Quaternary Constructions for the Binary Single-Error-Correcting Codes of Julin, Best and Others

J. H. Conway

Mathematics Department
Princeton University
Princeton, NJ 08544

N. J. A. Sloane

Mathematical Science Research Center
AT&T Bell Laboratories
Murray Hill, NJ 07974

February 22, 1993

ABSTRACT

Certain nonlinear binary single-error-correcting codes found by Julin, Best and others have simple descriptions as codes over the ring of integers modulo 4.

Quaternary Constructions for the Binary Single-Error-Correcting Codes of Julin, Best and Others

J. H. Conway

Mathematics Department
Princeton University
Princeton, NJ 08544

N. J. A. Sloane

Mathematical Science Research Center
AT&T Bell Laboratories
Murray Hill, NJ 07974

1. Introduction

It has recently been shown ([4], [8], [10]) that the nonlinear binary codes found by Nordstrom-Robinson, Kerdock, Preparata, Goethals, etc. have a simple description as linear codes over $\mathbb{Z}_4$, the ring of integers modulo 4 (although this requires a slight modification of the Preparata and Goethals codes). The Nordstrom-Robinson and Preparata codes have minimal distance $d = 6$ and the Goethals codes have $d = 8$. In this note we consider codes with $d = 4$.

The following are the best lower bounds presently known for $A(n, 4)$, the maximal number of words in a binary code of length n with $d = 4$. This table is taken from [3] and [7], p. 248, which also gives upper bounds.

n	6	7	8	9	10	11	12
$A(n,4) \geq$	4^*	8^*	16^*	$20^{*\S}$	$40^{*\S}$	$72^{\S}$	$144^{\S}$
type	H	H	H	J	B	J	J
n	13	14	15	16	17	18	19
$A(n,4) \geq$	256^*	512^*	1024^*	2048^*	2720	5248	10496
type	H	H	H	H	R	HH	HH
n	20	21	22	23	24		
$A(n,4) \geq$	$20480^{\S}$	$36864^{\S}$	$73728^{\S}$	$147456^{\S}$	$294912^{\S}$		
type	U	U	U	U	U		

Here $*$ indicates that this is the exact value of $A(n, 4)$, H denotes a Hamming or shortened

Hamming code, and J, B, R, HH, U refer respectively to Julin [11], Best [1], [2], Romanov [15], Hämäläinen [9] and the $(u, u+v)$ construction of Sloane and Whitehead ([16]; [13, Chap. 2]).

In this paper we give simpler, quaternary constructions for codes corresponding to the entries marked §. Since the number of words in these codes is not a power of 2, these are nonlinear quaternary codes. However, these nonlinear quaternary codes, especially those of lengths 5 and 6, have a rich and interesting structure. (The codes of Romanov and Hämäläinen do not have any apparent $\mathbb{Z}_4$ structure.)

As in [4], [8], [10] we construct binary codes from codes over $\mathbb{Z}_4 = \{0,1,2,3\}$ by using the map

$$\phi: \ 0 \mapsto 00, \ \ 1 \mapsto 01, \ \ 2 \mapsto 11, \ \ 3 \mapsto 10 \ .$$

More formally, we define maps α, β, γ: $\mathbb{Z}_4 \to \mathbb{Z}_2$ by

$\mathbb{Z}_4$	α	β	γ
0	0	0	0
1	1	0	1
2	0	1	1
3	1	1	0 ,

extend them in the obvious way to maps from $\mathbb{Z}_4^n$ to $\mathbb{Z}_2^{2n}$, and define $\phi : \mathbb{Z}_4^n \to \mathbb{Z}_2^{2n}$ by

$$\phi(u) = (\beta(u), \gamma(u)) \ . \tag{1}$$

The map ϕ is an isometry from ($\mathbb{Z}_4^n$, Lee distance) to ($\mathbb{Z}_2^{2n}$, Hamming distance). See [10] for details.

Notation. $(n, M, d)_q$ denotes a code of length n, containing M codewords at Lee distance at least d apart, over an alphabet of size q. Two such codes are equivalent if one can be obtained from the other by a permutation of the n coordinates followed by a Lee-distance preserving permutation of the q symbols in each coordinate (possibly using a different permutation in each coordinate). The automorphism group of the code consists of the set of all such operations that fix the code as a whole.

