**Serdica**
Mathematical Journal
**Сердика**
Математическо списание

Serdica Math. J. **27** (2001), 263-278

**Serdica**
Mathematical Journal

Bulgarian Academy of Sciences
Institute of Mathematics and Informatics

# DIVISIBLE CODES – A SURVEY

Harold N. Ward

*Communicated by R. Hill*

Abstract. This paper surveys parts of the study of divisibility properties of codes. The survey begins with the motivating background involving polynomials over finite fields. Then it presents recent results on bounds and applications to optimal codes.

**1. Introduction.** Let $C$ be an $[n, k, d]_q$ code over $GF(q)$, where $q$ is a power of the prime $p$. Following Assmus and Mattson [2], we shall construe $C$ as a $k$-dimensional $GF(q)$-vector space endowed with an indexed set $\Lambda = \Lambda(C)$ of $n$ *coding* (or *coordinate*) *functionals* $\lambda_1, \ldots, \lambda_n$ that belong to the dual vector space $C^*$. A member $c$ of $C$ is encoded as the $n$-tuple $(\lambda_1(c), \ldots, \lambda_n(c))$ in the *ambient space* $GF(q)^n$. The weight $w(c)$ is the number of nonzero components of this $n$-tuple, and $d$ is the smallest nonzero weight among members of $C$. It may be that some $\lambda_i$ is a scalar multiple of some other $\lambda_j$, but one tacitly assumes that none of the $\lambda_i$ is the 0 functional. The $\lambda_i$ must satisfy the *coding axiom*: if $c \in C$

2000 *Mathematics Subject Classification:* 94B05.

*Key words:* divisible code, theorem of Ax, Reed-Muller code, group algebra, Delsarte-McEliece theorem, polarization, self-dual code, Gleason-Pierce theorem, Griesmer bound, optimal code.

and $c$ encodes to the all-0-word, then $c = 0$. The arc $\mathcal{K} = \mathcal{K}_C$ in the projective space $PG(C^*)$ based on $C^*$ is the multiset of points for which the multiplicity $\mathcal{K}(P)$ is the number of times that $P$ is represented by a member of $\Lambda$.

If $\Lambda' \subseteq \Lambda$, the *shortened* code $C'$ of $C$ determined by $\Lambda'$ is the subspace $\{c|\lambda_i(c) = 0 \text{ for all } \lambda_i \in \Lambda'\}$, with $\Lambda(C') = \{\lambda_j|\lambda_j \notin \Lambda'\}$. On the other hand, the *residual* code determined by $\Lambda'$ is $C/K$, where

$$K = \left\{c \in C|\lambda_i(c) = 0 \text{ for all } \lambda_i \in \Lambda'\right\}$$

and $\Lambda(C/K)$ is the set of functionals induced by the members of $\Lambda'$ on $C/K$. For the most common situation, that of the residual code $C/\langle c\rangle$ of a member $c$ of $C$, one takes $\Lambda' = \{\lambda_i|\lambda_i(c) = 0\}$.

If $D$ is a subspace of the code $C$, the *support* $\operatorname{supp}(D)$ of $D$ is the set of coding functionals of $C$ that do not vanish identically on $D$. The *support length* $n(D)$ is $|\operatorname{supp}(D)|$. For a codeword $c$, we put $|c| = \operatorname{supp}(\langle c\rangle)$; $w(c)$ is the support length of $\langle c\rangle$. The nonzero members of $\langle c\rangle$ form a *ray* of weight $w(c)$. When $D$ is regarded as a code with $\Lambda(D) = \operatorname{supp}(D)$, one calls $D$ a subcode of $C$ to emphasize this structure. Suppose that $P$ is represented by a member of $\operatorname{supp}(D)$. Then the restrictions to $D$ of the $\mathcal{K}_C(P)$ functionals $\lambda_i$ for which $P = \langle\lambda_i\rangle$ all represent a point $Q$ of $\mathcal{K}_D$ with multiplicity $\mathcal{K}_D(Q) \geq \mathcal{K}_C(P)$. We shall say that point $P$ of $\mathcal{K}_C$ is *contained in* point $Q$ of $\mathcal{K}_D$. To ease visualization we shall often work with a generator matrix of a code. A column displays the values of the corresponding coding functional on the members of the code selected for the rows of the matrix.

