Classification of Self-Orthogonal Codes over $\mathbb{F}_3$ and $\mathbb{F}_4$

Iliya Bouyukliev*
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
P.O. Box 323, 5000 V. Tarnovo, Bulgaria
E-mail: iliya@moi.math.bas.bg

Patric R. J. Östergård†
Department of Electrical and Communications Engineering
Helsinki University of Technology
P.O. Box 3000, 02015 HUT, Finland
E-mail: patric.ostergard@hut.fi

Abstract

Several methods for classifying self-orthogonal codes up to equivalence are presented. These methods are used to classify self-orthogonal codes with largest possible minimum distance over the fields $\mathbb{F}_3$ and $\mathbb{F}_4$ for lengths $n \leq 29$ and small dimensions (up to 6). Some properties of the classified codes are also presented. In particular, an extensive collection of quantum error-correcting codes is obtained.

Keywords: code equivalence, quantum codes, self-dual codes, self-orthogonal codes.

*Partially supported by the Bulgarian National Science Fund under Contract MM1304/2003.

†Partially supported by the Academy of Finland under Grants No. 100500 and No. 202315.

1 Introduction

Let $\mathbb{F}_q^n$ denote the vector space of n-tuples over the q-element field $\mathbb{F}_q$. A q-ary linear code C of length n and dimension k, or an $[n,k]_q$ code, is a k-dimensional subspace of $\mathbb{F}_q^n$. An inner product $(\mathbf{x},\mathbf{y})$ of vectors $\mathbf{x},\mathbf{y} \in \mathbb{F}_q^n$ defines orthogonality: Two vectors are said to be orthogonal if their inner product is 0. The set of all vectors of $\mathbb{F}_q^n$ orthogonal to all codewords from C is called the orthogonal code $C^\perp$ to C:

$$C^\perp = \{\mathbf{x} \in \mathbb{F}_q^n \mid (\mathbf{x},\mathbf{y}) = 0 \text{ for any } \mathbf{y} \in C\}.$$

It is well-known that the code $C^\perp$ is a linear $[n, n-k]_q$ code.

A $k \times n$ matrix $\mathbf{G}_C$ whose rows form a basis of C is called a generator matrix of C. A generator matrix of the code $C^\perp$, orthogonal to C, is a parity check matrix for C, denoted by $\mathbf{H}_C$.

The number of nonzero coordinates of a vector $\mathbf{x} \in \mathbb{F}_q^n$ is called its Hamming weight $\mathrm{wt}(\mathbf{x})$. The Hamming distance $d(\mathbf{x},\mathbf{y})$ between two vectors $\mathbf{x},\mathbf{y} \in \mathbb{F}_q^n$ is defined by

$$d(\mathbf{x},\mathbf{y}) = \mathrm{wt}(\mathbf{x}-\mathbf{y}).$$

The minimum distance of a linear code C is

$$d(C) = \min\{d(\mathbf{x},\mathbf{y}) \mid \mathbf{x},\mathbf{y} \in C, \mathbf{x} \neq \mathbf{y}\} = \min\{\mathrm{wt}(\mathbf{c}) \mid \mathbf{c} \in C, \mathbf{c} \neq \mathbf{0}\}.$$

A q-ary linear code of length n, dimension k and minimum distance d is said to be an $[n,k,d]_q$ code.

If $C \subseteq C^\perp$, then the code C is called *self-orthogonal*. Self-orthogonal codes with $n = 2k$ are of particular interest; then $C = C^\perp$ and the codes are called *self-dual*. The classes of self-orthogonal and self-dual codes are important in coding theory both from a practical and a theoretical point of view. Self-dual codes over $\mathbb{F}_3$ are particularly interesting because they include the Golay code of length 12, quadratic residue codes and symmetry codes. A vast number of papers have been devoted to the study of self-dual codes, see the excellent survey [19] for an overview of these results.

