ELSEVIER

Discrete Mathematics 203 (1999) 215–228

DISCRETE MATHEMATICS

Optimal self-dual codes over $\mathbb{Z}_4$

Eric Rains*

AT&T Research, Room C290, 180 Park Ave., Florham Park, NJ 07932-0971, USA

Received 17 November 1997; revised 14 August 1998; accepted 8 September 1998

Abstract

The optimal minimal Euclidean norm of self-dual codes over $\mathbb{Z}_4$ is known through length 24; the purpose of the present note is to determine the optimal minimal Hamming and Lee weights in this range. In the process, we classify all Lee-optimal codes of length 18, 21, 23, and 24. In particular, we find a total of 13 inequivalent codes with the same symmetrized weight enumerator as the Hensel-lifted Golay code. © 1999 Elsevier Science B.V. All rights reserved.

Keywords: Classification optimal self-dual $\mathbb{Z}_4$ code

0. Introduction

In a forthcoming paper [5], Dougherty et al. give tables of bounds on the optimal minimum Euclidean norm, Lee weight, and Hamming weight, for Type I self-dual codes over $\mathbb{Z}_4$, of length up to 24. Their tables are tight up to length 24 for Euclidean norm, but only up to length 16 for the Lee and Hamming weights (based on the classification of self-dual codes over $\mathbb{Z}_4$ through length 15 [6], and of Type II codes through length 16 [10]). The purpose of the present note is to tighten these bounds. To be precise, we give, for length 17 through 24, the optimum minimal Lee weight and the optimum minimal Hamming weight for a self-dual code over $\mathbb{Z}_4$.

The basic idea is to study self-dual codes over $\mathbb{Z}_4$ via their reductions mod 2. In several cases, we find that the reduction is uniquely determined by the minimal weight. This allows us to reduce the problem of finding optimal codes to a problem of enumerating the inequivalent lifts of a given doubly-even binary code. It turns out that the set of lifts of a fixed binary code has a natural affine structure, on which the automorphisms of the binary code act. The orbits of the resulting affine group are then in one-to-one correspondence with the equivalence classes of lifts. This technique allows us to enumerate the optimal codes of length 18 and 21.

* Corresponding author. E-mail: rains@research.att.com.

PII: S0012-365X(98)00358-6

A somewhat refined version of this method allows us to enumerate Lee-optimal codes of length 23 and 24. It turns out that there are 30 such codes at length 23, and 13 such codes at length 24. In particular, there are 12 other codes with the same symmetrized weight enumerator as the Hensel-lifted Golay code.

0.1. Type II codes and shadows

We will have occasion in the sequel to refer to results from the theory of shadows of self-orthogonal codes. In the case of codes over $\mathbb{Z}_4$, the basic identity of the theory is:

$$\tfrac{1}{2}(\mathrm{Norm}(v+w)-\mathrm{Norm}(v)-\mathrm{Norm}(w))\equiv\langle v,w\rangle \pmod 4,$$

for any vectors v and w in $\mathbb{Z}_4^n$; the left-hand side is defined by taking any lift of v and w to $\mathbb{Z}_8^n$. In particular, $\frac{1}{2}$Norm defines a linear functional on any self-orthogonal code. This has two major consequences. First, it is possible for the linear functional to vanish on a self-dual code; in that case, the code is said to be of Type II (by analogy with the binary case). Second, for any self-orthogonal code C, we can define a certain coset $S(C)$ of its dual known as its shadow, as follows. If $\frac{1}{2}$Norm vanishes on C, then $S(C)=C^{\perp}$. Otherwise, $S(C)=C_0^{\perp}-C^{\perp}$, where C_0 is the kernel of $\frac{1}{2}$Norm in C. The primary significance of the shadow is that the symmetrized weight enumerator of $S(C)$ can be computed from the symmetrized weight enumerator of C by an analogue of the MacWilliams transform.

For binary codes, the analogous identity is

$$\tfrac{1}{2}(\mathrm{wt}(v+w)-\mathrm{wt}(v)-\mathrm{wt}(w))\equiv\langle v,w\rangle \pmod 2;$$

the remaining definitions are analogous. A (not necessarily self-dual) code on which $\frac{1}{2}$wt vanishes (i.e., all weights are a multiple of 4) is said to be 'doubly-even'.

For an overview of shadow theory, see [11]; for the specific case of $\mathbb{Z}_4$ codes, see [5].

1. Reduction mod 2

After [4], we associate two binary codes to a $\mathbb{Z}_4$ code. If C is a $\mathbb{Z}_4$ code, $C^{(1)}$ (the 'residue code' of C) is the binary code consisting of the reduction mod 2 of every vector in C. $C^{(2)}$ is the 'torsion code' of C; that is, the set of vectors of C that reduce mod 2 to 0.