One final item of record: if $C$ is a $k$-dimensional code over $GF(q)$, then

$$\sum_{c\in C} w(c) = n(C)(q-1)q^{k-1},$$

or equivalently,

$$\sum w(c) = n(C)q^{k-1},$$

where this sum is taken over representatives of the rays in $C$. This well-known *average weight equation (AWE)* is the second of the MacWilliams identities. It is often proved separately by double-counting pairs of codewords and coordinate values. As we all know, $AWE$ is awesomely useful!

A linear code $C$ is said to be *divisible* by $\Delta$ if the weight of every codeword is a multiple of $\Delta$. We say that $\Delta$ is a divisor of $C$ and write $\Delta|C$. The following fact is elementary but important [27, Theorem 1]:

**Theorem 1.** *If $\Delta$ is relatively prime to the field size $q$, then a code divisible by $\Delta$ (with no 0 coordinates) is a $\Delta$-fold* replicated *code: $\Delta | \mathcal{K}_C(P)$ for all $P$.*

Such a replicated code is equivalent to one obtained from a shorter code by repeating each coordinate $\Delta$ times.

## 2. The theorem of Ax.

Several families of classical codes exhibit nontrivial divisibility, and the most prominent family comprises the generalized Reed-Muller (GRM) codes. The theorem of Ax [3] describes their divisibilities.

**Theorem 2.** *The $r$-th order generalized Reed-Muller code $R_q(r, m)$ over the field $GF(q)$ is divisible by $q^{\lceil m/r \rceil - 1}$. Moreover, if $p$ is the prime dividing $q$, this divisor is the highest power of $p$ that divides the code.*

This theorem was the end of a sequence of theorems about the existence of zeros for polynomials in several variables that were proved in response to a conjecture of Artin. The intermediate results were established by Chevalley and Warning in the early 1930s.

Ax's theorem leads naturally to two sorts of generalizations. Let $V$ be the underlying vector space upon which $R_q(r, m)$ is based. That is, $V$ has dimension $m$ over $GF(q)$, and the codewords of $R_q(r, m)$ are the evaluation vectors on $V$ of polynomials in $m$ variables of degree at most $r$ over $GF(q)$. The affine general linear group $AGL(V)$ consists of the transformations $v \to Av + b$, where $A$ is a nonsingular linear transformation from $V$ to $V$ (a member of the general linear group $GL(V)$) and $b \in V$. The group $AGL(V)$ induces automorphisms of $R_q(r, m)$ by the induced change of polynomial variables. On the one hand, the translation subgroup $T(V)$, consisting of the transformations with $A$ the identity, is an elementary Abelian group of order $q^m$. Because of the action of $T(V)$, the GRM codes can be realized as ideals in the group algebra of $T(V)$ over $GF(q)$ [20]. On the other hand, $GL(V)$ contains an element of order $q^m - 1$ permuting the nonzero members of $V$ (leading to the famous *Singer cycle* on $PG(V)$). Puncturing $R_q(r, m)$ by omitting the evaluation at 0 produces a cyclic code $R_q(r, m)^*$ which is, in fact, a subcode of a BCH code whose designed minimum weight is that of $R_q(r, m)^*$ itself [1, Section 5.5]. Thus the GRM codes arise as (extended) group algebra codes for which the group algebra is semisimple (the group order is relatively prime to $q$) in the cyclic case, and as far as possible from being semisimple in the elementary Abelian case. Both of these aspects of the GRM codes have served as inspirations for the study of divisibility properties of other families of group algebra codes.

**2.1. The semisimple case.** Delsarte and McEliece proved a major generalization for Abelian groups in the semisimple case, using Ax's techniques [9]. It is rather complicated, but for a cyclic code over the prime field $GF(p)$, it becomes an easily stated earlier theorem of McEliece [22].

**Theorem 3.** *Let $C$ be a cyclic code over $GF(p)$, $p$ a prime, whose length $n$ is prime to $p$. Let $x$ be the cyclic shift of order $n$ involved in the definition of $C$, and let $E$ be the set of eigenvalues of $x$ on $C$. Then the highest power of $p$ dividing $C$ is $p^e$, where $m = (p-1)(e+1)$ is the smallest multiple of $p-1$ for which a product of $m$ members of $E$ (allowing repetitions) is equal to* 1.

