A Linear Construction for Certain Kerdock and Preparata Codes

A. R. Calderbank

Mathematical Sciences Research Center
AT&T Bell Laboratories, Murray Hill, NJ 07974 U.S.A.

A. R. Hammons, Jr.

Hughes Aircraft Company
8433 Fallbrook Avenue, Canoga Park, CA 91304 U.S.A.

P. Vijay Kumar

Communication Science Institute, EE-Systems
University of Southern California, Los Angeles, CA 90089 U.S.A.

N. J. A. Sloane

Mathematical Sciences Research Center
AT&T Bell Laboratories, Murray Hill, NJ 07974 U.S.A.

Patrick Solé

CNRS – I3S, 250 rue A. Einstein, bâtiment 4
Sophia – Antipolis, 06560 Valbonne, France

May 20, 1993

ABSTRACT

The Nordstrom-Robinson, Kerdock and (slightly modified) Preparata codes are shown to be linear over $\mathbb{Z}_4$, the integers mod 4. The Kerdock and Preparata codes are duals over $\mathbb{Z}_4$, and the Nordstrom-Robinson code is self-dual. All these codes are just extended cyclic codes over $\mathbb{Z}_4$. This provides a simple definition for these codes, and explains why their Hamming weight distributions are dual to each other. First- and second-order Reed-Muller codes are also linear codes over $\mathbb{Z}_4$, but Hamming codes in general are not, nor is the Golay code.

A Linear Construction for Certain Kerdock and Preparata Codes

A. R. Calderbank

Mathematical Sciences Research Center
AT&T Bell Laboratories, Murray Hill, NJ 07974 U.S.A.

A. R. Hammons, Jr.

Hughes Aircraft Company
8433 Fallbrook Avenue, Canoga Park, CA 91304 U.S.A.

P. Vijay Kumar

Communication Science Institute, EE-Systems
University of Southern California, Los Angeles, CA 90089 U.S.A.

N. J. A. Sloane

Mathematical Sciences Research Center
AT&T Bell Laboratories, Murray Hill, NJ 07974 U.S.A.

Patrick Solé

CNRS – I3S, 250 rue A. Einstein, bâtiment 4
Sophia – Antipolis, 06560 Valbonne, France

1 Introduction

Some of the best-known examples of nonlinear binary error-correcting codes that are better than any linear codes are the Nordstrom-Robinson, Kerdock and Preparata codes [Ke72], [NR67], [Pr68], [MS77]. Besides their excellent error-correcting capabilities these codes are remarkable because the Kerdock and Preparata codes are 'formal duals', in the sense that although these codes are nonlinear, the weight distribution of one is the MacWilliams transform of the weight distribution of the other [MS77, Chap. 15]. The main unsolved question concerning these codes has always been whether they are duals in some more algebraic sense. Many authors have investigated these codes, and have found that (except for the Nordstrom-Robinson code) they are not unique, and indeed that large numbers of codes exist with the same weight distributions [BLW83], [Ca89], [Ka82], [Ka82a], [Ka83], [VL83]. Kantor [Ka83] declares that the "apparent relationship between these [families of codes] is merely a coincidence."

Although this may be true for many versions of these codes, we will show that, when properly defined, Kerdock and Preparata codes are *linear* over $\mathbb{Z}_4$ (the integers mod 4), and that as $\mathbb{Z}_4$-codes they *are* duals. All these codes are in fact just extended cyclic codes.

The version of the Kerdock code that we use is the standard one, while our version of the Preparata code differs from the standard one in that it is not a subcode of the Hamming code but of a nonlinear code with the same weight distribution as the Hamming code. Since the new construction is so simple, we propose that this is the 'correct' way to define these codes.

Kerdock and Preparata codes exist for all lengths $n = 4^m \geq 16$. At length 16 they coincide, giving the Nordstrom-Robinson code [NR67]. The $\mathbb{Z}_4$ version of the Nordstrom-Robinson code is the 'octacode', a self-dual code of length 8 over $\mathbb{Z}_4$ that is obtained when the Leech lattice is decomposed into eight copies of the face-centered cubic lattice. This result was announced in [FST93]. (The octacode itself is described in [CS92], [CS93] and Section 3 below.)

The very good nonlinear codes of minimal distance 8 discovered by Goethals [Go74], [Go76], and the high minimal distance codes of Delsarte and Goethals [DG75], also have a simple description as codes over $\mathbb{Z}_4$ (see [HKCSS]).

This work developed out of the discovery that four-valued sequences have excellent correlation properties ([So89], [Bo90], [BHK92]), and was carried out independently by Hammons and Kumar [HK93], and (very slightly later) by the other three authors. Theorems 4, 5 and 6 appear in Hammons' dissertation [Ha92]. In view of the considerable overlap, we have now joined forces. This announcement is a compositum of our results, and full details will be given in [HKCSS].

For undefined terminology from coding theory, see [MS77].

