The Nordstrom-Robinson Code is the Binary Image of the Octacode

G. David Forney, Jr.

Motorola Codex
Mansfield, MA 02048 USA

N. J. A. Sloane

Mathematical Sciences Research Center
AT&T Bell Laboratories
Murray Hill, New Jersey 07974 USA

Mitchell D. Trott

Department of Electrical Engineering and Computer Science
M. I. T.
Cambridge, MA 02139 USA

January 6, 1993

ABSTRACT

The Nordstrom-Robinson code, a nonlinear binary code of length 16 and minimal Hamming distance 6, is the binary image of the octacode, a linear self-dual code over $\mathbb{Z}_4$ of length 8 and minimal Lee distance 6. Since the octacode is the $\mathbb{Z}_4$-analogue of a Hamming code, this provides an extremely simple definition of the Nordstrom-Robinson code.

The Nordstrom-Robinson Code is the Binary Image of the Octacode

G. David Forney, Jr.
Motorola Codex
Mansfield, MA 02048 USA

N. J. A. Sloane
Mathematical Sciences Research Center
AT&T Bell Laboratories
Murray Hill, New Jersey 07974 USA

Mitchell D. Trott
Department of Electrical Engineering and Computer Science
M. I. T.
Cambridge, MA 02139 USA

1. Introduction

This note records an interesting result of the DIMACS/IEEE Workshop that was obtained outside of the formal sessions.

Briefly, as the Workshop began, one of us (Trott), acting on a suggestion by Forney, had just succeeded in proving that the Nordstrom-Robinson (or NR) code was the binary image of a linear code over $\mathbb{Z}_4$, the integers $\bmod 4$. Trott asked Sloane if this result was known previously. Sloane thought not,* but immediately recognized that the NR code must be the binary image of the octacode, a self-dual code over $\mathbb{Z}_4$ which is used as a glue code in a construction of the Leech lattice from the face-centered cubic lattice [CS92, Chaps. 16, 24], [CS93].

The purpose of this note is to establish this result, to show that there is no analogous self-dual code of length 12 whose binary image is the Golay code, and to give a simple construction for the E_8 lattice from the octacode.

2. Preliminaries

The symmetry group of binary Hamming n-space $\mathbb{Z}_2^n$ is a semidirect product of the group of translations by elements of $\mathbb{Z}_2^n$ (isomorphic to $\mathbb{Z}_2^n$) by the group of coordinate permutations

*He was wrong! R. Hammons and P. V. Kumar had noticed this in June, although they had not identified the $\mathbb{Z}_4$-code as the octacode. For further details see [CHKSS], [HKCSS].

(the symmetric group S_n). In particular, the symmetry group of $\mathbb{Z}_2^2$ is a semidirect product of $\mathbb{Z}_2^2$ by $\mathbb{Z}_2$, which is isomorphic to the dihedral group of order 8. This group has a subgroup isomorphic to $\mathbb{Z}_4$, namely the group $R = \langle \rho \rangle$ generated by the isometry $\rho = \{$swap coordinates and add 01$\}$. ρ induces the permutation

$$00 \to 01 \to 11 \to 10 \to 00$$

on $\mathbb{Z}_2^2$. Thus R is a sharply transitive generating group of $\mathbb{Z}_2^2$.

This leads to an 'isometric labeling' [Fo91] of $\mathbb{Z}_2^2$ by $\mathbb{Z}_4$, namely

$$00 \leftrightarrow 0, \quad 01 \leftrightarrow 1, \quad 11 \leftrightarrow 2, \quad 10 \leftrightarrow 3 \ . \tag{1}$$

We use (1) to define a mapping from $\mathbb{Z}_4^n$ to $\mathbb{Z}_2^{2n}$ as follows. Let $\alpha, \beta : \mathbb{Z}_4 \to \mathbb{Z}_2$ be given by

i	$\alpha(i)$	$\beta(i)$
0	0	0
1	0	1
2	1	1
3	1	0

Then the *binary image* $C = \phi(D)$ of a code D in $\mathbb{Z}_4^n$ is defined to be the image of D under the map $\phi : \mathbb{Z}_4^n \to \mathbb{Z}_2^{2n}$ given by

$$\phi(a_1, a_2, \ldots, a_n) = (\alpha(a_1), \beta(a_1), \alpha(a_2), \ldots, \beta(a_n)) \ . \tag{2}$$

A linear code D of length n over $\mathbb{Z}_4$ is an additive subgroup of $\mathbb{Z}_4^n$. We define an inner product on $\mathbb{Z}_4^n$ by $a \cdot b = a_1 b_1 + \cdots + a_n b_n \pmod 4$, and then the notions of dual code (D^*) and self-dual code ($D = D^*$) are defined in the usual way (cf. [Kl87], [MS77]).