2. Best's code of length 10

A $(10, 40, 4)_2$ code was found by Best [1], [2], and has been shown to be unique by Litsyn and Vardy [12]. In this section we give a simple quaternary construction for this code.

The construction

Theorem 1. *Let $\mathcal{B}_0$ be the $(5,40,4)_4$ code consisting of the vectors*

$$(c-d, b, c, d, b+c), \quad b, c, d \in \{+1, -1\} , \tag{2}$$

and all of their cyclic shifts. Then the binary image of $\mathcal{B}_0$ under the map ϕ is equivalent to Best's $(10,40,4)_2$ code described in [1]; [2]; [7], p. 140.

Proof. The map from $(v_1, \ldots, v_{10})$ to

$$(\phi^{-1}(v_9, v_4),\ \phi^{-1}(v_7, v_2),\ \phi^{-1}(v_5, v_{10}),\ \phi^{-1}(v_3, v_8),\ \phi^{-1}(v_1, v_6))$$

takes Best's code to ours. ∎

We call $\mathcal{B}_0$ the *pentacode*. It consists of all cyclic shifts and negations of the four vectors

$$01112,\ 03110,\ 21310,\ 21132\ . \tag{3}$$

If we denote the i^{th} cyclic shift of (2) by v_{bcdi} $(0 \le i \le 4)$, then $\mathcal{B}_0$ is almost a 'systematic' code: that is, the values of b, c, d, i can be read off v_{bcdi}.

The automorphism group. The automorphism group of $\mathcal{B}_0$ is generated by

$$\begin{aligned}
\rho_{-1}:&\ (a,b,c,d,e) &\mapsto&\ (-a,-b,-c,-d,-e)\ ,\\
\rho_c:&\ (a,b,c,d,e) &\mapsto&\ (-a, 2-b, c, 2-d, -e)\ ,\\
\sigma:&\ (a,b,c,d,e) &\mapsto&\ (b,c,d,e,a)\ ,\\
\tau^2:&\ (a,b,c,d,e) &\mapsto&\ (2+e, 2+d, 2+c, 2+b, 2+a)\ .
\end{aligned}$$

The elements ρ_{-1}, ρ_c, $\rho_d = (\rho_c)^\sigma$, $\rho_e = (\rho_d)^\sigma$, $\rho_a = (\rho_e)^\sigma$, $\rho_b = (\rho_a)^\sigma$ generate an elementary abelian group of type 2^5 (note that $\rho_a\rho_b\rho_c\rho_d\rho_e = 1$); σ and τ^2 generate a dihedral group D_{10} of order 10; and the full group $G = \mathrm{Aut}(\mathcal{B}_0)$ is a semidirect product $2^5 : D_{10}$ of order 320. This is also the full automorphism group of the binary code, as found by Best. Best's description of the group in [2] is more complicated, however. (In his second generator, β, the bar over the 9 should be omitted.)

The elements ρ_b, ρ_c, ρ_d permute the words shown in (3), and so the group is transitive on codewords. This establishes that $\mathcal{B}_0$ (and hence also its binary image) is distance invariant. The weight enumerator of the binary code is

$$X^{10} + 22X^6Y^4 + 12X^4Y^6 + 5X^2Y^8\ . \tag{4}$$

Distances of vectors from the code, and the four pentacodes. We next classify the quaternary vectors of length 5 under the action of G. It is simpler to consider first the smaller group $H = 2^4 : D_{10}$, of order 160, obtained by omitting the generator ρ_{-1}. It turns out that H actually preserves four copies of the pentacode. We denote these by $\mathcal{B}_0$, $\mathcal{B}_1$, $\mathcal{B}_2$, $\mathcal{B}_3$ and display them in Table 1.

Table 1: The i^{th} pentacode $\mathcal{B}_i$ consists of all cyclic shifts of the eight words shown.