In this work ternary and quaternary self-orthogonal codes with maximum possible minimum distance are considered. Such codes are classified for lengths $n \leq 29$ and dimensions $k \leq 6$ (except for sets of parameters where this was not computationally feasible using our algorithms). Two different methods are used in the classification, so (in nearly all cases) the results have been obtained by two independent algorithms. Very little has earlier been known about the minimum distance and number of self-orthogonal codes, since most of the research effort has been put on the special case of self-dual

codes. For general linear codes, extensive tables of bounds can be found in [3].

In Section 2, two types of inner products are defined and some properties of the weight distributions of self-orthogonal codes are presented. Two classification methods are considered in Section 3, and the computational results obtained by these methods are tabulated in Section 4. Finally, in Section 5 some data for quantum error-correcting codes obtained from the classified quaternary self-orthogonal codes is presented.

2 Preliminaries

The *Euclidean inner product* of two vectors $\mathbf{u} = (u_1, u_2, \ldots, u_n)$ and $\mathbf{v} = (v_1, v_2, \ldots, v_n)$ from $\mathbb{F}_q^n$ is defined by

$$(\mathbf{u}, \mathbf{v})_E = u_1 v_1 + u_2 v_2 + \cdots + u_n v_n.$$

For codes over $\mathbb{F}_q$ where q is an even power of an arbitrary prime p, one can consider another type of inner product, the Hermitian inner product. The *Hermitian inner product* of two vectors $\mathbf{u} = (u_1, u_2, \ldots, u_n)$ and $\mathbf{v} = (v_1, v_2, \ldots, v_n)$ from $\mathbb{F}_q^n$ is defined by

$$(\mathbf{u}, \mathbf{v})_H = u_1 \bar{v}_1 + u_2 \bar{v}_2 + \cdots + u_n \bar{v}_n,$$

where $\bar{v}_i = v_i^{\sqrt{q}}$ for $v_i \in \mathbb{F}_q$. Consequently, for $q = 4$ the Hermitian inner product is defined by

$$(\mathbf{u}, \mathbf{v})_H = u_1 v_1^2 + u_2 v_2^2 + \cdots + u_n v_n^2.$$

In the ternary case we consider the Euclidean inner product and in the quaternary case (like in most other studies) the Hermitian inner product. Throughout the paper, these inner products are assumed in the discussion of self-dual and self-orthogonal codes.

The MacWilliams identities can give a lot of information about possible weight distributions of self-dual codes. However, in the current study we do not use this information. We shall now present some known basic results on the codes considered here. For a proof of Lemma 1, see [8, Theorem 1.4.10]. A code is even (resp. doubly-even) if the weights of all codewords are divisible by 2 (resp. 4).

Lemma 1 *Let C be a code over F_q with $q = 3$ or 4.*

(i) When $q = 3$, every codeword of C has weight divisible by three if and only if C is self-orthogonal.

(ii) When $q = 4$, every codeword of C has weight divisible by two if and only if C is Hermitian self-orthogonal.

3 Two Classification Methods

In any work on classifying mathematical objects, one should carefully define the concept of equivalence (or, depending on the conventional terminology, isomorphism). For self-dual and self-orthogonal codes, the definition of equivalence depends on the inner product. For ternary codes with Euclidean inner product and quaternary codes with Hermitian inner product, the definition coincides with the definition for general linear codes, cf. [19].

Two linear q-ary codes, C_1 and C_2, are said to be *equivalent* if the codewords of C_2 can be obtained from the codewords of C_1 via a sequence of transformations of the following types:

1. permutation of coordinates;
2. multiplication of the elements in a given coordinate by a nonzero element of $\mathbb{F}_q$;
3. application of a field automorphism to the elements in all coordinates simultaneously.

(The field $\mathbb{F}_3$ does not have nontrivial automorphisms, and the only nontrivial automorphism of $\mathbb{F}_4$ is conjugation.) An *automorphism* of a linear code C is a sequence of such transformations that maps each codeword of C onto a codeword of C. The automorphisms of a code C form a group, called the automorphism group of the code and denoted by $\mathrm{Aut}(C)$.