Theorem 1. *If C is self-dual, then $(C^{(1)})^{\perp}=C^{(2)}$. Furthermore, the minimum Hamming weight of C is equal to the minimum distance of $C^{(2)}$.*

Proof. The first statement follows from dimension counting [4]. For the second statement, we remark that multiplication by 2 never increases the Hamming weight. Thus

the minimum Hamming weight is determined solely by those vectors v such that $2v = 0$. But this is precisely the definition of $C^{(2)}$. □

Since every binary code with all weights a multiple of 4 is the residue code of some self-dual code over $\mathbb{Z}_4$, this reduces the problem of determining the optimal Hamming weight to a problem of binary codes, namely that of finding doubly-even binary codes with largest possible dual distance. We say a code is 'Hamming-optimal' if it has the largest possible minimum Hamming distance, and similarly for 'Lee-optimal'.

Theorem 2. *For* $n = 17, 18, 19, 20, 21, 22, 23,$ *and* 24, *the optimal Hamming weight of a self-dual* $\mathbb{Z}_4$ *code of length* n *is* $4, 4, 3, 4, 5, 6, 7,$ *and* 8, *respectively. The residue code of a Hamming-optimal code of length* 17 *is the maximally self-orthogonal code* $(d_{10}e_7)^+$. *The residue code of a Hamming-optimal code of length* 18 *is the doubly-even subcode of the self-dual code* $(d_6^3)^+$. *Finally, the residue code of a Hamming-optimal code of length* 21 *through* 24 *is a shortened Golay code.*

Proof. Consider, first, length 17. Here, we are looking for a doubly-even code of length 17, with minimum dual distance at least 4. Such a code must have a weight enumerator of the form

$$x^{17} + a_4 x^{13} y^4 + a_8 x^9 y^8 + a_{12} x^5 y^{12} + a_{16} x y^{16}.$$

But $a_{16} = 0$, since the full-weight vector is in $C^{(2)}$. To be precise, if there were a vector of weight 16 in $C^{(1)}$, then there would perforce be a vector of weight 16 in $C^{(2)}$. But the sum of that vector and the full-weight vector would be a vector of weight 1 in $C^{(2)}$, which is not allowed. From the fact that the dual has no vectors of weight 1, 2, and 3, we get equations:

$$\begin{aligned} 9a_4 + a_8 - 7a_{12} + 17 &= 0, \\ 32a_4 - 8a_8 + 16a_{12} + 136 &= 0, \\ 48a_4 - 8a_8 + 680 &= 0. \end{aligned}$$

Solving these equations, we deduce that $C^{(1)}$ has weight enumerator

$$x^{17} + 17x^{13} y^4 + 187x^9 y^8 + 51x^5 y^{12}.$$

Since $a_4 \neq 0$, we immediately conclude that the optimal Hamming weight at length 17 is at most 4. On the other hand, the maximally self-orthogonal code $(d_{10}e_7)^+$ has this weight enumerator, so Hamming weight 4 is attainable. Indeed, this is the unique such code. From the weight enumerator, we see that $C^{(1)}$ has dimension 8, and thus is maximally self-orthogonal. We can construct a self-dual code C' of length 18 from $C^{(1)}$ by appending 0 to all vectors of $C^{(1)}$ and appending 1 to all vectors of $C^{(2)}$ not in $C^{(1)}$. The weight enumerator of C' is thus determined; from the list of codes in [3], we conclude that $(d_{10}e_7 f_1)^+$ is the unique possibility for C', and thus that $(d_{10}e_7)^+$ is the unique possibility for $C^{(1)}$.

Similarly, dual distance at least 4 at length 18 suffices to determine the weight enumerator, and the code (as the doubly-even subcode of a uniquely determined self-dual code). At lengths 21–24, we need only assume that the dual distance is at least 5 to determine the weight enumerator. Indeed, at lengths 21–23, if we assume that the dual distance is at least 4, then we obtain a one-dimensional family of weight enumerators. Applying linear programming, we find that precisely one weight enumerator in the family has nonnegative coefficients and dual coefficients.

At length 19, the unique weight enumerator with dual distance at least 4 has negative coefficients. At length 20, the assumption that the dual distance is at least 5 leads to incompatible equations. In both cases, we can meet the resulting bound by shortening the Golay code. Here, however, the weight enumerator is not unique. At length 19, the weight enumerators with dual distance 3 are

$$x^{19} + 78x^{11}y^8 + 48x^7y^{12} + x^3y^{16},$$
$$x^{19} + x^{15}y^4 + 75x^{11}y^8 + 51x^7y^{12},$$
$$x^{19} + 4x^{15}y^4 + 150x^{11}y^8 + 100x^7y^{12} + x^3y^{16}.$$

At length 20, the weight enumerators with dual distance 4 are

$$x^{20} + 130x^{12}y^8 + 120x^8y^{12} + 5x^4y^{16},$$
$$x^{20} + x^{16}y^4 + 126x^{12}y^8 + 126x^8y^{12} + x^4y^{16} + y^{20},$$
$$x^{20} + 5x^{16}y^4 + 250x^{12}y^8 + 250x^8y^{12} + 5x^4y^{16} + y^{20}.$$

(In both cases, the first weight enumerator (the one with minimum distance 8) corresponds to a shortened Golay code.) □

The constraint that a code have a given minimal Hamming weight has surprisingly strong implications for the symmetrized weight enumerator. For any vector v in C, the number of ± 1's in v must be the weight of some vector in $C^{(2)}$ (since, of course, $2v \in C$). Moreover, if v is a vector in the shadow of C [5], then again $2v \in C^{(2)}$. This gives a number of linear constraints on the coefficients of C's symmetrized weight enumerator.