(Note that when 1 is an eigenvalue $C$ contains the all-1 word and $e = 0$.) For example, if $\zeta$ is a primitive 11-th root of unity over $GF(3)$, the 5-dimensional "even-like" cyclic subcode of the $[11, 6, 5]_3$ ternary Golay code of words with weight divisible by 3 can be taken to have check polynomial equal to the minimal polynomial of $\zeta$. Then $E = \left\{\zeta, \zeta^3, \zeta^4, \zeta,^5, \zeta^9\right\}$. No product of two members of $E$ is 1, but $\zeta \times \zeta \times \zeta^4 \times \zeta^5 = 1$. Thus $e = 1$ (as is obvious - the word weights are 6 and 9!).

The fact that a product of $m$ eigenvalues of $x$ is 1 means that the code $C$, as a space on which the cyclic group $\langle x \rangle$ acts, has a nontrivial $\langle x \rangle$-invariant multilinear form of degree $m$. Such forms can be produced from $\langle x \rangle$-invariant functions, using the inclusion-exclusion polarization formula developed in [26][1]. In particular, if $C$ is divisible by $p^e$, the function $c \to w(c)p^{-e}$ can be read modulo $p$ to produce such a function on $C$. This was the point of departure for the paper [28] that led to generalizations both of Theorem 3 and of results in [9]. Among the codes studied in the paper are one-sided ideals that are direct summands of the group algebra $GF(q)G$ of a finite group $G$. Such codes include group algebra codes in the semisimple case.

Some recent researches deal with the binary case of McEliece's theorem. In one direction, the theorem was reproved and extended to cyclic codes over $\mathbb{Z}_{2^l}$, $l$ arbitrary, by Calderbank, Li, and Poonen [8]. Their methods involve local fields, and they suggest that their strategy will extend to group ring codes for Abelian groups over $\mathbb{Z}_q$, where $q$ is a prime power relatively prime to the group order. In another direction, Hollmann and Xiang have used the theorem to determine weight distributions of a number of binary cyclic codes of primitive length ($n = 2^m - 1$) whose generator polynomials are products of few irreducible

[1] When I wrote [26], I was sure the idea was not new, but I did not discover a source. Recently I found a number of papers that deal extensively with this form of polarization for modules (some preceding mine), including a long series by A. Prószyński beginning with [23].

polynomials [14, 15]. Their work involves developing methods for computing the required shortest product of eigenvalues equal to 1.

**2.2. The radical case.** When GRM codes over $GF(q)$ are viewed as ideals of the group algebra of an elementary Abelian $p$-group, $p$ the prime dividing $q$, one is confronted with what might be called the *radical* case, since the radical of the group algebra has codimension 1 (it is the set of elements whose coefficient sum is 0). The paper [31] dealt with codes that are powers of the radical of $GF(q)G$, where $G$ is a $p$-group, and certain generalizations. The description of their divisibility properties required the results of [29]. These provide criteria for determining the highest power of $p$ dividing a code in terms of computations made from a spanning set of the code. The criteria involve lifting components of codewords back to a $p$-adic field by means of Teichmüller representatives. Methods employed in their development are similar to those used in [3] and [9], and they make use of polarization formulas.

The criterion for divisibility for binary codes is particularly easy to describe. It can be proved from the classic formula

$$w(a+b) = w(a) + w(b) - 2w(a * b)$$

for binary words $a, b$, where $a * b$ is the component-wise product of $a$ and $b$. This formula itself is the prototype for the polarization process applied to codes. Let $M$ be a generator matrix for a binary code, and let $M^0$ be $M$ regarded as a matrix of 0s and 1s in $\mathbb{Z}$. The $m$-fold dot product of a collection of rows $r_1, \ldots, r_m$ of $M^0$ is the sum of the entries in $r_1 * \cdots * r_m$. In this binary case this is simply the weight of $r_1 * \cdots * r_m$ with the $r_i$ taken as the original binary words; but it is the computation in $\mathbb{Z}$ that generalizes.

**Proposition 4.** *The code with generator matrix $M$ has $2^e$ as a divisor exactly when for all positive $m \leq e$, $2^{e-m+1}$ divides the $m$-fold dot product of all collections of $m$ rows of $M^0$, duplications allowed.*

For example, the matrix

$$\begin{bmatrix} 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1 \\ 1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&0 \\ 1&1&1&1&0&0&0&0&1&1&1&1&0&0&0&0 \\ 1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0 \\ 1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0 \end{bmatrix}$$

generates $R_2(1,4)$ and satisfies the criterion with $e = 3$ (as it should, by Ax's theorem!).

