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

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

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

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

[28] P. V. Kumar, T. Helleseth, A. R. Calderbank and A. R. Hammons, Jr., *Large sequence families with good correlation for CDMA*, preprint, 1993.

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

[30] F. J. MacWilliams, N. J. A. Sloane, and J. M. Goethals, "The MacWilliams Identities for Nonlinear Codes," *Bell Sys. Tech. J.*, Vol. 51, 1972, pp. 803–819.

[31] N. J. A. Sloane and A. D. Wyner, Eds., *Claude Elwood Shannon: Collected Papers*, IEEE Press, NY, 1992.

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

[33] K. T. Phelps, *A general product construction for error correcting codes*, SIAM J. Algeb. and Discr. Methods, **5** (1984), 224–228.

[34] K. T. Phelps, *Every finite group is the automorphism group of some perfect 1-code*, J. Comb. Theory, Series A, **43** (1986), 45–51.

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

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

[37] J. L. Vasil'ev, *On nongroup close-packed codes*, Probl. Kibern., **8** (1962), 337–339. English translation in Probleme der Kybernetik, **8** (1965), 92–95.

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

[14] 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.

[15] J. H. Conway and N. J. A. Sloane, "Quaternary Constructions for the Binary Single-Error-Correcting Codes of Julin, Best and Others," *Designs, Codes and Cryptography*, **41** (1994), pp. 31–42.

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

[17] G. D. Forney Jr., N. J. A. Sloane, and M. D. Trott, "The Nordstrom-Robinson Code is the Binary Image of the Octacode," *Coding and Quantization: DIMACS/IEEE Workshop October 19–21, 1992*, R. Calderbank, G. D. Forney Jr., and N. Moayeri, Eds., Amer. Math. Soc., 1993, pp. 19–26.

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

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

[20] A. R. Hammons Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, "The Z_4-Linearity of Kerdock, Preparata, Goethals and Related Codes," *IEEE Trans. Information Theory*, 1994 to appear.

[21] A. S. Hedayat, N. J. A. Sloane, and J. Stufken, "Orthogonal Arrays: Theory and Practice," book-in-progress.

[22] F. B. Hergert, *On the Delsarte-Goethals codes and their formal duals*, Discrete Math., **83** (1990), 249–263.

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

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

References

[1] E. F. Assmus, Jr. and J. D. Key, *Designs and Their Codes*, Cambridge Univ. Press, 1992.

[2] 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.

[3] E. R. Berlekamp, editor, *Key Papers in the Development of Coding Theory*, IEEE Press, NY, 1974.

[4] M. R. Best, A. E. Brouwer, F. J. MacWilliams, A. M. Odlyzko, and N. J. A. Sloane, "Bounds for Binary Codes of Length Less than 25," *IEEE Trans. Information Theory*, Vol. IT-24, 1978, pp. 81–91.

[5] I. F. Blake, editor, *Algebraic Coding Theory — History and Development*, Dowden, Hutchinson and Ross, Stroudsberg, PA, 1973.

[6] A. Bonnecaze, A. R. Calderbank and P. Solé, Quaternary quadratic residue codes and unimodular lattices, preprint.

[7] A. Bonnecaze and P. Solé, Quaternary constructions of formally self-dual binary codes and unimodular lattices, in *Proc. First France-Israeli Workshop on Coding Theory, Paris, July 1993*, Lecture Notes in Computer Science, Springer-Verlag 1994, to appear.

[8] 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.

[9] A. E. Brouwer, J. B. Shearer, N. J. A. Sloane, and W. D. Smith, "A New Table of Constant Weight Codes," *IEEE Trans. Information Theory*, Vol. 36, 1990, pp. 1334–1380.

[10] 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., **29** (1993), 218–222.

[11] A. R. Calderbank and N. J. A. Sloane, "Modular and p-Adic Cyclic Codes," *Designs, Codes and Cryptography*, submitted.