2. Lift spaces

For some purposes, it is nice to have not just the optimum weight, but also a list of all codes with that weight. Once we have a list of possible residue codes, it remains to enumerate the inequivalent lifts of each. The following result is the key:

Theorem 3. *Let A be a doubly-even binary code of dimension k. The set of self-dual codes C over $\mathbb{Z}_4$ with $C^{(1)} = A$ has a natural structure as an affine space $\mathscr{L}(A)$ of dimension $k(k+1)/2$ over* GF(2). *Moreover, this affine structure is preserved under column negation and any permutation in* Aut(A).

Proof. Pick a generator matrix M for A and a binary matrix B such that M together with B generates $A^{\perp}$, and consider the set $\mathscr{L}'(M,B)$ of all $(n-k)\times n$ matrices M' of the following form:

$$\begin{pmatrix} A' \\ 2B \end{pmatrix},$$

where A' is a $k\times n$ matrix that reduces to $M \bmod 2$. If we pick any matrix M'_0 in $\mathscr{L}'(M,B)$, then for any other matrix $M'\in\mathscr{L}'(M,B)$, $A'-A'_0$ reduces to $0 \bmod 2$; consequently, we can associate a $k\times n$ binary matrix $(A'-A'_0)/2$ to any element of $\mathscr{L}'(M,B)$. This clearly gives $\mathscr{L}'(M,B)$ the structure of an nk-dimensional affine space over GF(2).

For $M'\in\mathscr{L}'(M,B)$, any change of basis of M' that results in another element of $\mathscr{L}'(M,B)$ can be decomposed into steps of the following form: (1) negate one of the first k rows, (2) add twice one of the first k rows to another of the first k rows, or (3) add one of the last $n-2k$ rows to one of the first k rows. But each of these three transformations has the effect of a translation on $\mathscr{L}'(M,B)$. For instance, if we add twice the second row to the first row, then this has the same effect as adding the second row of M to the first row of $(A'-A'_0)/2$. Let V be the vector space generated by these translations. (Note that V is essentially given by k copies of $A^{\perp}$, since the above transformations allow us to add any element of $A^{\perp}$ to any row of $(A'-A'_0)/2$.)

Consider, now, the effect of column negation and permutations on $\mathscr{L}'(M,B)$. Column negation is again a translation (this time adding a particular column of M to the corresponding column of $(A'-A'_0)/2$). A permutation π of the columns, on the other hand, is somewhat more complicated. Assuming $\pi\in\mathrm{Aut}(A)$, there will be some change of basis that we can apply to $\pi(M)$ that again produces M. But, then we can lift that change of basis to take any $\pi(M')$ back to $\mathscr{L}'(A,B)$. The combined operation clearly acts linearly on M', and thus induces an affine transformation on $\mathscr{L}'(M,B)$. Moreover, this transformation preserves the vector space V, since π preserves $A^{\perp}$.

Finally, we note that the set of M' that generate a self-dual code is a subspace $\mathscr{L}'_0(M,B)$ of $\mathscr{L}'(M,B)$, since the condition of self-duality is a linear one on $(A'-A'_0)/2$. Since changes of basis, column negation, and permutations all preserve self-duality, we see that the corresponding affine transformations preserve $\mathscr{L}'_0(M,B)$. But then we can define an affine structure on $\mathscr{L}(A)$ as the quotient of $\mathscr{L}'_0(M,B)$ by the translations in V; this clearly has the invariance properties claimed. Furthermore, we can compute the dimension of $\mathscr{L}(A)$ from the fact that $\mathscr{L}(A)$ has $2^{k(k+1)/2}$ elements [7].

It remains only to show that the derived affine structure on $\mathscr{L}(A)$ is independent of the choices of M and B. But by applying a $\mathbb{Z}_4$-linear change of basis to the elements of $\mathscr{L}'(M,B)$, we can obtain the space corresponding to any other choices of M and B; this change of basis induces an affine transformation. □

Note that any equivalence of codes in $\mathscr{L}(A)$ must, by definition, take the form of a permutation followed by some number of column negations; since this must preserve the residue code, it follows that the permutation must be in $\mathrm{Aut}(A)$. Consequently, two

codes in $\mathscr{L}(A)$ are equivalent if and only if they are in the same orbit under the action of $\mathrm{Aut}(A)$ and column negations. Indeed, since column negations act as translations, we can quotient out by those as well. Note that this will not, in general, reduce the dimension by n, since some combinations of column negations will leave the codes in $\mathscr{L}(A)$ unchanged (e.g. negation of all columns). For the codes of present interest to us, there are only two such possibilities (negation of all columns and negation of no columns), so the quotient has dimension $k(k+1)/2-n+1$.