Determining equivalence of codes plays a central role in any classification algorithm. Not only must one make sure that all completed codes are inequivalent, but determining equivalence of partial codes is also important for efficiency reasons. The first author utilized an algorithm for determining code equivalence that was developed in [1] and is based on the ideas in [12]. The approach of the second author depends on the graph isomorphism program *nauty* [12, 13] for this matter; see [15] for further details (but some enhancements of the basic method will be presented here).

The approaches to be presented differ in the ways the codes are built up via smaller codes. For efficiency reasons, Lemma 1 should be taken into account.

The first approach utilizes results on the parameters of residuals of codes. Let $\mathbf{G}$ be a generator matrix of a linear $[n, k, d]_q$ code C. Then the *residual code* $\mathrm{Res}(C, \mathbf{c})$ of C with respect to a codeword $\mathbf{c}$ is the code generated by the restriction of $\mathbf{G}$ to the columns where $\mathbf{c}$ has a zero entry. The following result is from [6].

Lemma 2 *Suppose C is an $[n, k, d]_q$ code and suppose $\mathbf{c} \in C$ has weight w, where $d > w(q-1)/q$. Then $Res(C, \mathbf{c})$ is an $[n-w, k-1, d']_q$ code with $d' \geq d - w + \lceil w/q \rceil$.*

In addition to constructing $[n, k, d]_q$ codes from their $[n-w, k-1, d']_q$ residual codes, one may also start from $[n-i, k, d']_q$ codes. On the bottom of this hierarchy of extensions is the trivial $[k, k, 1]_q$ code.

In the second approach, $[n, k, d]_q$ codes are constructed by extending $[n-i, k-i, d]_q$ or $[n-i-1, k-i, d]_q$ codes. The following result shows when the latter type of codes can be used [10, p. 592].

Lemma 3 *Let C be an $[n, k, d]_q$ code. If there exists a codeword $\mathbf{c} \in C^\perp$ with $wt(\mathbf{c}) = i$, then there is an $[n-i, k-i+1, d]_q$ code.*

If $\mathbf{G}$ is a generator matrix for an $[n-i, k-i, d]_q$ or an $[n-i-1, k-i, d]_q$ code, we extend it (in all possible ways) to

$$\left(\begin{array}{c|c} * & \mathbf{I}_i \\ \hline \mathbf{G} & \mathbf{0} \end{array}\right) \quad \text{or} \quad \left(\begin{array}{c|c} * & \mathbf{1}\ \mathbf{I}_i \\ \hline \mathbf{G} & \mathbf{0} \end{array}\right), \tag{1}$$

respectively, where $\mathbf{I}_i$ is the $i \times i$ identity matrix, $\mathbf{1}$ is an all-1 column vector, and the starred submatrix is to be determined. If we let the matrix $\mathbf{G}$ be in systematic form, we can fix k more columns to get

$$\left(\begin{array}{c|c|c} * & \mathbf{0} & \mathbf{I}_i \\ \hline \mathbf{G}_1 & \mathbf{I}_k & \mathbf{0} \end{array}\right) \quad \text{or} \quad \left(\begin{array}{c|c|c} * & \mathbf{0} & \mathbf{1}\ \mathbf{I}_i \\ \hline \mathbf{G}_1 & \mathbf{I}_k & \mathbf{0} \end{array}\right). \tag{2}$$

More information on this approach can be found in [2]. The subcodes through which the codes are constructed must also be self-orthogonal. For the approach via residual codes, on the other hand, such a restriction does not apply.

If $i = 1$ in the second approach, we get the method used in [15], where $[n, k, d]_q$ codes are obtained from $[n-1, k-1, d]_q$ codes by adding a new column in all possible ways to the parity check matrix, checking the minimum distance and orthogonality of the new code, and finally removing copies of equivalent codes. We shall now see how the equivalence test can be enhanced for this particular variant.