The symmetrized weight enumerator (s.w.e.) of a linear code D over $\mathbb{Z}_4$ is

$$swe_D(x, y, z) = \sum_{a \in D} x^{N_0(a)} y^{N_1(a)} z^{N_2(a)} \ ,$$

where $N_i(a)$ is the number of components of a congruent to $\pm i \pmod 4$. The Lee weight enumerator of D is given by

$$Lee_D(x) = swe_D(1, x, x^2) \ . \tag{3}$$

(The Lee weights of $0, 1, 2, 3$ are respectively $0, 1, 2, 1$.)

The binary image $C = \phi(D)$ is in general nonlinear. (Necessary and sufficient conditions for $\phi(D)$ to be linear are given in [HKCSS].) We say that a binary code is $\mathbb{Z}_4$-*linear* if after a suitable permutation of coordinates it has the form $\phi(D)$ for some linear code D.

Although a binary $\mathbb{Z}_4$-linear code C need not be linear, it follows from the fact that D is linear that $C = \phi(D)$ is 'a geometrically uniform code' in Hamming space [Fo91]. In particular, C is distance invariant: the set of Hamming distances from any word in C to all other words is the set of Lee weights in D. The weight enumerator $W_C(x)$ of C is therefore well-defined, and is given by

$$W_C(x) = Lee_D(x) = swe_D(1, x, x^2) \ . \tag{4}$$

If we replace $\{0, 1\}$ by $\{+1, -1\}$, the binary image $\phi(x)$ of a vector $x \in \mathbb{Z}_4^n$ is a vertex of the $2n$-cube. The transformation ρ now becomes a $90°$ rotation in 2-space, Lee distance becomes Euclidean distance, and the image of a linear code over $\mathbb{Z}_4$ becomes a geometrically uniform subset of the hypercube in Euclidean $2n$-space (a 'group code for the Gaussian channel', in the sense of Slepian [Sl68]). The codewords of D become a group of vectors of rotations of 2-space, and then $C = \phi(D)$ is the image of a vertex of the $2n$-cube under this group. Each codeword in D is a symmetry of C.

Example. The binary image of the $\mathbb{Z}_4$ code with generator matrix

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 2 & 2 & 2 & 2 \\ 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 \\ 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \tag{5}$$

is the first-order Reed-Muller code $\mathcal{R}$ of length 16. (In [HKCSS] it is shown that any binary Reed-Muller code of length 2^m and order $0, 1, 2, m-1$ or m is $\mathbb{Z}_4$-linear.)

3. The Nordstrom-Robinson code

The NR code has an interesting history, recounted in [Be74]. In the course of a public lecture in 1967, Robinson pointed out that the smallest parameters allowed by known distance bounds for which a linear code was not yet known to exist were $[15, 8, 5]$. Nordstrom, then a high-school student, succeeded in constructing a nonlinear code with these parameters [NR67]. The NR code of this paper is obtained by extending Nordstrom's code with an overall parity check. It is now known that no linear code exists with these parameters, and in fact that the NR code is the unique code of length 16, minimal distance 6 and containing 256 words (Snover [Sn73]).

The usual definition of the NR code is the following [MS77, Chaps. 2, 15]. Let $\mathcal{G}$ denote the $[24, 12, 8]$ Golay code with coordinates arranged so that $1^8 0^{16} \in \mathcal{G}$. The $[16, 5, 8]$ first-order

Reed-Muller code $\mathcal{R}$ consists of all vectors $v \in \mathbb{Z}_2^{16}$ such that $0^8 v \in \mathcal{G}$. The NR code consists of all vectors $v \in \mathbb{Z}_2^{16}$ such that $uv \in \mathcal{G}$, where u is one of the eight vectors

$$00000000, \quad 11000000, \quad 10100000, \ldots, 10000001 \ .$$

$\mathcal{N}$ is the union of eight translates of $\mathcal{R}$, and is a nonlinear code of length 16 containing 256 words with minimal Hamming distance 6. $\mathcal{N}$ has weight enumerator

$$1 + 112x^6 + 30x^8 + 112x^{10} + x^{16} \ . \tag{6}$$

This definition makes it easy to study the properties of the NR code, via the properties of the Golay code and its symmetry group $Aut(\mathcal{G})$, since that group is well understood [CS92, Chaps. 10, 11]. For example, [CS90] classifies all vectors of $\mathbb{Z}_2^{16}$ into orbits under the symmetry group $Aut(\mathcal{N})$ of the NR code.