This, then, is our technique for classifying all lifts of A. We first construct the action of the automorphism group on the quotient of the space of lifts by the action of column negations. We then compute the orbits of this affine group. (The computational mathematics package `magma`, for instance, contains routines for finding orbits of matrix groups.)

We thus find a total of 62 Hamming-optimal codes of length 17, 66 Hamming-optimal codes of length 18, and 384 Hamming-optimal codes of length 21. For length 21, the quotient affine space had dimension 25, which made direct orbit finding somewhat tricky. However, the resulting 26-dimensional matrix group has an invariant submodule of dimension 16, which can be used to simplify the calculation (first find representatives of the orbits in the quotient, then find the equivalence classes within each of those cosets).

At length 22, the space has dimension 34, while the group has only 887 040 elements; we find therefore, that there are at least 19 368 orbits, and thus at least 19 368 inequivalent Hamming-optimal codes. Similarly, at length 23, there are at least 1.7 million inequivalent Hamming-optimal codes, and at length 24, there are at least 147 million inequivalent Hamming-optimal codes.

3. Lee weights

To determine the optimal Lee weights, we first note that we can use the Hamming weight to bound the Lee weight:

Lemma 4. *If C is a self-dual code over $\mathbb{Z}_4$, with minimal Hamming weight h and minimal Lee weight l, then*

$$l \leqslant 2h.$$

Proof. Since the minimal Hamming weight is h, it follows that there exists a vector in C with h 2's, and $n-h$ 0's. But that vector has Lee weight $2h$. □

Corollary 5. *A self-dual code over $\mathbb{Z}_4$ with length* 17 *and minimum Lee weight* 8 *must be Hamming-optimal. Similarly, a self-dual code of length* 18, 19, 20, 21, 22, 23, *and* 24, *with minimum Lee weights at least* 8, 6, 8, 8, 8, 8, *or* 10, *respectively, must be Hamming-optimal.*

Proof. A self-dual code of length 17 with minimum Lee weight 8 must have minimum Hamming weight 4 by the above lemma. For lengths 21 through 23, we recall, as remarked in the proof of Theorem 2, that a self-dual code with minimum Hamming weight 4 must be Hamming-optimal, by linear programming. □

Theorem 6. *The optimal Lee weight of a self-dual code of length* 18 *through* 24 *is* $8, 6, 8, 8, 8, 10,$ *and* 12, *respectively. A self-dual code of length* 21 *or* 22 *is Lee-optimal if and only if it is Hamming-optimal.*

Proof. At length 18, for instance, a self-dual code with Lee weight greater than 8 would have to have Hamming weight at least 5. But this is impossible by Theorem 2. The same argument applies for lengths 19 and 20. For length 21 and 22, the Euclidean norm is bounded above by 8 (this follows from the general bound in [12]), which bounds the Lee weight above by 8. The bound for length 23 and 24 follows from the fact that shortening reduces the minimal Lee weight by at most 2.

For length 18, the codes in Fig. 1 show that Lee weight 8 is attainable.

For lengths 19 through 22, any self-dual code that reduces to a shortened Golay code will have the desired minimum Lee weight. At length 20, for instance, the number of ± 1's in a vector must be one of 0, 8, 12, or 16. In all but the first case, this already forces the Lee weight to be greater than 8. A vector without ± 1's, on the other hand, is in $C^{(2)}$; since $C^{(2)}$ has minimum weight 4, such a vector has Lee weight at least 8.

At length 24, the extended $\mathbb{Z}_4$ quadratic residue code, also known as the Hensel-lifted Golay code, has Lee weight 12; shortening this code gives a code of length 23 and Lee weight 10. More examples are given in the following section. □

Theorem 7. *The optimum Lee weight of a self-dual* $\mathbb{Z}_4$ *code of length* 17 *is* 6.

Proof. By Corollary 5, any code of minimum Lee weight at least 8 must be Hamming-optimal. Of the 62 Hamming-optimal codes of length 17, none have Lee weight 8. There are, however, 17 such codes with Lee weight 6, including the code with generator matrix

$$\begin{pmatrix}
1&0&0&0&0&0&0&0&1&2&1&1&1&1&1&1&2\\
0&1&0&0&0&0&0&0&1&1&0&0&0&1&2&2&0\\
0&0&1&0&0&0&0&0&1&3&2&0&0&2&3&2&2\\
0&0&0&1&0&0&0&0&1&3&0&0&0&2&0&3&0\\
0&0&0&0&1&0&0&0&0&1&3&3&3&3&1&1&2\\
0&0&0&0&0&1&0&0&0&0&0&3&1&0&2&0&3\\
0&0&0&0&0&0&1&0&0&0&3&2&1&0&0&0&3\\
0&0&0&0&0&0&0&1&0&0&1&3&2&0&0&0&3\\
0&0&0&0&0&0&0&0&2&2&2&2&2&0&0&0&0
\end{pmatrix}. \quad \square$$