$\mathcal{B}_0$	$\mathcal{B}_1$	$\mathcal{B}_2$	$\mathcal{B}_3$
01112	01030	21110	03010
21132	01012	01130	03032
21310	03210	01312	01230
01330	03232	21332	01212
03110	23030	23112	21010
23130	23012	03132	21032
23312	21210	03310	23230
03332	21232	23330	23212

The twelve orbits of H on $\mathbb{Z}_4^5$ are described in Table 2. Four orbits are the pentacodes $\mathcal{B}_0, \ldots, \mathcal{B}_3$. The orbit that contains any other vector is determined by the parities of its five digits. In Table 2 the pentacodes are indicated by their leading words and the other orbits by the parities (using d = odd, e = even) of their vectors, up to cyclic shifts. The columns headed D give the distance of the H-orbit from $\mathcal{B}_0$, and N is the size of the orbit. The arrows indicate the action of the map τ defined by

$$\tau : \ (a, b, c, d, e) \mapsto (1 + d, 1 + a, 1 + c, 1 + e, 1 + b) \ .$$

(Note that τ is not in G.) The map ρ_{-1} fixes ten of the twelve orbits, but interchanges the pentacodes $\mathcal{B}_1$ and $\mathcal{B}_3$ (represented by the vectors 01030 and 03010 in the table). Modulo H, τ and ρ_{-1} generate a dihedral group of order 8 that permutes the four pentacodes.

We see from the table that there are 40 vectors in the code $\mathcal{B}_0$, 400 vectors at distance 1 from it, 472 vectors at distance 2 from it, and 112 vectors at distance 3. The covering radius of $\mathcal{B}_0$ (and of its binary image the $(10, 40, 4)_2$ code) is therefore 3.

The orbits of the group G itself on $\mathbb{Z}_4^5$ are as follows. Since $G = \langle H, \rho_{-1} \rangle$, we see from Table 2 that $\mathcal{B}_1$ and $\mathcal{B}_3$ (which are interchanged by ρ_{-1}) fuse into a single orbit under G. The other H-orbits, being fixed by ρ_{-1}, are also G-orbits.

Table 2: Orbits of H on vectors of $\mathbb{Z}_4^5$.

D	N	vectors	action of τ	vectors	N	D
0	40	01112	$\longleftrightarrow$	01030	40	1
2	40	21110	$\longleftrightarrow$	03010	40	1
2	160	$eedee$	$\longleftrightarrow$	$ddedd$	160	1
2	160	$deded$	$\longleftrightarrow$	$deeed$	160	1
2	80	$eddde$	$\longleftrightarrow$	$edede$	80	3
2	32	$ddddd$	$\longleftrightarrow$	$eeeee$	32	3

A decoding algorithm. The covering radius of the $(10, 40, 4)_2$ code is 3. The following is a complete decoding algorithm for this code. We describe it in the $\mathbb{Z}_4$ domain as a decoding algorithm for the pentacode $\mathcal{B}_0$ that corrects any error pattern of Lee weight 1, and detects all error patterns of Lee weight 2 and some of Lee weight 3.

We denote the received vector by

$$v = (v_0, v_1, v_2, v_3, v_4) \in \mathbb{Z}_4^5 ,$$

let $w = (w_0, \ldots, w_4) = \alpha(v)$, and let $W = 5 - wt(w)$.

1. If $W = 0$ or 4, or $W = 2$ and $w_i = w_{i+2} = 0$ (subscripts mod 5), decide that an error pattern of Lee weight 2 occurred.

2. Suppose $W = 1$, say $w_i = 0$. If $v_i = v_{i+2} + v_{i-2}$, decide that a single error of $v_{i+1} + v_{i-1} - v_{i-2}$ occurred at position $i+1$. Otherwise, a single error of $-v_{i+1} + v_{i-1} - v_{i+2}$ occurred at position $i-1$.

3. Suppose $W = 2$ and $w_i = w_{i+1} = 0$. If $v_{i+1} = v_{i-2} - v_{i-1}$ and $v_i = v_{i+2} + v_{i-2}$, decide that no errors occurred; otherwise decide that an error pattern of weight 2 occurred.

4. Suppose $W = 3$ and $w_i = w_{i+1} = 1$. If $v_{i-2} = v_i + v_{i+1}$, decide that a single error of $v_{i-1} - v_{i+1} + v_{i+2}$ occurred at position $i+2$. Otherwise a single error of $v_{i-1} + v_i - v_{i+2}$ occurred at position $i-1$.