2 Codes over $\mathbb{Z}_4$

A quaternary linear code is an additive subgroup of $\mathbb{Z}_4^n$. Duality is defined with respect to the inner product $a \cdot b = a_1 b_1 + \cdots + a_n b_n \pmod 4$. We define three maps from $\mathbb{Z}_4$ to $\mathbb{Z}_2$ by

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

Then we construct binary codes from quaternary codes using the map $\phi : \mathbb{Z}_4^n \to \mathbb{Z}_2^{2n}$ given by

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

A binary code is $\mathbb{Z}_4$-*linear* if its coordinates can be permuted so that it is the image under this map of a linear code over $\mathbb{Z}_4$.

Theorem 1 *(a) The binary image $\phi(D)$ of a quaternary linear code D is linear if and only if*

$$a, b \in D \Rightarrow 2\alpha(a) * \alpha(b) \in D \ , \tag{2}$$

where $*$ is componentwise multiplication. (b) A binary linear code C of even length is $\mathbb{Z}_4$-linear if and only if its coordinates can be permuted so that

$$u, v \in C \Rightarrow (u + s(u)) * (v + s(v)) \in C \ , \tag{3}$$

where s is the 'swap' map that interchanges the left and right halves of a vector.

Theorem 2 *Binary Reed-Muller codes of length $n = 2^m \geq 2$ and orders $0, 1, 2, m-1, m$ are $\mathbb{Z}_4$-linear.*

Theorem 3 *Extended Hamming codes of lengths $n = 2^m \geq 32$ are not $\mathbb{Z}_4$-linear, nor is the Golay code of length 24.*

Remark. In (3), if u, v are represented by Boolean functions of degree r, and $(u + s(u)) * (v + s(v)) \neq 0$, then $(u + s(u)) * (v + s(v))$ is a Boolean function of degree $2r - 2$. So an r-th order Reed-Muller code with $r \leq m/2$ satisfies (3) provided $r \leq 2$, and we conjecture does not satisfy (3) if $3 \leq r \leq m - 2$. The first assertion of Theorem 3 establishes that $(m-2)$nd-order Reed-Muller codes are not $\mathbb{Z}_4$-linear for $m \geq 5$.

Let D be a quaternary linear code and $C = \phi(D)$ the corresponding binary code. In general C is not linear, but we define the $\mathbb{Z}_4$-dual of C to be $C^{\perp_4} = \phi(D^\perp)$, where $D^\perp$ denotes the dual code to D, as in the diagram

$$\begin{array}{ccccc} D & \xrightarrow{\phi} & C & = & \phi(D) \\ \text{dual} \downarrow & & & & \\ D^\perp & \xrightarrow{\phi} & C^{\perp_4} & = & \phi(D^\perp) \end{array}$$

The familiar Hamming weight enumerator for a binary linear code C will be denoted by $W_C(x, y)$. This weight enumerator is also well-defined for binary nonlinear codes provided they are distance-invariant [MS77]. The *symmetrized weight enumerator* of a quaternary linear code D 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 $\pm i \pmod 4$. Then (see [CS93], [Kl87])

$$swe_{D^\perp}(x,y,z) = \frac{1}{|D|} \ swe_D(x+2y+z, x-z, x-2y+z) \ . \tag{4}$$

Theorem 4 *If D is a quaternary linear code then $C = \phi(D)$ and $C^{\perp_4} = \phi(D^\perp)$ are distance invariant, and*

$$W_C(x,y) = swe_D(x^2, xy, y^2) \ , \tag{5}$$

$$W_{C^{\perp_4}}(x,y) = \frac{1}{|C|} W_C(x+y, x-y) \ . \tag{6}$$

3 Kerdock, Preparata and Nordstrom-Robinson codes

Let $h_2(X) \in \mathbb{Z}_2[X]$ be a primitive irreducible polynomial of degree m. There is a unique monic polynomial $h(X) \in \mathbb{Z}_4[Z]$ of degree m such that $h(X) \equiv h_2(X) \pmod 2$ and $h(X)$ divides $X^n - 1 \ (\bmod\ 4)$, where $n = 2^m - 1$ [So89], [Ya90]. Let $g(X)$ be the reciprocal polynomial to $(X^n - 1)/((X-1)h(X))$.

Theorem 5 *The cyclic code generated by $g(X)$, extended by an overall parity check, is a quaternary code D of length 2^m containing 4^{m+1} words. For m odd ≥ 3 the corresponding binary code $K = \phi(D)$ is the Kerdock code of length 2^{m+1} containing 2^{2m+2} words and with minimal distance $2^m - 2^{(m-1)/2}$.*

The proof is by showing that D has a simple definition in terms of the relative trace function from $\mathbb{Z}_4[\xi]$ to $\mathbb{Z}_4$, where ξ is a root of $h(X)$ (cf. [Bo90], [BHK92]), and in this form it agrees with the definition of the Kerdock code given in [MS77, pp. 457–458].