One property that is not stated in [CS90] but which is very easy to establish is that NR is geometrically uniform. As in [CS90], [CS92] we describe words in the Golay code by coordinates arranged in 4×6 arrays consisting of three 4×2 arrays called 'bricks' (these are the Miracle Octad Generator or MOG coordinates for $\mathcal{G}$). $\mathcal{N}$ is formed by taking all words of $\mathcal{G}$ whose left brick is one of

$$\begin{array}{|cc|}\hline \ & \ \\ & \\ & \\ & \\ \hline\end{array}\,,\ \begin{array}{|cc|}\hline 1 & \\ 1 & \\ & \\ & \\ \hline\end{array}\,,\ \begin{array}{|cc|}\hline 1 & \\ & \\ 1 & \\ & \\ \hline\end{array}\,,\ \begin{array}{|cc|}\hline 1 & \\ & \\ & \\ 1 & \\ \hline\end{array}\,,\ \begin{array}{|cc|}\hline 1 & 1 \\ & \\ & \\ & \\ \hline\end{array}\,,\ \begin{array}{|cc|}\hline 1 & \\ & 1 \\ & \\ & \\ \hline\end{array}\,,\ \begin{array}{|cc|}\hline 1 & \\ & \\ & 1 \\ & \\ \hline\end{array}\,,\ \begin{array}{|cc|}\hline 1 & \\ & \\ & \\ & 1 \\ \hline\end{array}\,, \tag{7}$$

and projecting onto the other two bricks. The words corresponding to the first figure in (7) comprise the Reed-Muller code $\mathcal{R}$.

If we translate $\mathcal{N}$ by adding to it a vector from one of the nonzero cosets of $\mathcal{R}$ in $\mathcal{N}$, say that corresponding to the second figure in (7), we obtain a code $\mathcal{N}'$ which is formed from the Golay words whose left brick is one of

$$\begin{array}{|cc|}\hline 1 & \\ 1 & \\ & \\ & \\ \hline\end{array}\,,\ \begin{array}{|cc|}\hline \ & \ \\ & \\ & \\ & \\ \hline\end{array}\,,\ \begin{array}{|cc|}\hline & \\ 1 & \\ 1 & \\ & \\ \hline\end{array}\,,\ \begin{array}{|cc|}\hline & \\ 1 & \\ & \\ 1 & \\ \hline\end{array}\,,\ \begin{array}{|cc|}\hline & 1 \\ 1 & \\ & \\ & \\ \hline\end{array}\,,\ \begin{array}{|cc|}\hline & \\ 1 & 1 \\ & \\ & \\ \hline\end{array}\,,\ \begin{array}{|cc|}\hline & \\ 1 & \\ & 1 \\ & \\ \hline\end{array}\,,\ \begin{array}{|cc|}\hline & \\ 1 & \\ & \\ & 1 \\ \hline\end{array}\ . \tag{8}$$

But $Aut(\mathcal{G})$ contains permutations that fix the left brick as a whole and apply any even permutation inside it, thus sending (7) to (8) (see [CS92, Chap. 11, §10]). So $\mathcal{N}$ and $\mathcal{N}'$ are geometrically congruent.

This result is also a consequence of Theorem 1 below. However, arguments such as this demonstrate that the old definition of the NR code is not totally superseded by the new one from the octacode. For one thing, the symmetry group of the NR code has order $2^4 \cdot 7! = 80640$, while the group of the octacode (the group of all permutations and sign-changes of coordinates that preserve the set of codewords, which in this case is isomorphic to $GL(4,2)$), has order only 1344.

4. The octacode

The octacode $\mathcal{O}_8$ may be defined in several equivalent ways. The first definition guarantees that the definitions are equivalent.

(i) $\mathcal{O}_8$ is the unique self-dual code of length 8 over $\mathbb{Z}_4$ with minimal Lee distance 6 [CS93, Theorem 2]. It has symmetrized weight enumerator

$$x^8 + 16y^8 + 14x^4z^4 + z^8 + 112xy^4z(x^2+z^2) \ . \tag{9}$$

(ii) Form the cyclic code of length 7 over $\mathbb{Z}_4$ with generator polynomial $g(X) = X^3 + 3X^2 + 2X + 3$, and add an overall parity check to make the coordinates sum to zero. The result is $\mathcal{O}_8$. $g(X)$ is a divisor of $X^7 - 1 \pmod 4$ and reduces to $X^3 + X^2 + 1 \pmod 2$, so $\mathcal{O}_8$ may be regarded as a $\mathbb{Z}_4$-analogue of a Hamming code. Then $\mathcal{O}_8$ is the code of length 8 over $\mathbb{Z}_4$ with generator matrix