5. Suppose $W = 3$ and $w_i = w_{i+2} = 1$. If $-v_{i-1} + v_{i+1} - v_{i+2} = -v_{i-2} + v_i + v_{i+1} = \epsilon$ (say), decide that a single error of ϵ occurred at position $i+1$. Otherwise decide that an error pattern of Lee weight 3 occurred.

6. If $W = 5$, decide that an error pattern of Lee weight 3 occurred.

We omit the straightforward verification that the algorithm is correct.

A code of length 9. The vectors $\{(a,b,c,d) : (a,b,c,d,e) \in \mathcal{B}_0,\ e = 0 \text{ or } 1\}$ form a $(4,20,3)_4$ code over $\mathbb{Z}_4$ whose binary image is an $(8,20,3)_2$ code. By adding an overall parity check we obtain a $(9,20,4)_2$ code, with the same parameters as Julin's code [11].

The 10-dimensional packing. The densest sphere-packing presently known in ten dimensions, P_{10c}, is obtained by applying Construction A to the $(10,40,4)_2$ binary code (see [7, Table 1.2 and Chap. 5]). This packing may be obtained directly from the pentacode by the following simple construction.

Let L denote the (two-dimensional) square lattice I_2. We associate the four cosets of $2L$ in L with the elements of $\mathbb{Z}_4$ by

$$(0,0)+2L \mapsto 0,\ (0,1)+2L \mapsto 1,\ \ (1,1)+2L \mapsto 2,\ \ (1,0)+2L \mapsto 3\ .$$

Note that the minimal norm (i.e. squared length) in a coset of $L/2L$ agrees with the Lee weight of the associated element of $\mathbb{Z}_4$. In this way we obtain a map

$$\pi :\ L \rightarrow L/2L \rightarrow \mathbb{Z}_4$$

as shown in Fig. 1. We extend this in the obvious way to a map from L^n to $\mathbb{Z}_4^n$.

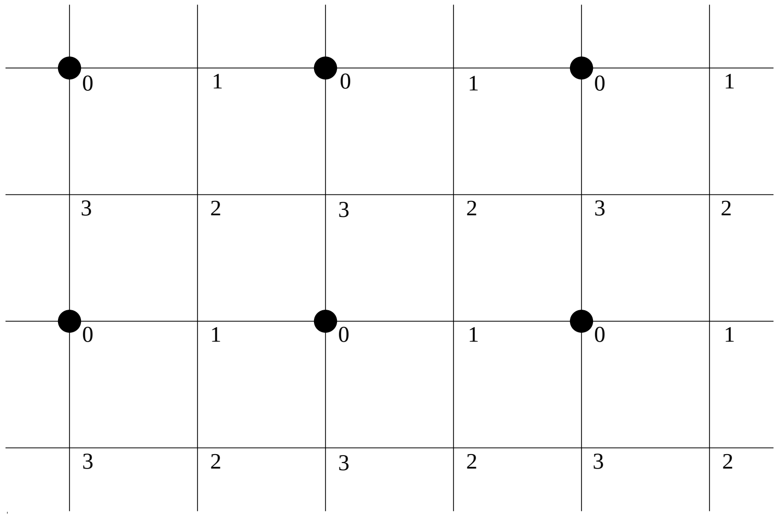


Figure 1: Square lattice L labeled by elements of $\mathbb{Z}_4$.

Theorem 2. *If C is an $(n,M,d)_4$ code over $\mathbb{Z}_4$, define*

$$\Lambda(C) := \{x = (x_1,\ldots,x_n) \in L^n :\ \pi(x) \in C\}\ .$$

The $2n$-dimensional packing corresponding to $\Lambda(C)$ has minimal norm $\mu = \min\{d, 4\}$ and center density

$$\delta = M\left(\frac{\mu}{4}\right)^n \ .$$

We omit the proof. This is similar to the construction of sphere packings from nonbinary codes given in [7, Chap. 7] and [5]. We mention in passing that L can be identified with the Gaussian integers $\mathbb{Z}[i]$, and then $\Lambda(C)$ is a subset of $\mathbb{Z}[i]^n$. If C is a linear code over $\mathbb{Z}_4$ then $\Lambda(C)$ is a lattice over the Gaussian integers, i.e. a $\mathbb{Z}[i]$-module.