For ternary codes, the analogous result is

**Proposition 5.** *Let $M$ be a generator matrix for a code over $GF(3)$, with $GF(3) = \{0, 1, -1\}$, and let $M^0$ be the matrix obtained by reading the members of $GF(3)$ as integers. Then $3^e$ is a divisor of the code exactly when $3^{e+1-m}$ divides all $2m$-fold dot products of the rows of $M^0$ (again with duplications allowed), for all positive $m \le e$.*

Here is a generator matrix for the $[11, 5, 6]_3$ subcode of the Golay code mentioned before:

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

Of course, in this case the check amounts to verifying that the code is self-orthogonal. For general $q$ the divisibility criteria are more complicated. They were recently used in all their detail by Chris Boner in his thesis [5, 6], in which he determined the divisors of the projective GRM codes.

Theorem 2 is reproved in [29], but the proof is quite close to that of Ax. Rather unexpectedly, when the divisibility criteria are applied to the codes in [31] and tailored to the situation there, a bin-packing problem emerges for finding the divisor! The divisors of the radical powers of the group algebras of several classes of $p$-groups were determined in [31]. Further investigations along these lines appear in the thesis of Deirdre Smeltzer [25]. A major tool in these $p$-group investigations is the *Jennings basis* for powers of the radical of the group algebra [17] (see also [16, Chapter VIII]). This basis was important in the paper of Landrock and Manz [20].

## 3. The divisible code bound.

Theorem 1 implies that if $C$ is an $[n, k]_q$ code divisible by $\Delta$, and $\Delta$ is relatively prime to $q$, then $k \le n/\Delta$. The *divisible code bound* removes the relatively prime restriction. With $p$ the prime dividing $q$, let $v$ be the $p$-adic valuation on $\mathbb{Z}$: $v(x)$ is the exponent of the highest power of $p$ dividing $x$, with $v(0) = \infty$.

**Theorem 6.** *Let $C$ be an $[n, k]_q$ code whose nonzero word weights lie in the sequence $(b - m + 1)\Delta, \ldots, b\Delta$ of $m$ consecutive multiples of $\Delta$. Then*

$$kv(q) \le m(v(\Delta) + v(q)) + v\left(\binom{b}{m}\right).$$

This bound was proved in [30] by character-theoretic means that were inspired by polarization formulas. A more combinatorial proof using divisibility properties of Stirling numbers (of both kinds!) appears in [33]. There the divisible code bound is a special case of a more general bound: let $C$ be an $[n,k]_q$ code whose nonzero weights are among $w_1,\ldots,w_m$. Then

$$kv(q) \le \sum_j v(w_j) + \max_{i:i\le m}\{iv(q) - v(i!)\}.$$

Both of these bounds can be disappointingly weak, but there are cases of equality. For example, the $[11,5,6]_3$ Golay subcode has $\Delta = 3$, $m = 2$, and $b = 3$. The right side of the divisible code bound is indeed $2 \times (1+1) + v(\binom{3}{2}) = 5$.

The main use of the bound was a sharpening of the upper bound on the minimum weight of type I binary self-dual codes that comes from Gleason's theorem on the form of the weight enumerator of such codes (see the comprehensive report [24] by Rains and Sloane on self-dual codes). For an $[n,n/2,d]_2$ self-dual code, the Gleason bound is $d \le 2\lfloor n/8\rfloor + 2$; asymptotically this is $d \lesssim n/4$. Conway and Sloane improved this to $d \lesssim n/5$ (with a small bounded error term). When the divisible code bound is applied to the subcode of words with weights divisible by 4, one obtains the asymptotic bound $d \lesssim n/6$, with an error term that is $O(\log n)$ (coming from the binomial coefficient). Finally, Rains showed that $d \le 4\lfloor n/24\rfloor + 4$, except when $n \equiv 22 \pmod{24}$, when the "$+\,4$" becomes a "$+\,6$." Even here, however, the divisible code bound rules out the possibility of equality in some cases.