[12] C. Carlet, A general case of formal duality between binary nonlinear codes, *Discrete Math.*, **111** (1993), 77–85.

where C and $C_\perp$ are binary (nonlinear) codes of length $2n$, as in the following diagram:

$$\begin{array}{ccccc} \mathcal{C} & \xrightarrow{\phi} & C & = & \phi(\mathcal{C}) \\ \text{dual} \Big\downarrow & & & & \\ \mathcal{C}^\perp & \xrightarrow{\phi} & C_\perp & = & \phi(\mathcal{C}^\perp) \ . \end{array} \tag{16}$$

Although C and $C_\perp$ are nonlinear, it follows from (11) and (13) that their weight enumerators are related by the MacWilliams identity!

Similar explanations for the Goethals, Delsarte-Goethals and Hergert codes are also given in [20]. Reference [15] similarly gives simple explanations for certain important binary nonlinear *single-error-correcting* codes.

The Theorem above shows that we get the 'Preparata' codes by lifting the generator polynomial for a Hamming code from $\mathbb{Z}_2 = GF(2)$ to $\mathbb{Z}_4$. Reference [11] investigates what happens if we continue to lift to $\mathbb{Z}_8$, $\mathbb{Z}_{16}, \ldots$, even to the p-adic integers.

Finally, ... No, there is no "Finally" yet — many topics remain to be investigated! Reference [20] leaves many open questions. Research continues ...

Let $g(x)$ be the reciprocal polynomial to

$$\frac{x^n - 1}{(x-1)\tilde{M}(x)} .$$

Theorem. [20] *(a) The cyclic code with generator polynomial $g(x)$, extended by the addition of an overall parity check symbol, is mapped by the Gray map ϕ onto the Kerdock code $K(2m)$.*

(b) The cyclic code with generator polynomial $\tilde{M}(x)$, extended by the addition of an overall parity check symbol, is mapped by the Gray map ϕ onto the 'Preparata' code $P'(2m)$.

Note that the linear codes over $\mathbb{Z}_4$ in (a) and (b) are dual to each other.

There are quotes around 'Preparata' in the Theorem, since although this code has the same parameters and the same weight distribution as the Preparata code, it is not equivalent to it. However, because our construction is so simple, we propose that this is the 'correct' way to define the Preparata codes. The situation may be compared with that for Hamming codes. It is known that there are many codes with the same weight distribution as the Hamming code — all are perfect single-error correcting codes, but one is distinguished by being linear (see [33], [34], [37]). Similarly, there are many codes with the same weight distributions as the Kerdock and Preparata codes; one pair is distinguished by being the images of a pair of dual linear codes over $\mathbb{Z}_4$. It happens that Kerdock picked out the distinguished code, although Preparata did not.

The Theorem implies (compare Section 3) that the Kerdock and 'Preparata' codes are now simply $\mathbb{Z}_4$-analogues of first-order Reed-Muller and extended Hamming codes, respectively.

In particular, if ξ denotes a root of $g(x)$, then the matrix

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & \xi & \xi^2 & \xi^3 & \cdots & \xi^{n-1} \end{bmatrix} , \tag{15}$$

$n = 2^m - 1$, is both a generator matrix for the Kerdock code and a parity check matrix for the 'Preparata' code. Nothing could be simpler! The case $m = 3$ gives the Nordstrom-Robinson code (in which case (14) and (15) are equivalent matrices).

The duality between the Kerdock and 'Preparata' codes is now also explained. Starting from a linear code $\mathcal{C}$ over $\mathbb{Z}_4$ of length n (for example, that defined in part (a) of the Theorem) we construct the codes $\mathcal{C}^\perp$, and

$$C = \phi(\mathcal{C}), \quad C_\perp := \phi(\mathcal{C}^\perp) ,$$

To get a binary code from a $\mathbb{Z}_4$ code, one uses the *Gray map* ϕ. This is a map from $\mathbb{Z}_4$ to $GF(2)^2$ defined by

$$0 \to 00, \quad 1 \to 01, \quad 2 \to 11, \quad 3 \to 10 \ , \tag{12}$$

and extended to a map from $\mathbb{Z}_4^n$ to $GF(2)^{2n}$ in the natural way. The key property, obvious from (12), is that the map

$$\phi : (\mathbb{Z}_4^n, \text{ Lee distance}) \to (GF(2)^{2n}, \text{ Hamming distance}) \tag{13}$$

is an isometry of metric spaces.