Taking C to be the pentacode $\mathcal{B}_0$, we obtain Best's packing P_{10c} of center density $\delta = 5/128$. This packing looks most symmetrical when viewed from the origin (which is not a point of P_{10c}). The full subgroup of the real 10-dimensional orthogonal group that fixes the origin and takes P_{10c} to itself is generated by all 2^{10} sign-changes, and by the $2^5 \times 10$ symmetries of the code. This is a group P of structure $2^{10} : (2^5 : D_{10})$ and order 327680. (The stabilizer of a point of P_{10c} has size only one-fortieth of this.) This can be proved by using parity considerations to show that the only translations that preserve the packing are those by vectors with even integer coordinates — these translations extend P to give the full space group of P_{10c}.

3. Best's codes of length 11 and 12

In 1965 Julin ([11]; [13, Chap. 2]) constructed several $(12, 144, 4)_2$ codes from the Steiner system $S(5, 6, 12)$, which we will describe in more detail in Section 4. The situation here is less satisfactory than at length 10, for a number of reasons: it is not known whether 144 words is optimal, several different 144-word codes are known, and none of them are distance invariant. In fact, in 1978 Best [1] found further examples of $(12, 144, 4)_2$ codes. However, Best conjectured that $A(12, 4) = 144$, and the present authors concur.

In this section we give a quaternary construction for the most interesting of Best's $(12, 144, 4)_2$ codes. Unlike Julin's code, this contains a $(10, 40, 4)_2$ code as a subcode. It does not contain a Steiner system $S(5, 6, 12)$. This code is described in the report [1], but not in the published version [2].

We first give a concise definition of this code via its group, and then list the codewords in full.

The maps $\rho_{-1}, \rho_a, \ldots, \rho_e$ were defined in Section 2 to act on vectors in $\mathbb{Z}_4^5$. We extend them to act on $(a, b, c, d, e, f) \in \mathbb{Z}_4^6$ by fixing f.

The automorphism group of the code is the group K of order 128 generated by

$$\rho_{-a} = \rho_{-1}\rho_a,\ \rho_b,\ \rho_c,\ \rho_d,\ \rho_{-e} = \rho_{-1}\rho_e\ ,$$

together with the operations that take $(a,b,c,d,e,f) \in \mathbb{Z}_4^6$ to

$$\begin{array}{llllll}
(\ 2+a, & 2+b, & 2+c, & 2+d, & 2+e, & 2+f\ )\ , \\
(\ \ -e, & -d, & -c, & -b, & -a, & 2-f\ )\ , \\
(\ d+1, & e+1, & f+1, & a-1, & b-1, & c-1\ )\ .
\end{array}$$

(The maps ρ_{-1}, ρ_a and ρ_e are not in this group.)

Theorem 3. *Let $\mathcal{C}$ be the $(6,144,4)_4$ code consisting of the vectors*

$$010301, \quad 011100, \quad 100110, \quad 300101, \quad 333000$$

and their images under K. These have respectively

$$16, \qquad 16, \qquad 64, \qquad 32, \qquad 16$$

images. Then the binary image of $\mathcal{C}$ under the map ϕ is equivalent to Best's $(12,144,4)_2$ code described in [1].

We omit the proof.

We can give a compact listing of the codewords of $\mathcal{C}$ as follows. Let $\mathcal{B}_0'$ denote the $(5,32,4)_4$ code displayed in Table 3. (Speaking informally, this is a twisted version of the pentacode with eight words left off.) The words in any column of Table 3 all have the same parity.

Table 3: The $(5,32,4)_4$ code $\mathcal{B}_0'$ used to build the $(6,144,4)_4$ code $\mathcal{C}$.