For type II, III, and IV self-dual codes, the divisible code bound generally matches the bound obtained by applying the appropriate version of Gleason's theorem – provided that the binomial coefficient term can be controlled! That term cannot be dispensed with in general, as the example suggests, but one might hope it could be tightened.

The classification of divisible formally self-dual codes (codes with the same weight-enumerators as their duals) into five types in the Gleason-Pierce theorem (see [24, Section 4.1]) has a divisible code version [27]:

**Theorem 7.** *Suppose an $[n,n/2]_q$ code $C$ is divisible by $\Delta > 1$. Then the possibilities for $q$ and $\Delta$ are limited to the following five types:*

*Type I* $q = \Delta = 2$.
*Type II* $q = 2$, $\Delta = 4$, *and* $C$ *is self-dual.*
*Type III* $q = \Delta = 3$ *and* $C$ *is self-dual.*
*Type IV* $q = 4$, $\Delta = 2$, *and* $C$ *is Hermitian self-dual.*
*Type V* $\Delta = 2$ *and* $C$ *is equivalent to the* 2*-fold replication of* $GF(q)^{n/2}$.

In this classification, codes that are formally but not actually self-dual appear in types I and V. The divisible code bound leads to the following result upon which the previous theorem can be based [33, Section 6]:

**Proposition 8.** *For a given constant* $\delta > 1$, *consider* $[n, k]_q$ *codes that are divisible by* $\Delta$ *and for which* $k \geq n/\delta$. *Then* $\Delta$ *is bounded; and if* $\Delta > \delta$, *then* $q$ *is also bounded.*

**4. Optimal codes.** For given $k, q, d$, let $n_q(k, d)$ be the smallest value of $n$ among $[n, k, d]_q$ codes, a code with that $n$ being called *length-optimal.* Then one has the classic *Griesmer bound*:

$$n_q(k, d) \geq g_q(k, d) = \sum_{j=0}^{k-1} \left\lceil \frac{d}{q^j} \right\rceil .$$

A code attaining this bound is called a *Griesmer code.* For such a code, the last term in the sum, $\lceil d/q^{k-1} \rceil$ (traditionally labelled $s$), is the largest multiplicity among points in the corresponding arc $\mathcal{K}$. A point $P$ with $\mathcal{K}(P) = s$ will be called an *endpoint*, since such points occur at the end of the usual generator matrix for Griesmer codes, represented by the last $s$ columns. Shortening at an endpoint $P$, that is, shortening with $\Lambda'$ equal to the set of $\lambda_i$ for which $\langle \lambda_i \rangle = P$, produces a Griesmer code of dimension $k - 1$.

Dodunekov and Manev proved that for a binary Griesmer code, the highest power of 2 dividing the minimum weight of the code is a divisor of the code itself [10]. Making use of the criteria in [29], one can extend this result to Griesmer codes over prime fields [32]. This general theorem has recently been reproved by Landjev using polynomial methods [19]. These same methods were used to show the divisibility of certain of the codes arising in the study of $(q^2+q+2, q+2)$-arcs by Ball, Hill, Landjev, and me [4].

**Theorem 9.** *Let* $C$ *be a Griesmer code over* $GF(p)$, $p$ *a prime. Then if* $p^e$ *divides the minimum weight,* $p^e$ *is a divisor of the code.*

This theorem places restrictions on the weight enumerator of a Griesmer code, and they are often strong enough to show that a particular set of parameters for such a code is impossible. For example, $g_3(5,45) = 68$, but it has been known for some time that there is no $[68,5,45]_3$ code. The theorem quickly rules such a code out: the dual code would have no words of weight 1 or 2, since the corresponding shortenings violate the Griesmer bound. As the only nonzero weights for the code would be 45, 54, and 63, the first three MacWilliams identities determine the weight enumerator. But the solution does not have integer values.

On the other hand, there *is* a $[69,5,45]_3$ code, discovered and shown to be unique by Hill and van Eupen [12]. It is also divisible by 9, a fact illustrating what seems to be a fairly common phenomenon: divisibility of length-optimal codes. Such divisibilities can often be proved by careful examination of residual codes and judicious applications of *AWE.* The thesis of Chris Jones contains many examples of such divisibilities for optimal ternary codes that are not Griesmer codes [18].