The octacode is an especially important code over $\mathbb{Z}_4$ that originally arose in one of the "holy constructions" of the Leech lattice ([13, Chap. 24]), in particular in the construction based on A_3^8. The Leech lattice, the conjecturally densest sphere packing in 24 dimensions, can be built up from a product of eight copies of the face-centered cubic lattice A_3, the conjecturally densest sphere packing in three dimensions. The quotient of A_3 in its dual lattice A_3^* is a cyclic group of order 4, and so to get the Leech lattice from A_3 one needs a code of length 8 over $\mathbb{Z}_4$. The appropriate code, the octacode, is a code with 256 codewords and minimal Lee distance 6, i.e. an $(8, 256, 6)_4$ code, defined by the generator matrix

$$\begin{bmatrix} 3 & 3 & 2 & 3 & 1 & 0 & 0 & 0 \\ 3 & 0 & 3 & 2 & 3 & 1 & 0 & 0 \\ 3 & 0 & 0 & 3 & 2 & 3 & 1 & 0 \\ 3 & 0 & 0 & 0 & 3 & 2 & 3 & 1 \end{bmatrix} . \tag{14}$$

The octacode is self-dual, so (14) is also a parity check matrix.

We can now state the astonishing 1992 discovery: the Nordstrom-Robinson code is the image of the octacode under the Gray map! (The verification is easy.)

Analogous descriptions of the Preparata and Kerdock codes followed soon afterwards. The paper [20] by Roger Hammons, Vijay Kumar, Robert Calderbank, Patrick Solé and myself is the main reference for this material.

One of the principal results in that paper is the following. Take the binary primitive irreducible polynomial $M(x)$ of degree m defined in Section 3, a divisor of $x^n - 1$, $n = 2^m - 1$. There is a unique monic polynomial $\tilde{M}(x)$ of degree m over $\mathbb{Z}_4$ such that

$$\tilde{M}(x) \equiv M(x) \pmod 2 \ ,$$
$$\tilde{M}(x) \mid x^n - 1 \pmod 4 \ .$$

(See [11] for a proof.) For example, if $m = 3$, $M(x) = x^3 + x + 1$, we find $\tilde{M}(x) = x^3 + 2x^2 + x - 1$.

essential relationship between the Preparata and Kerdock codes described in [20]. In partial justification it can be said that we were working with the wrong form for the Preparata codes — their definition must be changed slightly before the duality becomes evident.

A number of other authors (even as recently as 1991 [12]) also investigated these codes, showing among other things that (except at length 16) there are many different codes with the same parameters [2], [24]–[26]. These authors were also unable to give a simple explanation for the "duality" phenomenon. In fact [26] declares that the "apparent relationship between these [families of codes] is merely a coincidence."

5. Codes over $\mathbb{Z}_4$

The breakthrough came in 1992 with the discovery [10], [17], [20] that the Nordstrom-Robinson code is essentially the same as a certain well-known *linear* code over $\mathbb{Z}_4$ (the ring of integers modulo 4) called the octacode.

The definitions for codes over $\mathbb{Z}_4$ are similar to those given in Section 2 for codes over fields (cf. [14], [38]). A code of length n is a subset of $\mathbb{Z}_4^n$, a linear code is an additive subgroup of $\mathbb{Z}_4^n$, and dual and self-dual codes are defined via the inner product $u \cdot v = v_1 v_1 + \cdots + u_n v_n \pmod 4$. The essential difference between binary and quaternary codes is that the former have characteristic 2 ($1 + 1 = 0$) whereas the latter have characteristic 4 ($1 + 1 = 2$). This is sometimes difficult for a coding theorist to remember!