$$\begin{bmatrix}
100000001030330131\\
010000001131123122\\
001000001001002223\\
000100001110012331\\
000010001101131322\\
000001001000221003\\
000000101130312233\\
000000011101301130\\
000000002022022020\\
000000000222222222
\end{bmatrix}$$
$|\mathrm{Aut}| = 144$

$$\begin{bmatrix}
100000001012310113\\
010000001133121100\\
001000001001002223\\
000100001132032313\\
000010001101131322\\
000001001002223001\\
000000101112332211\\
000000011123303132\\
000000002022022020\\
000000000222222222
\end{bmatrix}$$
$|\mathrm{Aut}| = 48$

$$\begin{bmatrix}
100000001030330131\\
010000001133121100\\
001000001021222203\\
000100001130030313\\
000010001101131322\\
000001001000221003\\
000000101130312233\\
000000011123303132\\
000000002022022020\\
000000000222222222
\end{bmatrix}$$
$|\mathrm{Aut}| = 48$

$$\begin{bmatrix}
100000001030330131\\
010000001131123122\\
001000001021222203\\
000100001130030313\\
000010001101131322\\
000001001000221003\\
000000101130312233\\
000000011101301130\\
000000002022022020\\
000000000222222222
\end{bmatrix}$$
$|\mathrm{Aut}| = 48$

$$\begin{bmatrix}
100000001012310113\\
010000001133121100\\
001000001003220021\\
000100001130030313\\
000010001121113300\\
000001001002023201\\
000000101110330211\\
000000011123303132\\
000000002022022020\\
000000000222222222
\end{bmatrix}$$
$|\mathrm{Aut}| = 36$

$$\begin{bmatrix}
100000001012310113\\
010000001111101122\\
001000001003220021\\
000100001130030313\\
000010001103133322\\
000001001020001223\\
000000101110330211\\
000000011101323110\\
000000002022022020\\
000000000222222222
\end{bmatrix}$$
$|\mathrm{Aut}| = 36$

$$\begin{bmatrix}
100000001012310113\\
010000001133121100\\
001000001021222203\\
000100001112010331\\
000010001101131322\\
000001001002223001\\
000000101112332211\\
000000011123303132\\
000000002022022020\\
000000000222222222
\end{bmatrix}$$
$|\mathrm{Aut}| = 24$

Fig. 1. Self-dual codes of length 18 and minimal Lee weight 8.

Similarly, by examining the Hamming-optimal codes of length 18, 21, and 22, we find:

Theorem 8. *There are precisely* 7 *Lee-optimal codes of length* 18, *and precisely* 384 *Lee-optimal codes of length* 21. *There are at least* 19 368 *Lee-optimal codes of length* 22.

It is worth noting that the 7 codes of length 18 all have the same symmetrized weight enumerator; indeed, the constraint that the code is both Lee-optimal and Hamming-

optimal is enough to determine the symmetrized weight enumerator. There are one code with automorphism group of order 144, three with automorphism group of order 48, two with automorphism group of order 36, and one with automorphism group of order 24. These codes are listed in Fig. 1.

The main obstacle to extending Theorem 8 to lengths 19 and 20 is that the residue codes in those cases are no longer unique; it will be necessary to classify these first.

4. Length 23 and 24

Of particular interest are Lee-optimal codes of length 24, especially since such codes can be used to produce 5-designs [1].

Theorem 9. *If C is a self-dual $\mathbb{Z}_4$ code of length* 24, *with minimum Lee weight* 12, *then C has minimum Hamming weight* 8, *and minimum Euclidean norm* 16. *Furthermore, C is Type II; that is, the norm of any vector in C must be a multiple of* 8.

Proof. We have already seen that such a code must be Hamming-optimal. Applying the resulting constraints, together with the minimum Lee weight constraints, to the symmetrized weight enumerator leaves a one-parameter family, of which precisely one member has nonnegative coefficients in both itself and its shadow. The remaining claims follow by examination of this weight enumerator. □

For conciseness, we will call such a code a 'pseudo-Golay' code. The above theorem implies that any pseudo-Golay code lies between the Golay code and the Leech lattice, in that it reduces modulo 2 to the Golay code, and extends (via 'Construction A_4') to the Leech lattice. It is therefore somewhat shocking to find (as we will soon see) that not only is such a code not unique, but, in fact, there exists one such code with only 6 automorphisms!