To speed up the algorithm and reduce the need for extensive tables of intermediate codes, a classification technique developed by McKay [14] was implemented. Essentially, the idea is that (in our case) a code can be obtained from several subcodes, only one of which is identified as the "parent" of the new code. Then a new code is rejected unless it was obtained from its

parent. Note that identifying a certain subcode essentially means identifying a coordinate, and with the encoding used in [15] the output of *nauty* can be used to get a canonical labelling of the coordinates.

Shortening a $[n, k, d]_q$ linear code by deleting one coordinate and keeping the codewords with a 0 in the given coordinate gives a $[n-1, k', d]_q$ code with $k' = k$ if the original code has only 0s in the coordinate to be deleted, and $k' = k - 1$ otherwise. Therefore, in the parent test of a McKay-type algorithm—after adding one coordinate via a new column in the parity check matrix—one should first check which coordinates are all-zero. In the test itself, only coordinates that are not all-zero should be considered. For fields with nontrivial automorphisms, like $\mathbb{F}_4$, if one uses the idea of producing one graph for each automorphism [15], a code passes the parent test if at least one of the $|\mathrm{Aut}(\mathbb{F}_q)|$ instances passes the test.

4 Results

We first give a short overview of old results on classifying ternary and quaternary self-dual and self-orthogonal codes. See [19] for more details and references.

The length of any ternary self-dual code is divisible by 4, and this necessary condition is also sufficient. Such codes of length less than or equal to 20—and self-orthogonal codes of maximal dimension and length less than or equal to 19—have been completely classified in [5, 11, 16, 17]. A partial classification of the self-dual codes of length 24 can be found in [9], including a classification of such codes with maximum minimum distance. For ternary self-dual codes, $d \leq 3\left\lfloor \frac{n}{12} \right\rfloor + 3$ holds [19, Theorem 28]. Codes meeting this bound are called *extremal* and are known to exist for admissible lengths $n \leq 48$, $56 \leq n \leq 64$, and do not exist for $n = 72, 96, 120$ and $n \geq 144$.

Quaternary self-dual codes have even lengths. They have been classified up to length 16 in [5]. For quaternary self-dual codes, $d \leq 2\left\lfloor \frac{n}{6} \right\rfloor + 2$ holds [19, Theorem 28]. Extremal codes (which meet this bound) exist for admissible lengths $n \leq 10$, $14 \leq n \leq 22$ and $n = 28, 30$, and do not exist for $n = 12, 24, 102, 108, 114, 120, 122$ and $n \geq 126$.

There are only sporadic classification results for ternary and quaternary self-orthogonal codes in the literature [7]. This work makes a contribution towards filling this gap.

The classification results are presented in Tables 1 and 2. For lengths $n \leq 29$ and dimensions $3 \leq k \leq 6$, the maximal minimum distance and the number of corresponding codes is shown. Entries that could not be computed with a reasonable amount of CPU time are empty. For such in-

Table 1: Classification of ternary self-orthogonal codes

$n\backslash k$	3		4		5		6	
7	3	1						
8	3	1	3	1				
9	6	1	3	1				
10	6	1	6	1				
11	6	2	6	1	6	1		
12	6	6	6	6	6	1	6	1
13	9	1	6	10	6	4	6	1
14	9	1	6	27	6	15	6	4
15	9	4	9	3	6	73	6	20
16	9	9	9	13	9	1	6	121
17	9	16	9	58	9	35	6	885
18	12	2	9	308	9	997	9	105
19	12	4	12	1	9	15207	9	18019
20	12	14	12	32	12	2	9	
21	12	36	12	406	12	359	9	
22	15	1	12	3679	12	107017	12	698
23	15	3	12	20673	12		12	
24	15	15	15	13	12		12	
25	18	45	15	699	15	23	12	
26	18	1	15	17703	15		15	2
27	18	4	18	1	15		15	
28	18	14	18	6	15		15	
29	18	49	18	406	18	1	15	

stances, one could consider a subclass of codes. We considered *doubly-even* self-orthogonal quaternary codes to find out that the number of $[20, 4, 12]_4$, $[20, 5, 12]_4$, $[21, 5, 12]_4$, $[25, 4, 16]_4$ and $[25, 5, 16]_4$ such codes is 16, 4, 4, 333 and 31, respectively.