01110	00313	10011	11221	33300
21112	02311	12213	11023	11302
01132	20331	12031	13201	13320
21130	22333	10233	13003	31322
03112		30211	31001	
23110		32013	31203	
03130		32231	33021	
23132		30033	33223	

Then the $(6,144,4)_4$ code $\mathcal{C}$ consists of all the words

$$(a_i, b_i, c_i, d_i, e_i, i)\ , \quad i = 0,1,2,3\ ,$$

where $(a_0, \ldots, e_0) \in \mathcal{B}'_0$, $(a_1, \ldots, e_1) \in \mathcal{B}_1$, $(a_2, \ldots, e_2) \in \mathcal{B}'_2 = (2,2,2,2,2) + \mathcal{B}'_0$, and $(a_3, \ldots, e_3) \in \mathcal{B}_3 = (2,2,2,2,2) + \mathcal{B}_1$.

Furthermore, the vectors $\{(a,b,c,d,e) : (a,b,c,d,e,f) \in \mathcal{C},\ f = 0 \text{ or } 1\}$ form a $(5,72,3)_4$ code over $\mathbb{Z}_4$ whose binary image is a $(10,72,3)_2$ code. By adding an overall parity check we obtain an $(11,72,4)_4$ code. Similarly the vectors $\{(a,b,c,d,e) : (a,b,c,d,e,1) \in \mathcal{C}\}$ form the $(5,40,4)_4$ pentacode $\mathcal{B}_1$.

4. Julin's codes of length 12

The $(12,144,4)_2$ codes constructed by Julin ([11]; [13, Chap. 2]) in 1965 are formed by taking as words the 132 blocks of the Steiner system $S(5,6,12)$ and adjoining six words of weight 2 and six of weight 10. There are however several inequivalent ways to choose the words of weights 2 and 10 to adjoin to the Steiner system [7, Chap. 5].

In this section we give a quaternary construction for the Steiner system $S(5,6,12)$ and for a canonical version of Julin's code.

Theorem 4. *Let $\mathcal{J}$ be the $(6,144,4)_4$ code over $\mathbb{Z}_4$ consisting of all cyclic shifts and negations of the vectors*

$$\begin{array}{lllll} 001122, & 002211, & 010212, & 020121, & 012021, \\ 011332, & 012313, & 013123, & 013231, & 021133, \\ 311111, & 200000, & 022222\,. & & \end{array} \tag{5}$$

Then the binary image of $\mathcal{J}$ under ϕ forms a $(12,144,4)_2$ code. If the last two vectors are omitted from (5), the binary images form the blocks of a Steiner system $S(5,6,12)$.

Proof. Let $(v_\infty, v_0, v_1, v_4, v_2, v_3) \in \mathbb{Z}_4^6$ denote an arbitrary vector in $\mathcal{J}$. Then it is straightforward to verify that the permutations of the group $PGL_2(5)$ acting on $\{\infty, 0, 1, 2, 3, 4\}$ preserve this code. We can now refer to [6] (see the M_{12} entry) for the verification that the images of the first eleven vectors in (5) form a Steiner system $S(5,6,12)$. In fact this form of the Steiner system was discovered many years ago by S. P. Norton [14] when he constructed the Mathieu group M_{12} — which is the full automorphism group of $S(5,6,12)$ — from the group $PGL_2(5)$. This construction of M_{12} is also briefly mentioned in [7, Chap. 11, Sect. 17].

That the binary image of $\mathcal{J}$ has minimal distance 4 follows because (i) two blocks of the Steiner system cannot (by definition) meet in five places, and so must have Hamming distance at least 4 apart, and (ii) the words of weights 2 and 10 obtained from the last two vectors in (5) clearly are at distance at least 4 from each other and from the rest of the code. ■

Remarks

1. It is not difficult to show (we omit the details) that the full group of the binary code $\phi(\mathcal{J})$ is $2^2 \times PGL_2(5)$, of order 480. We have already seen how $PGL_2(5)$ acts, and the two symmetries of order 2 are negation of the $\mathbb{Z}_4$ words and complementation of the binary words.

2. $\mathcal{J}$ may be more concisely defined as the set of images of the vectors $(v_\infty, v_0, v_1, v_4, v_2, v_3) \in \{001122, 021133, 311111, 200000, 022222\}$ under negation and the action of $PGL_2(5)$.