$$\begin{array}{c} \begin{array}{cccccccc} \infty & 0 & 1 & 2 & 3 & 4 & 5 & 6 \end{array} \\ \left[\begin{array}{cccccccc} 3 & 3 & 2 & 3 & 1 & 0 & 0 & 0 \\ 3 & 0 & 3 & 2 & 3 & 1 & 0 & 0 \\ 3 & 0 & 0 & 3 & 2 & 3 & 1 & 0 \\ 3 & 0 & 0 & 0 & 3 & 2 & 3 & 1 \end{array}\right] \end{array} , \tag{10}$$

or equivalently

$$\left[\begin{array}{cccccccc} 2 & 0 & 0 & 0 & 1 & 3 & 1 & 1 \\ 2 & 0 & 1 & 1 & 2 & 2 & 3 & 1 \\ 0 & 1 & 0 & 1 & 2 & 3 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{array}\right] . \tag{11}$$

The order-2 words in (10) and (11) are generated by

$$\left[\begin{array}{cccccccc} 2 & 2 & 2 & 0 & 2 & 0 & 0 & 0 \\ 2 & 0 & 2 & 2 & 0 & 2 & 0 & 0 \\ 2 & 0 & 0 & 2 & 2 & 0 & 2 & 0 \\ 2 & 0 & 0 & 0 & 2 & 2 & 0 & 2 \end{array}\right] \quad \text{and} \quad \left[\begin{array}{cccccccc} 0 & 0 & 0 & 0 & 2 & 2 & 2 & 2 \\ 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 \\ 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \end{array}\right] ,$$

respectively. These are familiar generator matrices for the $[8,4,4]$ binary Hamming code, multiplied by 2.

(iii) $\mathcal{O}_8$ is the 'glue code' used in the 'holy construction' of the Leech lattice from eight copies of the face-centered cubic lattice A_3 [CS92, Chaps. 16, 24]. The connection between these lattices and codes over $\mathbb{Z}_4$ arises from the fact that the quotient A_3^*/A_3 of the dual lattice A_3^* by A_3 is isomorphic to $\mathbb{Z}_4$.

The main result of this note is the following.

Theorem 1. *The image $\phi(\mathcal{O}_8)$ is the Nordstrom-Robinson code.*

Proof. It follows from (4) and (9) that the binary image of $\mathcal{O}_8$ has minimal distance 6. From Snover's uniqueness theorem [Sn73], this code is equivalent to the NR code. ■

Here is an explicit isomorphism. We use (10) to define $\mathcal{O}_8$, labeling the coordinates as shown in that matrix, and map the words of $\mathcal{O}_8$ to binary vectors of length 16 by sending $a_\infty\ a_0\ a_1 \ldots a_6$ to the MOG vector

$$\begin{array}{|cc|cc|}
\hline
\alpha(a_\infty) & \alpha(a_0) & \beta(a_\infty) & \beta(a_0) \\
\alpha(a_3) & \alpha(a_2) & \beta(a_3) & \beta(a_2) \\
\hline
\alpha(a_5) & \alpha(a_1) & \beta(a_5) & \beta(a_1) \\
\alpha(a_6) & \alpha(a_4) & \beta(a_6) & \beta(a_4) \\
\hline
\end{array}$$

(cf. [CS92, Figure 11.28]). It is now a routine calculation to verify that this map sends the words of $\mathcal{O}_8$ to words of the NR code as defined by (7).

In [HKCSS] it is shown that Kerdock and (slightly modified) Preparata codes are also binary images of linear codes over $\mathbb{Z}_4$, as are the Goethals and Delsarte-Goethals nonlinear codes. In fact the Kerdock and Preparata codes are the binary images of a dual pair of extended cyclic codes over $\mathbb{Z}_4$.

5. The Golay code

Because of the relationship between the NR code and the Golay code, it is natural to ask if the Golay code itself is the image of a self-dual code over $\mathbb{Z}_4$. It is not.

