Mathematics, Statistics, and Computer Science,
322 SEO(M/C 249),
University of Illinois–Chicago,
851 S. Morgan, Chicago, IL 60607-7045, USA

Abstract. In order to construct good quantum-error-correcting codes, we construct good Hermitian self-orthogonal linear codes over GF(4). In this paper we construct record-breaking pure quantum-error-correcting codes of length 24 with 2 encoded qubits and minimum weight 7 from Hermitian self-orthogonal codes of length 24 with dimension 11 over GF(4). This shows that length $n = 24$ is the smallest length for any known $[[n, k, d]]$ quantum-error-correcting code with $k \geq 2$ and $d = 7$. We also give a construction method to produce Hermitian self-orthogonal linear codes GF(4) from a shorter length such code.

1 Introduction

It was shown [4] in 1995 that there could exist quantum-error-correcting codes (QECC throughout the paper) which would protect quantum information as classical error-correcting codes protect classical information. See [1] for the brief history of QECC. It is also known [1] that the problem of finding QECC is transformed into the problem of finding additive self-orthogonal codes under a certain inner product over the finite field GF(4). These additive self-orthogonal codes include the classical Hermitian self-orthogonal codes over GF(4). So our purpose is to construct good Hermitian self-orthogonal codes in order to construct good QECC using the ideas of [3].

We recall some basic definitions from [1,2]. Let $\mathrm{GF}(4) = \{0, 1, \omega, \overline{\omega}\}$ with the convention that $2 = \omega$ and $3 = \overline{\omega}$ where $\overline{\omega} = \omega^2 = 1 + \omega$. An *additive code* $\mathcal{C}$ *over* GF(4) *of length* n is an additive subgroup of $\mathrm{GF}(4)^n$. As $\mathcal{C}$ is a free GF(2)-module, it has size 2^k for some $0 \leq k \leq 2n$. We call $\mathcal{C}$ an $(n, 2^k)$ code. It has a basis, as a GF(2)-module, consisting of k basis vectors; a *generator matrix* of $\mathcal{C}$ will be a $k \times n$ matrix with entries in GF(4) whose rows are a basis of $\mathcal{C}$. The *weight* $\mathrm{wt}(\mathbf{c})$ of $\mathbf{c} \in \mathcal{C}$ is the number of nonzero components of $\mathbf{c}$. The minimum weight d of $\mathcal{C}$ is the smallest weight of any nonzero codeword in $\mathcal{C}$. If $\mathcal{C}$ is an $(n, 2^k)$ additive code of minimum weight d, $\mathcal{C}$ is called an $(n, 2^k, d)$ code.

To study QECC, we consider a somewhat different inner product from the ordinary inner product. We start with the following trace map. The *trace*

map $\mathrm{Tr} : \mathrm{GF}(4) \to \mathrm{GF}(2)$ is given by

$$\mathrm{Tr}(x) = x + x^2.$$

In particular $\mathrm{Tr}(0) = \mathrm{Tr}(1) = 0$ and $\mathrm{Tr}(\omega) = \mathrm{Tr}(\overline{\omega}) = 1$. The *conjugate* of $x \in \mathrm{GF}(4)$, denoted $\overline{x}$, is the image of x under the Frobenius automorphism; in other words, $\overline{0} = 0$ $\overline{1} = 1$, and $\overline{\overline{\omega}} = \omega$. We now define the *trace inner product* of two vectors $\mathbf{x} = x_1 x_2 \cdots x_n$ and $\mathbf{y} = y_1 y_2 \cdots y_n$ in $\mathrm{GF}(4)^{\mathrm{n}}$ to be

$$\mathbf{x} \star \mathbf{y} = \sum_{i=1}^{n} \mathrm{Tr}(x_i \overline{y_i}) \in \mathrm{GF}(4). \tag{1}$$

If $\mathcal{C}$ is an additive code, its *dual*, denoted $\mathcal{C}^{\perp}$, is the additive code $\{\mathbf{x} \in \mathrm{GF}(4)^{\mathrm{n}} \mid \mathbf{x} \star \mathbf{c} = 0 \text{ for all } \mathbf{c} \in \mathcal{C}\}$. If $\mathcal{C}$ is an $(n, 2^k)$ code, then $\mathcal{C}^{\perp}$ is an $(n, 2^{2n-k})$ code. As usual, $\mathcal{C}$ is *trace self-orthogonal* if $\mathcal{C} \subseteq \mathcal{C}^{\perp}$ and *self-dual* if $\mathcal{C} = \mathcal{C}^{\perp}$. In particular, if $\mathcal{C}$ is trace self-dual, $\mathcal{C}$ is an $(n, 2^n)$ code.