The appropriate notion of distance for codes over $\mathbb{Z}_4$ is Lee distance, defined as follows. First we define the *Lee weight* wt_L of the element of $\mathbb{Z}_4$ by

$$\begin{array}{cccccc} x & 0 & 1 & 2 & 3 \\ wt_L(x) & 0 & 1 & 2 & 1 \end{array} ,$$

and extend it to $\mathbb{Z}_4^n$ by

$$wt_L(u) = \sum_{i=1}^{n} wt_L(u_i)$$

if $u = (u_1, \ldots, u_n)$. The *Lee distance* between $u, v \in \mathbb{Z}_4^n$ is then $dist_L(u, v) = wt_L(u - v)$.

The Lee weight enumerator of a linear code $\mathcal{C}$ over $\mathbb{Z}^4$ is

$$Lee_{\mathcal{C}}(x, y) = \sum_{u \in \mathcal{C}} x^{2n - wt_L(u)} y^{wt_L(u)} ,$$

and the MacWilliams identity has the form

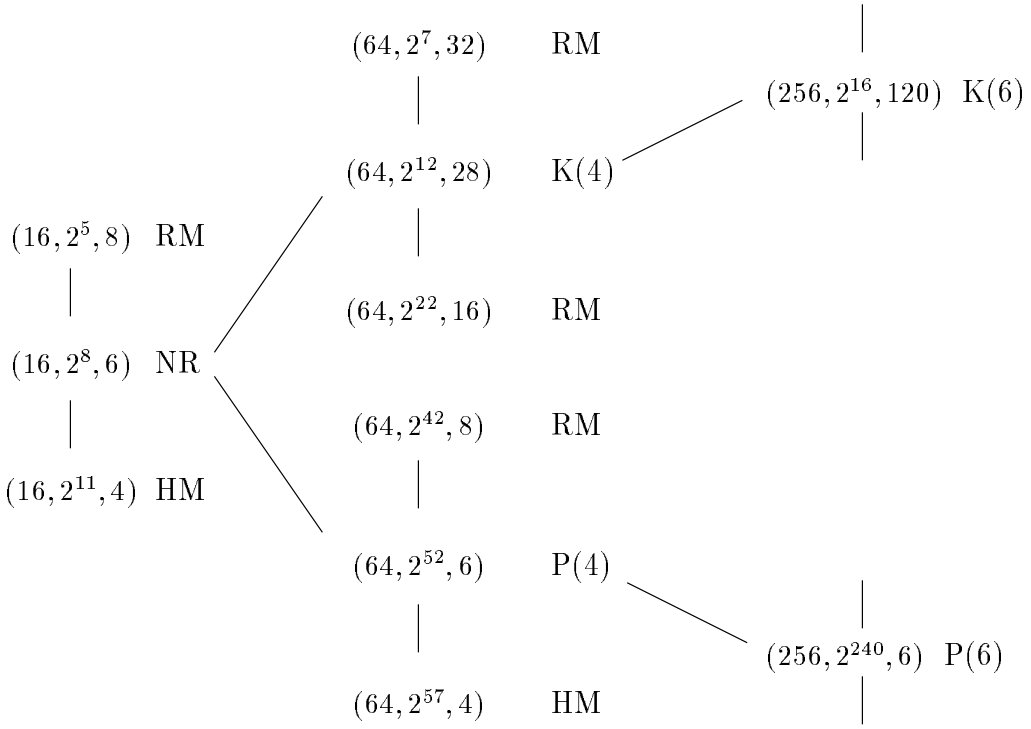
$$Lee_{\mathcal{C}^\perp}(x, y) = \frac{1}{|\mathcal{C}|} Lee_{\mathcal{C}}(x + y, x - y) . \tag{11}$$

dual to the Preparata codes. The Kerdock code $K(m)$ has parameters

$$n = 2^m, \quad M = 2^{2m}, \quad d = 2^{m-1} - 2^{(m-2)/2}, \tag{10}$$

for even $m \geq 4$. For $m = 4$ the Preparata and Kerdock codes coincide with the Nordstrom-Robinson code.