We now discuss the sense in which $\mathcal{J}$ is unique. As already mentioned, there are many inequivalent $(12, 144, 4)_2$ codes. To limit the possibilities, we first restrict consideration to codes which contain the 132 blocks of the Steiner system $S(5, 6, 12)$ as a subcode. This forces the remaining twelve words to consist of six mutually disjoint words of weight 2 and six words of weight 10 whose complements are mutually disjoint. Any such code therefore defines two partitions of the twelve coordinates into six pairs. A third such partition is needed to specify how the coordinates are to be combined in pairs to produce a quaternary code.

It is reasonable to require that the first two partitions should agree, so that the words of weight 10 are the complements of those of weight 2. In an attempt to make the quaternary code have as many of the symmetries of the binary code as possible, we also insist that the third partition must coincide with the first two. So we shall define a quaternary Julin code to be a $(6, 144, 4)_4$ code whose binary image contains a Steiner system $S(5, 6, 12)$ and is such that the three partitions of the twelve coordinates into six pairs defined by the words of weight 2, the words of weight 10, and the $\mathbb{Z}_4$ structure all coincide.

Theorem 5. *There are precisely five inequivalent quaternary Julin codes. Just one, $\mathcal{J}$, is closed under negation.*

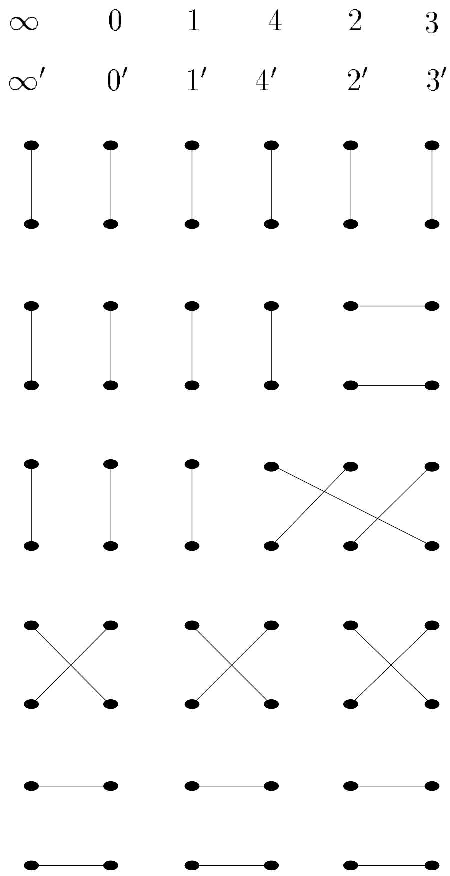
Proof. The full automorphism group of the Steiner system is the Mathieu group M_{12}. Modulo the action of this group one can show that there are exactly five ways to partition the coordinates into six pairs. Let the coordinates be labeled

$$\infty\ 0\ 1\ 4\ 2\ 3\ \infty'\ 0'\ 1'\ 4'\ 2'\ 3'\ ,$$

as in the above description of $\mathcal{J}$. Then the five partitions are shown in Table 1, together with the subgroup of M_{12} that fixes the partition. By using the six words of weight 2 defined by one of these partitions, together with their complements, we obtain the five codes, which we call the

(a) involutary, (b) duadic, (c) icosahedral,
(d) synthematic, (e) congruential

types.



	Partition	Stabilizer in M_{12}
(a)		$2 \times PSL_2(5)$, order 240
(b)		$2 \times D_8$, order 16
(c)		icosahedral, order 60
(d)		$2 \times S_4$, order 48
(e)		$4^2.\, D_{12}$, order 192

Table 4: Classification of partitions of twelve coordinates into six pairs under the action of the Mathieu group M_{12}.

Negation of the quaternary code corresponds to the permutation of type 2^6 defined by the partition of the twelve coordinates. This permutation is in M_{12} (and so preserves the words of weight 6) only for the involutary type. ■

12-dimensional packings. The code $\phi(\mathcal{J})$ is not distance invariant, and in fact four different distance distributions occur. In particular, the number of words at distance 4 from a given word is 35, 45, 47 or 49. This is also true for the duadic and synthematic types. But for the icosahedral and congruential types some codewords have 51 neighbors at distance 4, the maximal possible number [3]. The congruential type has the greatest number of words with this property.