If we try to classify these codes directly, as lifts of the Golay code, we run into the slight problem that there are over 100 million Hamming-optimal codes. Admittedly, the situation is not quite that dire, since all norms must be a multiple of 8. This constraint (which is linear on lift space) reduces the affine space from 55-dimensional to 44-dimensional. There would still be at least 71 857 codes to consider, however. If we insist that the code have certain automorphisms, the problem becomes tractable. By examining the possible permutations of order 3, 4, 5, 7, 11, and 23 (recall that the automorphism must reduce to an element of the automorphism group of the Golay code (the Mathieu group M_{24}), so there are only 9 possibilities), we obtain a list of 13 candidates, with automorphism groups of order 12 144 ($SL_2(23)$; the extended $\mathbb{Z}_4$ quadratic residue code), 336 ($SL_2(7)$), 48, 48, 48, 48, 44, 44, 28, 24, 16, 16, and 6. Five of these (the ones with automorphisms of order 7, 11, or 23) are precisely the codes $\mathscr{C}_1 \simeq \mathscr{C}_6$, $\mathscr{C}_5$, $\mathscr{C}_7$, $\mathscr{C}_9$, and $\mathscr{C}_{12}$ of [9], and one of the codes with

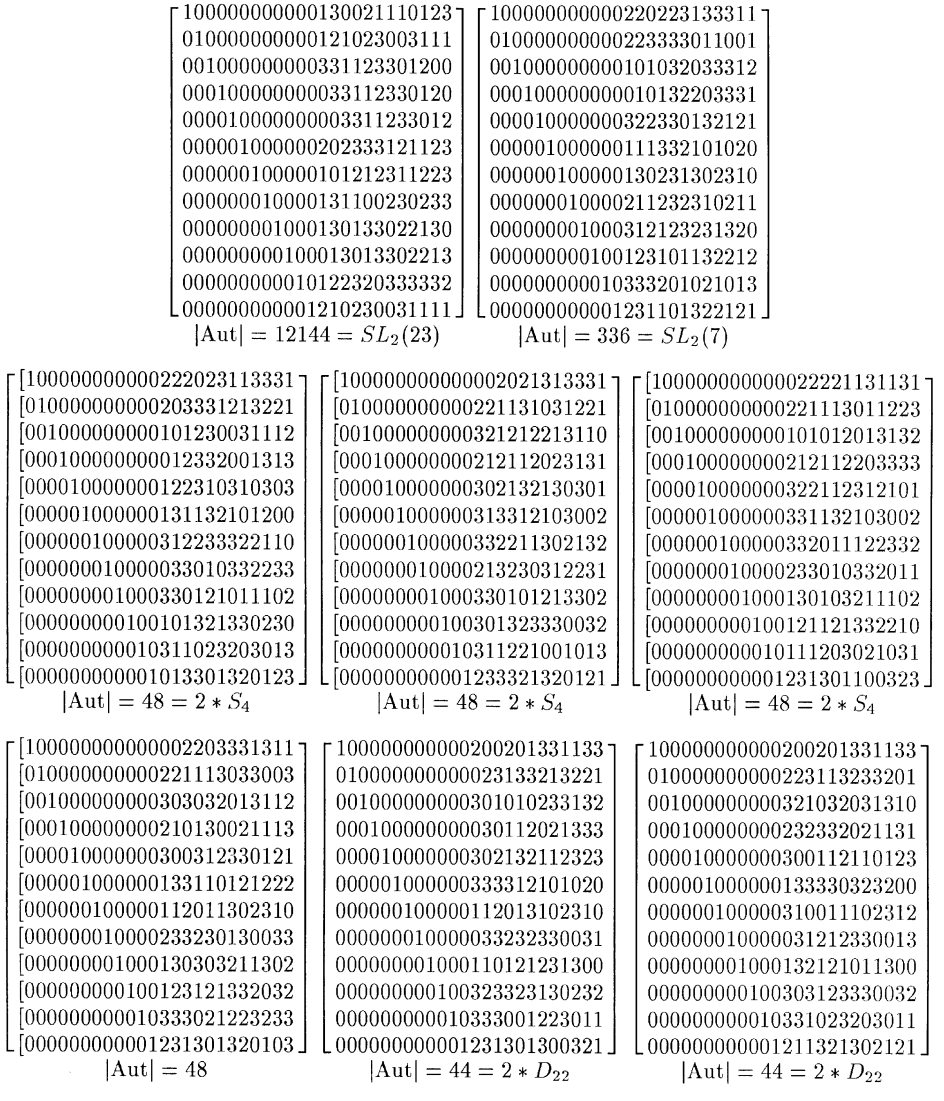

Fig. 2. Self-dual codes of length 24 and minimal Lee weight 12.

automorphism group of order 16 appeared in [8]. The remaining 7 codes are new. Fig. 2 gives generator matrices and automorphism group orders for each of the 13 codes.