Theorem 2. *There is no self-dual code of length 12 over $\mathbb{Z}_4$ whose binary image is the* $[24, 12, 8]$ *Golay code.*

Proof. It follows from Theorem 6 of [CS93] that the symmetrized weight enumerator of any self-dual code over $\mathbb{Z}_4$ is a polynomial function of the three generators

$$f_1 = x + z ,$$

$$\begin{aligned} f_4 &= 2y^4 - xz(x^2+z^2) , \\ f_8 &= y^4(x-z)^4 . \end{aligned}$$

A self-dual code of length 12 therefore has s.w.e. of the form

$$a_1 f_8 f_1^4 + a_2 f_8 f_4 + a_3 f_4^3 + a_4 f_4^2 f_1^4 + a_5 f_4 f_1^8 + a_6 f_1^{12} , \tag{12}$$

where the a_i are integers. The condition that this should collapse to the weight enumerator of the Golay code when x, y, z are replaced respectively by $1, x, x^2$ implies $a_1 = 6-a_4$, $a_2 = 64-a_3$, $a_5 = 12$, $a_6 = 1$. When these values are substituted in (12), the coefficient of $x^3 y^8 z$ becomes -512, which is impossible. ■

By using further properties of the Golay code, one can show that there is no linear code over $\mathbb{Z}_4$ whose binary image is the Golay code — see [HKCSS]. Of course there *is* a nonlinear code with this property: just map the Golay code into a $\mathbb{Z}_4$-code using (1).

6. The E_8 lattice

One of the standard constructions for the 8-dimensional lattice E_8 is that it consists of all vectors $u \in \mathbb{Z}^8$ such that $u(\text{mod } 2)$ is in the $[8,4,4]$ Hamming code ([CS92, Chaps. 5,7]). There is a similar construction from $\mathcal{O}_8$.

Theorem 3. *The set of vectors $u \in \mathbb{Z}^8$ such that u (mod 4) is in the octacode is isomorphic to the E_8 lattice.*

Proof. It is easy to see that this set of vectors forms a lattice Λ. By an argument similar to that used to prove Theorem 3 of [CS92, Chap. 7], the theta series of Λ is obtained from the s.w.e. of the octacode by replacing x, y, z by

$$\begin{aligned} &1 + 2q^{16} + 2q^{64} + \cdots , \\ &q + q^9 + q^{25} + \cdots , \\ &2q^4 + 2q^{36} + 2q^{100} + \cdots \end{aligned}$$

respectively. From Eq. (9) we find that the theta series of Λ begins $1 + 240q^8 + \cdots$. But Bannai and Sloane (see Chapter 14 of [CS92]) have shown that E_8 is the unique 8-dimensional lattice with kissing number 240. ■

It can be seen in retrospect that this version of the E_8 lattice was used in a construction of the Leech lattice in [Fo88].

Acknowledgment

M. D. Trott wishes to thank his student Rajeev Surati for his assistance.

References

[Be74] E. R. Berlekamp, editor, *Key papers in the development of coding theory*, IEEE Press, NY, 1974, p. 101.

[CHKSS] A. R. Calderbank, R. Hammons, P. V. Kumar, N. J. A. Sloane and P. Solé, *A linear construction for certain Kerdock and Preparata codes*, Bull. Amer. Math. Soc., submitted, 1992.

[CS90] J. H. Conway and N. J. A. Sloane, *Orbit and coset analysis of the Golay and related codes*, IEEE Trans. Inform. Theory, **36** (1990), 1038–1050.

[CS92] J. H. Conway and N. J. A. Sloane, *Sphere-packings, lattices and groups*, 2nd ed., Springer-Verlag, NY 1992.

[CS93] J. H. Conway and N. J. A. Sloane, *Self-dual codes over the integers modulo 4*, J. Comb. Theory, Ser. A, **62** (1993), in press.

[Fo88] G. D. Forney, Jr., *Coset codes — part II: binary lattices and related codes*, IEEE Trans. Inform. Theory, **34** (1988), 1152–1187.

[Fo91] G. D. Forney, Jr., *Geometrically uniform codes*, IEEE Trans. Inform. Theory, **37** (1991), 1241–1260.

[HKCSS] 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.

[Kl87] M. Klemm, *Über die Identität von MacWilliams für die Gewichtsfunktion von Codes*, Arch. Math., **49** (1987), 400–406.

[MS77] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*, North-Holland, Amsterdam, 1977.

[NR67] A. W. Nordstrom and J. P. Robinson, *An optimum nonlinear code*, Inform. Control, **11** (1967), 613–616. Reprinted in [Be74].

[Sl68] D. Slepian, *Group codes for the Gaussian channel*, Bell Syst. Tech. J., **47** (1968), 575–602.

[Sn73] S. L. Snover, *The uniqueness of the Nordstrom-Robinson and the Golay binary codes*, Ph.D. Dissertation, Math. Dept., Michigan State Univ., 1973.