We say that two additive codes $\mathcal{C}_1$ and $\mathcal{C}_2$ are *equivalent* provided there is a map sending the codewords of $\mathcal{C}_1$ onto the codewords of $\mathcal{C}_2$ where the map consists of a permutation of coordinates followed by a scaling of coordinates by elements of $GF(4)$ followed by conjugation of some of the coordinates. Notice that permuting coordinates, scaling coordinates, and conjugating some coordinates of a self-orthogonal (or self-dual) code does not change self-orthogonality (or self-duality) and the weight distribution of the code. The *automorphism group* of $\mathcal{C}$, denoted $\mathrm{Aut}(\mathcal{C})$, consists of all maps which permute coordinates, scale coordinates, and conjugate coordinates that send codewords of $\mathcal{C}$ to codewords of $\mathcal{C}$.

Now we state the relationship between QECC and additive self-orthogonal codes over GF(4).

Lemma 1 (Theorem 2, [1]). *Suppose that $\mathcal{C}$ is an additive trace self-orthogonal $(n, 2^{n-k})$ code of $\mathrm{GF}(4)^{\mathrm{n}}$ such that there are no vectors of weight $< d$ in $\mathcal{C}^{\perp} \backslash \mathcal{C}$. Then an additive quantum-error-correcting code with parameters $[[n, k, d]]$ is obtained.*

If there are no nonzero vectors of weight $< d$ in $\mathcal{C}^{\perp}$ in the above lemma, $\mathcal{C}$ is *pure* (or *nondegenerate*); otherwise it is *impure* (or *degenerate*) [1]. A $[[n, k, d]]$ QECC can correct $[(d-1)/2]$ errors, where k is the number of *encoded qubits* (*quantum bits*).

The *Hermitian inner product* is defined as

$$\mathbf{x} \cdot \mathbf{y} = x_1 \overline{y_1} + \cdots + x_n \overline{y_n} \in \mathrm{GF}(4), \tag{2}$$

for two vectors $\mathbf{x} = (x_1, \cdots, x_n)$ and $\mathbf{y} = (y_1, \cdots, y_n)$ in $\mathrm{GF}(4)^{\mathrm{n}}$. A linear code with length n, dimension k(as a vector space over GF(4)), and minimum weight d is called an $[n, k, d]$ code. The following theorem explains why Hermitian self-orthogonal linear codes are interesting in order to construct QECC.

Lemma 2 (Theorem 3, [1]). *A linear code $\mathcal{C}$ is self-orthogonal with respect to (1) if and only if it is self-orthogonal with respect to (2).*

Combining the above two lemmas, we get the following corollary.

Corollary 1 ([1,5]). *Let $\mathcal{C}$ be a Hermitian self-orthogonal linear $[n,k]$ code over* GF(4) *such that there are no vectors of weight $< d$ in $\mathcal{C}^{\perp}\backslash\mathcal{C}$, where $\mathcal{C}^{\perp}$ is the Hermitian dual of $\mathcal{C}$. Then there is a quantum-error-correcting $[[n, n-2k, d]]$ code.*

Proof. Since the given code $\mathcal{C}$ is linear, it has parameters as an additive code $(n, 2^{2k}) = (n, 2^{n-(n-2k)})$. Thus by Lemma 1 a quantum-error-correcting $[[n, n-2k, d]]$ code is obtained.

2 Construction method

By generalizing the building-up construction [3, Theorem 1] for self-dual codes over GF(4) to self-orthogonal codes, we have the following theorem. We remark that there was an error in [3, Theorem 1] about the definition of $\overline{y_i}$ and so correct it here.

Theorem 1. *Let $G_0 = (g_i)$ be a generator matrix(may not be in standard form) of a Hermitian self-orthogonal code $\mathcal{C}_0$ over* GF(4) *of length n with dimension k, where g_i are rows of G_0 respectively for $1 \le i \le k$. Let $\mathbf{x} = (x_1, \cdots, x_n)$ be a vector in* $\mathrm{GF}(4)^{\mathrm{n}}$ *with an odd weight. Suppose that $\overline{y_i} := (x_1, \cdots, x_n) \cdot g_i$ for $1 \le i \le k$. Here $\overline{y_i}$ is the conjugate of y_i and $\cdot$ denotes the Hermitian inner product. Then the following matrix*

$$G = \left[\begin{array}{cc|c} 1 & 0 & x_1\ x_2\ \cdots\ x_{n-1}\ x_n \\ \hline y_1 & y_1 & g_1 \\ \vdots & \vdots & \vdots \\ y_k & y_k & g_k \end{array}\right]$$

generates a Hermitian self-orthogonal code $\mathcal{C}$ over GF(4) *of length $n+2$ with dimension $k+1$.*

As an example of the above theorem, let $\mathcal{C}_0$ be a Hermitian self-dual code over GF(4) generated by $\{1010, 0101\}$. If we take $\mathbf{x} = (01\omega\overline{\omega})$, then the code $\mathcal{C}$ is generated by $\{1001\omega\overline{\omega}, \overline{\omega\omega}1010, \overline{\omega\omega}0101\}$ by Theorem 1. This is the unique $[6,3,4]$ Hexacode over GF(4).

As in [3, Theorem 2] we get the converse of the above theorem as follows.