Then 12 of the 144 codewords in the congruential code $\mathcal{J}'$ have 51 neighbors at Lee distance 4. Consequently the twelve-dimensional packing $\Lambda(\mathcal{J}')$ has the property that one-twelfth of its spheres have kissing number $2 \times 12 + 16 \times 51 = 840$ (cf. Eq. (4) of [7, p.138]). This is the highest kissing number known in twelve dimensions (Best [1], [2]; [7, Table 1.2]).

5. The $(u, u+v)$ construction and codes of length 20 to 24

The $(u, u+v)$ construction ([16], [13, Chap. 2]) is the following. Let $C_i (i = 1, 2)$ be an $(n, M_i, d_i)_2$ code. Then $C_3 = \{(u, u+v) : \ u \in C_1, \ v \in C_2\}$ is a $(2n, M_1M_2, \ \min\{2d_1, d_2\})_2$ code. Any code constructed in this way automatically has the structure of a quaternary code.

Theorem 6. *C_3 is the image under ϕ of the quaternary code consisting of all vectors $2u+v$, $u \in C_1$, $v \in C_2$ (regarding $\mathbb{Z}_2 = \{0, 1\}$ as a subset of $\mathbb{Z}_4$).*

Proof. For $u, v \in \mathbb{Z}_2^n$, we have the identity

$$\phi(2u + v) = (u, u + v) \ .$$

∎

In particular, taking C_1 to be an $(n, 2^{n-1}, 2)_2$ code and C_2 to be an $(n, M, d = 3 \text{ or } 4)_2$ code, where $10 \le n \le 12$, we obtain quaternary versions of the codes of lengths 20 through 24 mentioned in Section 1.

Of course the construction can be iterated to produce codes of lengths 32 to 48, and so on ([2], [13], [16]).

References

[1] M. R. Best, *Binary codes with minimum distance four*, Report ZW 112/78, Math. Centrum, Amsterdam, 1978.

[2] M. R. Best, *Binary codes with a minimum distance of four*, IEEE Trans. Inform. Theory, **26** (1980), 738–742.

[3] A. E. Brouwer, J. B. Shearer, N. J. A. Sloane and W. D. Smith, *A new table of constant weight codes*, IEEE Trans. Inform. Theory, **36** (1990), 1334–1380.

[4] A. R. Calderbank, A. R. Hammons, Jr., P. V. Kumar, N. J. A. Sloane and P. Solé, *A linear construction for certain Kerdock and Preparata codes*, Bull. Amer. Math. Soc., submitted.

[5] A. R. Calderbank and N. J. A. Sloane, *New trellis codes based on lattices and cosets*, IEEE Trans. Inform. Theory, **33** (1987), 177–195.

[6] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, *ATLAS of finite groups*, Oxford Univ. Press, 1985.

[7] J. H. Conway and N. J. A. Sloane, *Sphere-packings, lattices and groups*, 2nd ed., Springer-Verlag, NY 1992.

[8] G. D. Forney, Jr., N. J. A. Sloane and M. D. Trott, *The Nordstrom-Robinson code is the binary image of the octacode*, Proceedings DIMACS/IEEE Workshop on Coding and Quantization, 1993, to appear.

[9] H. Hämäläinen, *Two new binary codes with minimum distance three*, IEEE Trans. Inform. Theory, **34** (1988), 875.

[10] R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane and P. Solé, *The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and Related Codes*, preprint.

[11] D. Julin, *Two improved block codes*, IEEE Trans. Inform. Theory, **11** (1965), 459.

[12] S. N. Litsyn and A. Vardy, personal communication, January 1993.

[13] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*, North-Holland, Amsterdam, 1977.

[14] S. P. Norton, personal communication.

[15] A. M. Romanov, *New binary codes of minimal distance 3* (in Russian), Problemy Peredachi Informatsii, **19** (1983), 101–102.

[16] N. J. A. Sloane and D. S. Whitehead, *A new family of single-error correcting codes*, IEEE Trans. Inform. Theory, **16** (1970), 717–719.