The following diagram shows the relationship between some of these codes. (Here NR denotes the Nordstrom-Robinson code.)



Further nonlinear generalizations were later found by Goethals [18], [19], Delsarte and Goethals [16], and Hergert [22].

Since the Preparata and Kerdock codes are not linear, they cannot be dual to each other in the sense defined in Section 2. Yet besides satisfying

$$|P(m)| \cdot |K(m)| = 2^{2^m},$$

it is a remarkable fact that the weight enumerators of $P(m)$ and $K(m)$ also satisfy the MacWilliams identity (3).

F. J. MacWilliams and the present author spent a considerable amount of time when these codes were discovered, attempting to find a simple explanation for this phenomenon! We obtained some partial results (some of which are presented in [30] and [29]), but we missed the

At length $n = 2^4 = 16$, we now have the following codes:

n	M	d	type
16	2^{11}	4	Hamming or $RM(2,4)$
16	2^7	6	BCH
16	2^5	8	$RM(1,4)$

These were the best codes known in the mid 1960's. How good are they? If we let $A(n,d)$ denote the maximal number of codewords in a binary code of length n and minimal distance d, then it is not difficult to show (cf. [29], [4], [9]) that

$$A(16,4) \leq 2^{11}, \quad A(16,6) \leq 2^8, \quad A916,8) \leq 2^5 \ .$$

The codes given above show that equality holds in the first and last of these. But what about $A(16,6)$? Does there exist a code with 256 codewords?

4. Nonlinear codes appear

J. P. Robinson asked the above questions in a high school talk he gave in 1965, and one of the students in the audience, A. W. Nordstrom (who at the time was 14 years old) worked on the problem and together they solved it, by finding such a code. This is the infamous Nordstrom-Robinson code, which was published in 1967 [32], with parameters $(16,256,6)_2$. Thus indeed $A(16,6) = 2^8$.

However, the code is nonlinear. Furthermore no linear code of length 16 and minimal distance 6 can have more than 128 codewords. There is simple construction of this Nordstrom-Robinson code in terms of the Golay code of length 24 [29, p. 73]). It is also known to be unique [36].

One of the results of the investigations that are described in the present paper is that the Nordstrom-Robinson code now has a completely elementary and self-contained construction — see (15)!

In the following years a number of other nonlinear codes were discovered, generalizing the Nordstrom-Robinson code in various ways. In 1968 the *Preparata* codes appeared [35]. The Preparata code $P(m)$ has parameters

$$n = 2^m, \quad M = 2^{2^m - 2m}, \quad d = 6 \ , \tag{9}$$

for even $m \geq 4$, which by comparison with (8) is seen to have twice as many codewords as a double-error-correcting BCH code. The *Kerdock* codes, discovered in 1972 [27] are a kind of

This is the best form of the definition to remember, because it applies also to nonbinary codes. However, in the binary case,

$$M^{(2i)}(x) = M^{(i)}(x), \quad \text{for all} \quad i \ ,$$

and so we have

$$g(x) = l.c.m. \ \{M^{(1)}, M^{(3)}, \ldots\} \ ,$$

terminating at the largest odd number $\leq d-1$. One says "designed distance" rather than "distance," because the actual minimal distance of this code may exceed d. It will never be less.

We now give some key examples of BCH codes.