5 Quaternary Self-Orthogonal Codes and Quantum Codes

Quantum computers have received a lot of attention in the recent decade, after Shor proved that integer factorization can be solved in polynomial time on such computers [18]. The quantum analogue of a bit of information is called a *qubit* and is the state of a system in a 2-dimensional Hilbert space

Table 2: Classification of quaternary (Hermitian) self-orthogonal codes

$n\backslash k$	3		4		5		6	
6	4	1						
7	4	1						
8	4	4	4	1				
9	6	1	4	2				
10	6	4	4	12	4	2		
11	6	6	6	2	4	6		
12	8	5	6	22	6	2	4	5
13	8	10	8	5	6	19	6	1
14	10	1	8	92	8	4	6	23
15	10	7	8	911	8	460	8	3
16	12	1	10	50	8	45311	8	1081
17	12	4	12	1	10	91	8	
18	12	45	12	12	10		10	3
19	12	185	12	5673	10		10	
20	14	10	12		12		10	
21	16	1	14	212	12		12	
22	16	4	14		14	67	12	
23	16	46	16	3	14		12	
24	16	614	16	40397	16		14	
25	18	6	16		16		14	
26	18	185	18	14	16		16	
27	20	2	18		16		16	
28	20	46	20	1	18		16	
29	20	850	20	22656	18		16	

spanned by e_0 and e_1, where e_0 and e_1 are eigenvectors corresponding to the eigenvalues 0 and 1 of the qubit.

The setting in which quantum error-correcting codes (QECCs) exist is the quantum state space of n qubits (quantum bits, or 2-state quantum systems). This space is $\mathbb{C}^{2^n}$, and it has a natural decomposition as the tensor product of n copies of $\mathbb{C}^2$, where each copy corresponds to one qubit. Many known quantum codes have close connections to a finite group of unitary transformations of $\mathbb{C}^{2^n}$, known as a Clifford group.

A QECC is defined to be a unitary mapping (encoding) of k qubits (2-state quantum systems) into a subspace of the quantum state space of n qubits such that if any t of the qubits undergo arbitrary decoherence, not necessarily independently, the resulting n qubits can be used to faithfully reconstruct the original quantum state of the k encoded qubits. In general, by $[[n, k, d]]$ we denote a QECC that encodes k qubits of a quantum system into n qubits. The parameter d is the minimum distance of the code. A QECC with minimum distance d can be used to detect errors that involve at most $d-1$ of the n subsystems. Alternatively, one can correct errors that involve at most $\lfloor (d-1)/2 \rfloor$ subsystems. See [4] for more information about QECCs.

It is known that if C is a Hermitian self-orthogonal linear $[n, k]_4$ code such that there are no vectors of weight $< d$ in $C^{\perp} \setminus C$ (where $C^{\perp}$ is the Hermitian dual of C), then there is a quantum error-correcting $[[n, n-2k, d]]$ code [4]. By investigating the classified codes with respect to this property, a number of quantum error-correcting codes were detected. The parameters of these codes with $d \geq 3$ are tabulated in Table 3.

The first column of Table 3 shows the parameters of the quaternary codes, and the parameters of the corresponding quantum codes are given in the second column. The orders of the automorphism groups of the quaternary codes with dual distance at least 3 are given in the third column—an upper index gives the number of corresponding codes—and the last column lists the number of quaternary codes with maximum possible dual distance.