Theorem 2. *Any Hermitian self-orthogonal code $\mathcal{C}$ over* GF(4) *of length n and dimension $k > 1$ with minimum weight $d > 2$ is obtained from some Hermitian self-orthogonal code $\mathcal{C}_0$ of length $n-2$ and dimension $k-1$(up to equivalence) by the construction in Theorem 1.*

In the following section, we construct 19 inequivalent linear Hermitian self-orthogonal $[24, 11, 8]$ codes over GF(4) with its dual minimum weight 7. These give record-breaking $[[24, 2, 7]]$ quantum-error-correcting codes.

Table 1. Generator matrix of Q_{22}^1

$$G(Q_{22}^1) = \begin{bmatrix} 10000001000000133233203 \\ 01000003000020221231212 \\ 00100001000333030000120 \\ 00010002000122203320002 \\ 00001002000210312011003 \\ 00000102000210012332100 \\ 00000011000220203121001 \\ 00000000100001001133220 \\ 00000000010000011111110 \\ 00000000001000101122330 \end{bmatrix}$$

Table 2. New $[[24, 2, 7]]$ quantum-error-correcting codes using Q_{22}^1

codes C	$\mathbf{x} = (x_1, \cdots, x_{11})$	A_8, B_7	codes C	$\mathbf{x} = (x_1, \cdots, x_{11})$	A_8, B_7
$Q_{24,1}$	03001111121	117, 171	$Q_{24,2}$	22321301221	144, 156
$Q_{24,3}$	22131000321	141, 186	$Q_{24,4}$	10020033021	108, 174
$Q_{24,5}$	13013111132	99, 156	$Q_{24,6}$	12030021132	120, 198
$Q_{24,7}$	23310200132	105, 132	$Q_{24,8}$	20012000332	96, 150
$Q_{24,9}$	31100212032	105, 165	$Q_{24,10}$	02212022032	102, 162
$Q_{24,11}$	12010313032	126, 183	$Q_{24,12}$	11110021202	114, 150
$Q_{24,13}$	20223012202	96, 159	$Q_{24,14}$	33030202002	105, 147
$Q_{24,15}$	02311200002	108, 147	$Q_{24,16}$	31231302123	102, 150
$Q_{24,17}$	33321333303	102, 159	$Q_{24,18}$	20212031120	108, 180
$Q_{24,19}$	21121332320	90, 144			

3 Existence of $[[24, 2, 7]]$ quantum-error-correcting codes

According to [1, Table III], it is known that the highest minimum weight d for $[[24, 2, d]]$ codes is bounded by $6 \leq d \leq 8$. We apply Theorem 1 to a Hermitian self-orthogonal $[22, 10, 8]$ code Q_{22}^1 in Table 1 with many possibilities for vectors $\mathbf{x}$ to get 19 inequivalent Hermitian self-orthogonal $[24, 11, 8]$ codes such that their dual codes all have minimum weight $d = 7$. Hence it follows from Corollary 1 that there exist pure $[[24, 2, 7]]$ codes. Moreover length $n = 24$ is the smallest length for any known three error-correcting $[[n, k, 7]]$ codes with $k \geq 2$ according to [1, Table III]. See Table 2 for such codes, where A_8(resp, B_7) denotes the number of minimum vectors in $\mathcal{C}$(resp, $\mathcal{C}^{\perp}$), justifying the inequivalence of the codes. Here we gave the vectors $\mathbf{x}$ with only first 11 co-

ordinates, the right half being 1's. For example, $\mathbf{x} = (23310200132)$ in $Q_{24,7}$ means $\mathbf{x} = (2331020013211111111111)$. We summarize our result as follows.

Theorem 3. *There exist at least 19 inequivalent pure* $[[24, 2, 7]]$ *quantum-error-correcting codes, which are obtained from Hermitian self-orthogonal linear* $[24, 11, 8]$ *codes with its dual minimum weight 7.*

Acknowledgment. The author would like to thank Vera Pless for reading the first manuscript and the referee for useful comments.

References

1. Calderbank, A. R., Rains, E. M., Shor, P. W., Sloane, N. J. A. (1998) Quantum error correction via codes over GF(4). IEEE Trans. Inform. Theory. **44**, 1369–1387
2. Gaborit, P., Huffman, W. C., Kim, J.-L., and Pless, V. (2001) On additive GF(4) codes. DIMACS Workshop on Codes and Association Schemes DIMACS Series in Discrete Math. and Theoret. Computer Science, American Mathematical Society, **56**, 135–149
3. Kim, J.-L. (2001) New self-dual codes over GF(4) with the highest known minimum weights. IEEE Trans. Inform. Theory. **47**, 1575–1580
4. Shor, P. W. (1995) Scheme for reducing decoherence in quantum memory. Phys. Rev. A. **52**, 2493
5. Thangaraj, A., McLaughlin, S. W. (2001) Quantum codes from cyclic codes over GF(4^{m}). IEEE Trans. Inform. Theory. **47**, 1176–1178