Single-error-correcting codes. Here $d = 3$, so we take $g(x) = M^{(1)}(x)$. This is a *Hamming code*, with parameters

$$n = 2^m - 1, \quad k = 2^m - 1 - m, \quad d = 3 \quad (m \geq 2) \ . \tag{5}$$

By adding an "overall parity check" (i.e. appending a 0 or 1 to make the sum of the digits in each codeword equal to 0), we obtain a code with

$$n = 2^m, \quad k = 2^m - 1 - m, \quad d = 4 \quad (m \geq 2) \ . \tag{6}$$

For example when $m = 3$, $n = 7$, we obtain an $(8, 16, 4)_2$ code with parity check matrix

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & \xi & \xi^2 & \xi^3 & \xi^4 & \xi^5 & \xi^6 \end{bmatrix} \ . \tag{7}$$

(Certainly ξ is in the extension field $GF(2^3)$, but we can use this matrix to define a binary code via Eq. (2). Alternatively we could obtain a binary parity check matrix from (7) by mapping $GF(2^3)$ to $GF(2)^3$ in the standard way.) The Hamming codes (6) are essentially the same as the Reed-Muller codes $RM(m-2, m)$.

Double-error-correcting codes. Here $d = 5$, so $g(x) = M^{(1)}(x)M^{(3)}(x)$, which in general has degree $2m$, so $k = 2^m - 1 - 2m$. Adding an overall parity check, we obtain

$$n = 2^m, \quad k = 2^m - 1 - 2m, \quad d = 6 \quad (m \geq 3) \ . \tag{8}$$

- Reed-Solomon codes

(see [29] for details).

In the remainder of this section we will discuss only binary codes, i.e. we take $s = 2$.

Reed-Muller codes (1954) are binary linear codes with parameters

$$\begin{aligned} n &= 2^m, \quad m \geq 0 \ , \\ k &= 1 + \binom{m}{1} + \cdots + \binom{m}{r} \ , \\ d &= 2^{m-r} \ , \end{aligned}$$

where r, an integer in the range $0 \leq r \leq m$, is called the *order* of the code. An r-th order Reed-Muller code of length n is usually denoted by $RM(r, m)$. (For nonbinary generalizations see [7].)

Furthermore

$$RM(r, m)^{\perp} = RM(m - r - 1, m) \ . \tag{4}$$

Cyclic codes are linear codes with the property that if $c = c_0 c_1 \cdots c_{n-1} \in C$ then also $c_{n-1} c_0 c_1 \cdots c_{n-2} \in C$. We represent vectors by polynomials, representing c by $c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$. Provided $x^n = 1$, $xc(x)$ represents a cyclic shift of c! Therefore a cyclic code is represented by an ideal in the ring $GF(2)[x]/(x^n - 1)$. This is a principal ideal domain, so every cyclic code has a unique generator polynomial $g(x)$. In face we can take $g(x)$ to be the lowest degree nonzero polynomial in the code. Furthermore $g(x)$ divides $x^n - 1$, and the code has dimension $k = n - \deg g$.

BCH codes (1959, 1960). Let $M(x)$ be a primitive irreducible polynomial of degree m. Then $M(x) | x^n - 1$, where $n = 2^m - 1$. For example, if $m = 3$, $n = 7$,

$$x^7 - 1 = (x - 1)(x^3 + x + 1)(x^3 + x^2 + 1) \ ,$$

and we can take $M(x) = x^3 + x + 1$. (All this is mod 2, of course, although the construction of BCH codes is easily generalized to larger alphabets.)

If ξ is a root of $M(x)$, then $\xi^n = 1$. We let $M^{(i)}(x)$ denote the minimal polynomial of ξ^i. Then the simplest and most important class of BCH codes is defined as follows. A BCH code of length $n = 2^m - 1$ and designed distance d is the cyclic code with generator polynomial

$$g(x) = l.c.m. \ \{M^{(1)}, M^{(2)}, M^{(3)}, \ldots, M^{(d-1)}\} \ .$$

and H. The dual of an $(n, s^k, d)_s$ code is an $(n, s^{n-k}, d^\perp)_s$ code, where $d^\perp$ is the minimal distance of the dual. We also call $d^\perp$ the *dual distance* of C.