Table 3: Quaternary self-orthogonal codes and quantum codes

C	D	$\lvert\mathrm{Aut}(C)\rvert$	#
$[6,3,4]$	$[[6,0,3]]$	2160	1
$[7,3,4]$	$[[7,1,3]]$	1008	1
$[8,3,4]$	$[[8,2,3]]$	1728	1
$[8,4,4]$	$[[8,0,4]]$	8064	1
$[9,3,6]$	$[[9,3,3]]$	1296	1
$[9,4,4]$	$[[9,1,3]]$	$4320, 1152$	2
$[10,3,6]$	$[[10,4,3]]$	360	1
$[10,4,4]$	$[[10,2,3]]$	$1728, 192, 432, 259200$	4
$[10,5,4]$	$[[10,0,4]]$	$43200, 11520$	2
$[11,3,6]$	$[[11,5,3]]$	360	1
$[11,4,6]$	$[[11,3,3]]$	36	1
$[11,5,4]$	$[[11,1,3]]$	$1728, 12096, 8640, 576, 11520, 777600$	6
$[12,3,8]$	$[[12,6,3]]$	1296	1
$[12,4,6]$	$[[12,4,4]]$	$18, 144^2, 576, 12^2, 24, 1296, 720$	1
$[12,5,6]$	$[[12,2,4]]$	$72, 216$	1
$[12,6,4]$	$[[12,0,4]]$	$20736, 60480, 6912, 138240, 9331200$	5
$[13,3,8]$	$[[13,7,3]]$	1728	1
$[13,4,8]$	$[[13,5,3]]$	$24^2, 36, 432, 720$	5
$[13,5,6]$	$[[13,3,4]]$	$72, 12, 36^3, 144, 6^5, 24, 18^3, 48$	1
$[13,6,6]$	$[[13,1,5]]$	468	1
$[14,3,10]$	$[[14,8,3]]$	1008	1
$[14,4,8]$	$[[14,6,4]]$	$3^5, 12^8, 48^5, 24^3, 6^8, 432^2,$	1
		$42, 9, 36, 144^3, 18, 192, 3456, 8064$	
$[14,5,8]$	$[[14,4,4]]$	$36, 24, 72, 288$	4
$[14,6,6]$	$[[14,2,5]]$	$6^2, 48, 36^8, 12^3, 18, 72, 24, 144^2, 252$	1
$[15,3,10]$	$[[15,9,3]]$	2160	1
$[15,4,8]$	$[[15,7,3]]$	$24^5, 6^{52}, 12^{30}, 48^6, 2160, 3^{74}, 18^6, 36^4, 9^2$	
		$144^3, 192, 1152, 60, 432, 504, 120960$	189
$[15,5,8]$	$[[15,5,4]]$	$24^7, 48, 6^{95}, 3^{258}, 12^{22}, 9^5, 18^5$	
		$108, 72^3, 216, 30^2, 60, 36, 360, 288, 15$	26
$[15,6,8]$	$[[15,3,5]]$	$216, 72, 360$	3
$[16,3,12]$	$[[16,10,3]]$	17280	1
$[16,4,10]$	$[[16,8,3]]$	$3^{18}, 6^{10}, 24^2, 18, 96, 12^3, 9, 36, 72$	38
$[16,5,8]$	$[[16,6,4]]$	$48^{32}, 24^{118}, 6^{2824}, 3^{27856}, 12^{496}, 72^9$	
		$36^{19}, 9^{31}, 576^2, 192^6, 96^{18}, 18^{24}, 60^3, 216^3, 360$	
		$1080^2, 30^3, 288^2, 144^3, 15, 1728, 2160, 768^3, 3072$	
		$384^2, 18432, 2304^3, 54, 1152, 8064, 1935360$	519