To compute the automorphism groups, and to verify inequivalence, we could work entirely within the space of lifts of the Golay code. This approach tends to be rather cumbersome, however. A more feasible approach is to consider the images of the 12 144 vectors of Lee weight 12 under the Gray map ($0 \to 00$, $1 \to 01$, $2 \to 11$, and $3 \to 10$). One can then ask `magma` for the automorphism group of the resulting inci-

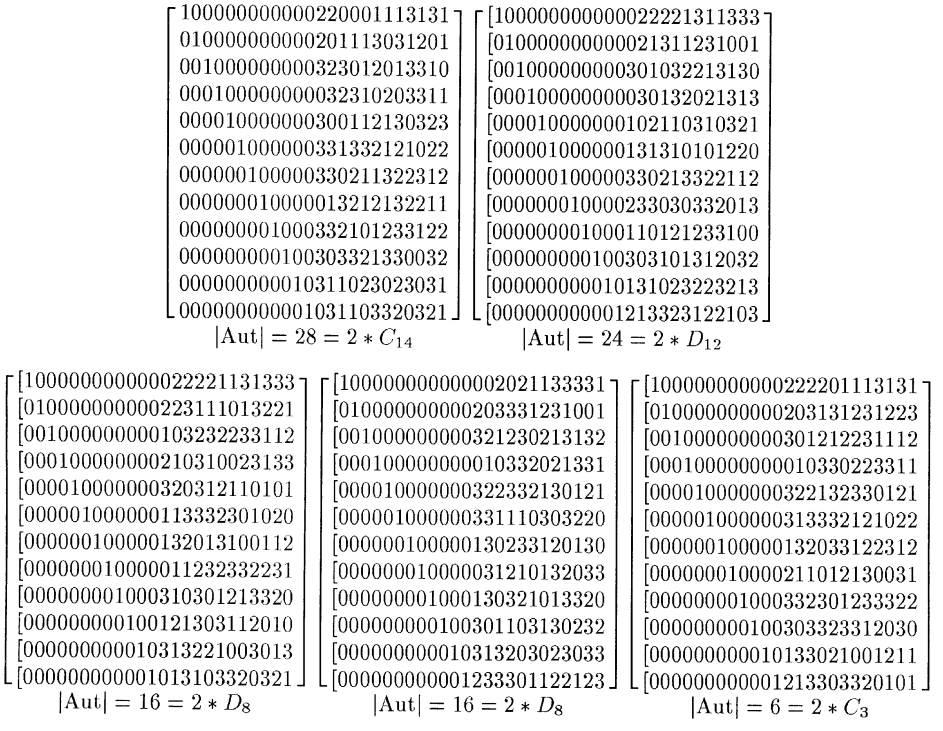

Fig. 2. Continued.

dence structure, or whether two such structures are equivalent. If desired, one could also check that the equivalence respects the column-pairing, but in this case, that check is unnecessary; paired columns hit a different number of blocks than unpaired columns. Thus we can check that these 13 codes are indeed inequivalent, and that their automorphism groups are as specified. (The mass formula below shows that all equivalences and automorphisms were indeed found; otherwise, the mass would have been overestimated.)

It remains to show that these 13 codes are the only possibilities. To show this, we will first consider the set of all codes of length 21 that could be obtained by shortening three columns of a pseudo-Golay code.

Theorem 10. *If C is a code of length* 21 *that occurs as a shortened pseudo-Golay code, then C reduces mod* 2 *to the shortened Golay code of length* 21, *and lifts to a lattice with kissing number* 84. *Similarly, at length* 22, *the code reduces to the shortened Golay code, and lifts to a lattice with kissing number* 44.

Proof. We consider length 21; length 22 is analogous. The code $C^{(2)}$ is clearly a punctured Golay code, so its dual must therefore be the shortened Golay code. For

the kissing number, we note that we can compute the *average* kissing number of all possible shortenings of a given pseudo-Golay code from its symmetrized weight enumerator, which, as we have seen, is uniquely determined. To wit, if we apply the operation $(\frac{d}{dx}+\frac{d}{dz})^3$ to the symmetrized weight enumerator (where the variables of the symmetrized weight enumerator are x, y, and z as usual), then divide by $24\cdot23\cdot22$, we obtain the average of the symmetrized weight enumerator over all shortenings. (Consider the action of $(\frac{d}{dx}+\frac{d}{dz})^3$ on the monomial associated to a given vector.) We find that the average kissing number is thus 84. But this is the smallest possible kissing number of a lattice of dimension 21. □

Remark. This also follows easily from the 5-design result of [1].

Similarly, at length 19 and 20, the kissing number must be 152 and 120, but we will not have occasion to use this in the sequel.

Of the 384 Hamming-optimal codes of length 21, only 80 have kissing number 84. For each of these 80 codes, we can then enumerate all possible ways (ignoring equivalence) to extend them to length 24. To be precise, for each of the three deleted columns, there are 512 ways to extend to a code of length 22, of which most will typically fail to have kissing number 44. Of the triples of such extensions, most will fail to satisfy the norm-divisibility criterion; for each of the survivors, there are precisely two ways to complete the extension. Thus we can obtain a list of 2556 codes that contains at least one representative of each equivalence class.