There are important connections between coding theory and statistics, especially the Design of Experiments, that are perhaps not sufficiently widely known. The dual distance $d^\perp$ plays a key role here. For example, the codewords of an $(n, s^k, d)_s$ code form a *fractional factorial design* of *resolution* $d^\perp$. Some of the binary nonlinear codes described below (the Nordstrom-Robinson code, for instance) provide orthogonal arrays that have fewer runs than those constructed by classical techniques. See [21] for more information about the connections between coding theory and the Design of Experiments.

The *Hamming weight* of a vector u, denoted by $wt(u)$, is the number of nonzero components. Thus $d(u, v) = wt(u - v)$. The *Hamming weight enumerator* of a code C *with respect to a codeword* $u \in C$ is given by

$$W_{C,u}(x, y) = \sum_{v \in C} x^{n-d(u,v)} y^{d(u,v)} \ ,$$

and the (average) Hamming weight enumerator of C is

$$W_C(x, y) = \frac{1}{M} \sum_{u \in C} W_{C,u}(x, y) \ .$$

For a linear code this simplifies to

$$W_C(x, y) = \sum_{u \in C} x^{n-wt(u)} y^{wt(u)} \ .$$

The *MacWilliams identity* ([29, Chap. 6]) relates the Hamming weight enumerators of a linear code and its dual:

$$W_{C^\perp}(x, y) = \frac{1}{M} W_C(x + (s-1)y, x - y) \ . \tag{3}$$

3. Some classical codes

Many families of linear codes were constructed in the 1950's and early 1960's, the most important of which were:

- Reed-Muller codes
- cyclic codes
- BCH codes

Algebraic Coding Theory: Recent Developments Related to $\mathbb{Z}_4$

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

1. Introduction

The main aim of this talk is to serve as an introduction to the papers (listed in historical order) [17], [10], [20], [15], [11], concentrating on the basic theory. For applications, practical and theoretical, see [8], [28], [7], [6].

2. History and terminology

Coding theory began in the late 1940's with the work of Shannon, Hamming, Golay and others (see [31], [5], [3], [29]). A *code* of *length* n and *size* M consists of a set of M vectors each with n components, the components being taken from some *alphabet* S. In the classical theory S is a Galois field of order s, denoted by $GF(s)$ (later we will allow more general alphabets). The *Hamming distance* $d(u,v)$ between two vectors u, v is the number of components where they differ. If d is the minimal Hamming distance between distinct codewords then the code can correct $[(d-1)/2]$ errors.

At this point a code is just a subset of S^n, and we say that it has parameters $(n, M, d)_s$. (Later we will use this same notation even when S is not a field.)

A *linear* code is a *subspace* of S^n. A linear code C can be specified by a *generator matrix*, that is, a $k \times n$ matrix G (of full rank) over S such that C is the row space of G:

$$C = \{uG : \ u \in S^k\} \ . \tag{1}$$

Then C contains s^k codewords, where k is called the *dimension* of C. The code may also be defined as the null space of the *parity check* matrix. This is an $(n-k) \times n$ matrix H (of full rank) such that

$$C = \{c \in S^n : \ Hc^{tr} = 0\} \ . \tag{2}$$

To every linear code C there corresponds its *dual code* $C^\perp$, obtained by interchanging G

Algebraic Coding Theory: Recent Developments Related to $\mathbb{Z}_4$

N. J. A. Sloane

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

March 9, 1994

ABSTRACT

This talk is intended to serve as an introduction to a number of recent papers by various authors that make use of codes over $\mathbb{Z}_4$ (the integers modulo 4) to greatly simplify the construction of a number of notorious nonlinear binary codes, in particular the codes of Nordstrom-Robinson, Preparata, Kerdock, Goethals, Delsarte-Goethals, Best and Julin. By expanding classical coding theory in this way, allowing alphabets that are rings rather than fields, we are able to give extremely simple descriptions of these codes.