Table 3: (cont.) Quaternary self-orthogonal codes and quantum codes

C	D	$\lvert\mathrm{Aut}(C)\rvert$	#
$[16,6,8]$	$[[16,4,4]]$	$12^{52}, 48^2, 96^6, 768, 36^{12}, 864, 3^{686}, 6^{259}, 144^2$	
		$24^{14}, 108, 9^3, 18^{15}, 72^2, 288, 384, 4608$	697
$[17,4,12]$	$[[17,9,4]]$	48960	1
$[17,5,10]$	$[[17,7,4]]$	$3^{82}, 6^6, 9^2, 126$	27
$[18,4,12]$	$[[18,10,3]]$	$24, 12, 72^3, 36^2, 60, 360, 432, 6480$	11
$[18,6,10]$	$[[18,6,5]]$	$18, 54, 108$	2
$[19,4,12]$	$[[19,11,3]]$	$3^{2111}, 18^9, 6^{350}, 36^{11}, 12^{55}, 72^7, 9^{10}, 144, 24^{12}, 27, 48^3$	2570
$[21,3,16]$	$[[21,15,3]]$	362880	1
$[21,4,14]$	$[[21,13,3]]$	$12^6, 6^{28}, 3^{169}, 9^4, 24, 42, 18, 63, 60$	212
$[22,5,14]$	$[[22,12,4]]$	$3^{42}, 6^{18}, 18^4, 9, 12, 36$	67
$[23,4,16]$	$[[23,15,3]]$	24	1
$[24,4,16]$	$[[24,16,3]]$	$6^{1302}, 60, 3^{18934}, 12^{139}, 18^{13}, 24^{28}, 9^{12}, 36^5$	
		$72^4, 288, 120, 192^3, 48^4, 1152, 144^2, 90$	
		$162, 414720, 576, 96, 648$	20456
$[26,4,18]$	$[[26,18,3]]$	$3^9, 12, 6^2, 18, 24$	14
$[28,4,20]$	$[[28,20,3]]$	42	1
$[29,4,20]$	$[[29,21,3]]$	$6^{840}, 3^{10385}, 12^{111}, 24^{10}, 18^5, 9^4, 36^5, 48^3, 72, 21$	11365

References

[1] I. Bouyukliev, An algorithm for finding isomorphisms of codes, Proceedings of the International Workshop OCRT, Sunny Beach, Bulgaria, June 2001, pp. 35–41.

[2] I. Bouyukliev and J. Simonis, Some new results for optimal ternary linear codes, *IEEE Trans. Inform. Theory* **48** (2002), 981–985.

[3] A. E. Brouwer, Bounds on the size of linear codes, in *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman, Eds., Elsevier, Amsterdam, 1998, pp. 295–461.

[4] 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* **44** (1998), 1369–1387.

[5] J. H. Conway, V. Pless and N. J. A. Sloane, Self-dual codes over GF(3) and GF(4) of length not exceeding 16, *IEEE Trans. Inform. Theory* **25** (1979), 312–322.

[6] S. Dodunekov, Minimal block length of a linear q-ary code with specified dimension and code distance, *Problems Inform. Transmission* **20** (1984), 239–249.

[7] M. van Eupen and P. Lisoněk, Classification of some optimal ternary linear codes of small length, *Des. Codes Cryptogr.* **10** (1997), 63–84.

[8] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, Cambridge, 2003.

[9] J. S. Leon, V. Pless and N. J. A. Sloane, On ternary self-dual codes of length 24, *IEEE Trans. Inform. Theory* **27** (1981), 176–180.

[10] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.

[11] C. L. Mallows, V. Pless and N. J. A. Sloane, Self-dual codes over GF(3), *SIAM J. Appl. Math.* **31** (1976), 649–666.

[12] B. D. McKay, Practical graph isomorphism, *Congr. Numer.* **30** (1981), 45–87.

[13] B. D. McKay, *nauty* user's guide (version 1.5), Computer Science Department, Australian National University, Tech. Rep. TR-CS-90-02, 1990.

[14] B. D. McKay, Isomorph-free exhaustive generation, *J. Algorithms* **26** (1998), 306–324.

[15] P. R. J. Östergård, Classifying subspaces of Hamming spaces, *Des. Codes Cryptogr.* **27** (2002), 297–305.

[16] V. Pless, On the uniqueness of the Golay codes, *J. Combin. Theory* **5** (1968), 215–228.

[17] V. Pless, N. J. A. Sloane and H. N. Ward, Ternary codes of minimum weight 6 and the classification of self-dual codes of length 20, *IEEE Trans. Inform. Theory* **26** (1980), 305–316.

[18] P. W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM J. Comput.* **26** (1997), 1484–1509.

[19] E. M. Rains and N. J. A. Sloane, Self-dual codes, in *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman, Eds., Elsevier, Amsterdam, 1998, pp. 177–294.