At this point, we could explicitly verify that each of those codes is equivalent to one from our list. However, there is a shortcut. Clearly, the number of distinct extensions of a given code of length 21 depends only on the equivalence class of the code; consequently, the number of codes that extend a given class is equal to the product of the size of the class and the number of extensions of one particular member of the class (which we computed in the previous paragraph). Summing over all 80 classes, we find that there are 245 260 800 distinct pseudo-Golay codes, modulo column negation. But then

$$\sum_C \frac{2}{|\mathrm{Aut}(C)|} = \frac{245260800}{|M_{24}|} = 10645/10626,$$

where the sum is over inequivalent pseudo-Golay codes. (The additional factor of 2 comes from the fact that global negation acts trivially on lift space.) We can immediately conclude that our list is complete.

We can also easily derive a classification of Lee-optimal codes of length 23. Any self-dual code of length 23 extends uniquely to a code of length 24 with all norms divisible by 8. By examining the weight enumerators of a Lee-optimal code of length 23 and its shadow, we find that such a code must extend to a pseudo-Golay code. Thus we obtain one equivalence class of 'shorter pseudo-Golay' codes for each orbit of columns under the automorphism group of each pseudo-Golay code. We readily compute that there are 30 such codes.

In summary:

Theorem 11. *There are* 13 *self-dual codes of length* 24 *over* $\mathbb{Z}_4$ *with minimum Lee weight* 12, *given in Fig.* 2. *There are* 30 *self-dual codes of length* 23 *over* $\mathbb{Z}_4$ *with minimum Lee weight* 10.

It is worth commenting on the structure of the pseudo-Golay codes with large automorphism groups. The code with group $SL_2(23)$ is, of course, simply the extended $\mathbb{Z}_4$ quadratic residue code. We can also give the structure of the code with group $SL_2(7)$ (the code appeared in [8,9], but neither reference gives any structural information). To construct this code, we label the 24 columns by

$$(1,0)(i,1)(2,0)(2i,2)(4,0)(4i,4),$$

where the labels lie in $GF(7)^2$, and i in each case ranges from 0 to 6. Then $SL_2(7)$ acts in the obvious way, except that if the resulting vector is not a valid label, we negate both the vector and the column. For instance, the matrix

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

takes $(0,1)$ to $(-1,0)$, which is not a valid label. So we move the column labelled $(0,1)$ into the column labelled $(1,0)$, then negate it. We find that there are precisely 12 self-dual codes having this automorphism group; the action of $GL_2(7)$ permutes these among themselves, leaving 2 orbits. A representative of the first orbit is generated by the images of the two vectors

$$[11111111\ 22222222\ 11111111], [13121000\ 13121000\ 13121000]$$

under $SL_2(7)$. This code, unfortunately, contains the vector

$$[00000000\ 00000000\ 11111111]$$

of Lee weight 8. However, the other orbit, with representative generated by the images of

$$[31111111\ 22222222\ 31111111], [13121000\ 13121000\ 13121000],$$

has minimum Lee weight 12, as desired. In both cases, the second generator essentially produces a quadratic residue code, while the first generator produces a 'triple sextic residue code' [2].

References

[1] A. Bonnecaze, E.M. Rains, P. Solé, $\mathbb{Z}_4$ codes and 5-designs, Preprint.
[2] R. Chapman, Higher power residue codes, Finite fields Appl. 3 (1997) 353–369.
[3] J.H. Conway, N.J.A. Sloane, A new upper bound on the minimal distance of self-dual codes, IEEE Trans. Inform. Theory 36 (6) (1990).

[4] J.H. Conway, N.J.A. Sloane, Self-dual codes over the integers modulo 4, J. Combin. Theory, Ser. A 62 (1) (1993) 30–45.
[5] S.T. Dougherty, M. Harada, P. Solé, Shadow codes over $\mathbb{Z}_4$, Finite fields and applications, to appear.
[6] J. Fields, P. Gaborit, J. Leon, V. Pless, All self-dual $\mathbb{Z}_4$ codes of length 15 or less are known, IEEE Trans. Inform. Theory 44 (1998) 311–322.
[7] P. Gaborit, Mass formulas for self-dual codes over $\mathbb{Z}_4$ and $\mathbb{F}_q + u\mathbb{F}_q$ rings, IEEE Trans. Inform. Theory 42 (1996) 1222–1228.
[8] P. Gaborit, M. Harada, Construction of extremal type II codes over $\mathbb{Z}_4$, Design, codes and cryptography, to appear.
[9] W. Cary Huffman, Decompositions and extremal type II codes over $\mathbb{Z}_4$, IEEE Trans. Inform. Theory 44 (1998) 800–809.
[10] V. Pless, J.S. Leon, J. Fields, All $\mathbb{Z}_4$ codes of Type II and length 16 are known, J. Combin. Theory, Ser. A 78 (1997) 32–50.
[11] E.M. Rains, N.J.A. Sloane, Self-dual codes, in: V.S. Pless, W.C. Huffman, R.A. Brualdi (Eds.), Handbook of Coding Theory (Elsevier, Amsterdam, 1998).
[12] E.M. Rains, N.J.A. Sloane, The shadow theory of modular and unimodular lattices, J. Number Theory, to appear.