Theorem 6 *The cyclic code generated by $h(X)$, extended by an overall parity check, is a quaternary code $D^\perp$ dual to D. For m odd ≥ 3, the corresponding binary code $P = \phi(D^\perp)$ has length 2^{m+1}, contains 2^k words, $k = 2^{m+1} - 2m - 2$, has minimal distance 6, and has the same weight enumerator as the Preparata code.*

P is the $\mathbb{Z}_4$-dual of K, both codes are distance invariant, and the weight distribution of one is the MacWilliams transform of the weight distribution of the other.

For example when $m = 5$ we may take $h(X) = \sum_{i=0}^{5} h_i X^i$, $g(X) = \sum_{i=0}^{25} g_i X^i$, where $h_0 \ldots$ and $g_0 \ldots$ are 323001 and 11120122010303133013212213. In this case the linear span of P has minimal distance 2, which shows that P is strictly different from Preparata's original construction [Pr68], for which the linear span is the extended Hamming code.

There is a distance-regular graph [BCN89] defined on cosets of our Preparata code which may be of some combinatorial interest.

In the case $m = 3$, both P and K become the Nordstrom-Robinson code [NR67], and the quaternary code $D = D^\perp$ is the octacode. The latter may be defined as the extended cyclic code generated by $h(X) = X^3 + 3X^2 + 2X + 3$, or as the unique quaternary self-dual code of length 8 which has the property that its binary image has minimal distance 6 [CS93], or as the 'glue code' used to construct the Leech lattice from a direct sum of eight copies of the face-centered cubic lattice A_3 (note that $A_3^\perp / A_3 \cong \mathbb{Z}_4$) [CS92, Chap. 24].

Theorem 7 [FST93]. *The Nordstrom-Robinson code is the binary image of the octacode.*

References

[BLW83] R. D. Baker, J. H. van Lint and R. M. Wilson, *On the Preparata and Goethals codes*, IEEE Trans. Inform. Theory, **29** (1983), 342–345.

[Bo90] S. Boztaş, *Near-optimal 4ϕ (4-phase) sequences and optimal binary sequences for CDMA*, Ph.D. dissertation, Univ. Southern Calif., Los Angeles, 1990.

[BHK92] S. Boztaş, A. R. Hammons, Jr. and P. V. Kumar, *4-Phase sequences with near-optimum correlation properties*, IEEE Trans. Inform. Theory, **38** (1992), 1101–1113.

[BCN89] A. E. Brouwer, A. M. Cohen and A. Neumaier, *Distance-regular graphs*, Springer-Verlag, NY, 1989.

[Ca89] C. Carlet, *A simple description of Kerdock codes*, Lect. Notes Computer Science, **388** (1989), 202–208.

[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), 30–45.

[DG75] P. Delsarte and J. M. Goethals, *Alternating bilinear forms over $GF(q)$*, J. Combin. Theory, Series A, **19** (1975), 26–50.

[FST93] 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, DIMACS Series in Discrete Mathematics and Theoretical Computer Science, Amer. Math. Soc., 1993, to appear.

[Go74] J. M. Goethals, *Two dual families of nonlinear binary codes*, Electronics Letters, **10** (1974), 471–472.

[Go76] J. M. Goethals, *Nonlinear codes defined by quadratic forms over $GF(2)$*, Inform. Control, **31** (1976), 43–74.

[Ha92] A. R. Hammons, Jr., *On four-phase sequences with low correlation and their relation to Kerdock and Preparata codes*, Ph.D. Dissertation, Univ. Southern California, Nov. 1992.

[HK93] A. R. Hammons, Jr. and P. V. Kumar, *On the apparent duality of Kerdock and Preparata codes*, Abstracts, IEEE Internat. Symp. Inform. Theory, San Antonio, TX, Jan. 1993.

[HKCSS] A. R. Hammons, Jr., 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*, IEEE Trans. Information Theory, in press, 1993.

[Ka82] W. M. Kantor, *An exponential number of generalized Kerdock codes*, Inform. Control, **53** (1982), 74–80.

[Ka82a] W. M. Kantor, *Spreads, translation planes and Kerdock sets*, SIAM J. Alg. Discr. Math., **3** (1982), 151–165 and 308–318.

[Ka83] W. M. Kantor, *On the inequivalence of generalized Preparata codes*, IEEE Trans. Inform. Theory, **29** (1983), 345–348.

[Ke72] A. M. Kerdock, *A class of low-rate nonlinear binary codes*, Inform. Control, **20** (1972), 182–187.

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

[VL83] J. H. van Lint, *Kerdock and Preparata codes*, Congressus Numerantium, **39** (1983), 25–41.

[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.

[Pr68] F. P. Preparata, *A class of optimum nonlinear double-error correcting codes*, Inform. Control, **13** (1968), 378–400.

[So89] P. Solé, *A quaternary cyclic code, and a family of quadriphase sequences with low correlation properties*, Lect. Notes Computer Science, **388** (1989), 193–201.

[Ya90] M. Yamada, *Distance-regular digraphs of girth 4 over an extension ring of $Z/4Z$*, Graphs and Combinatorics, **6** (1990), 381–394.