There seems to be sufficient evidence to support the following conjecture:

**Conjecture 10.** *Let $C$ be a $[g_q(k,d),k,d]_q$ Griesmer code, where $q$ is a power of the prime $p$. Suppose that $p^e|d$, with $p^e \geq q$. Then $C$ is divisible by $p^{e+1}/q$.*

In what follows, we shall prove this conjecture for $q = 4$ by rather elementary means.

**Lemma 11.** *Let $C$ be a $[g_q(k,d),k,d]_q$ Griesmer code. Let $s = \lceil d/q^{k-1} \rceil$ and put $t = d-(s-1)q^{k-1}$. Then the number of endpoints of $C$ is at least $g_q(k,t)$.*

Proof. We have $g_q(k,d) = \mathcal{K}_C(PG(C^*))$. If $e$ is the number of endpoints, then

$$\begin{aligned}\mathcal{K}_C(PG(C^*)) &\leq se + (|PG(C^*)| - e)(s-1) \\ &= e + (s-1)\frac{q^k-1}{q-1} = e + \sum_{j=0}^{k-1}(s-1)q^{k-1-j}.\end{aligned}$$

Therefore

$$e \geq g_q(k,d) - \sum_{j=0}^{k-1}(s-1)q^{k-1-j} = \sum_{j=0}^{k-1}\left\lceil \frac{d-(s-1)q^{k-1}}{q^j} \right\rceil = g_q(k,t). \qquad \square$$

In the same vein, we have

**Lemma 12.** *Let $D$ be an $l$-dimensional Griesmer subcode of the $[g_q(k,d),k,d]_q$ Griesmer code $C$. That is, $n(D)=g_q(l,d)$. Then each endpoint of $D$ contains at least*

$$q^{k-l}-\left\{q^{k-l}\left\lceil\frac{d}{q^{k-1}}\right\rceil-\left\lceil\frac{d}{q^{l-1}}\right\rceil\right\}$$

*endpoints of $C$ (and this number is positive).*

Proof. The positivity follows from the fact that $\lceil x\rceil<x+1$:

$$q^{k-l}\left\lceil\frac{d}{q^{k-1}}\right\rceil-\left\lceil\frac{d}{q^{l-1}}\right\rceil<q^{k-l}\left(\frac{d}{q^{k-1}}+1\right)-\frac{d}{q^{l-1}}=q^{k-l}.$$

Let $Q$ be an endpoint of $D$. For a given member $\mu$ of $D^*$, the number of $\lambda$ in $C^*$ for which $\lambda|D=\mu$ is $q^{k-l}$. Suppose that $e$ endpoints of $C$ are contained in $Q$. Then

$$\mathcal{K}_D(Q)=\left\lceil\frac{d}{q^{l-1}}\right\rceil\le e\left\lceil\frac{d}{q^{k-1}}\right\rceil+(q^{k-l}-e)\left(\left\lceil\frac{d}{q^{k-1}}\right\rceil-1\right).$$

That is,

$$\left\lceil\frac{d}{q^{l-1}}\right\rceil-q^{k-l}\left(\left\lceil\frac{d}{q^{k-1}}\right\rceil-1\right)\le e,$$

the desired inequality. □

Here are some consequences of these two lemmas.

**Proposition 13.** *Let $C$ be a $[g_q(k,d),k,d]_q$ Griesmer code, and suppose that $q|d$. Then $C$ is divisible by $p$, the prime dividing $q$.*

Proof. For fixed $d$, induct on $k$; the proposition is trivially true at $k=1$. We present functions on $C$ by means of polynomials, as in the construction of Reed-Muller codes [1, Section 5.4]. Thus let $c_1,\dots,c_k$ be a basis of $C$ and let $x_1,\dots,x_k$ be indeterminates corresponding to the components relative to $c_1,\dots,c_k$. As usual, we use the abbreviation $x=(x_1,\dots,x_k)$. Then any function on $C$ with values in $GF(q)$ is represented by a polynomial $f(x)$, the value of the function on $c=\sum\xi_i c_i$ being $f(c)=f(\xi_1,\dots,\xi_k)$. Interpret each $\lambda\in C^*$ as the linear polynomial $\lambda(x)=\sum\lambda(c_i)x_i$, and let $\Lambda(C)=\{\lambda_1,\dots,\lambda_n\}$. Then if $\overline{w}(x)=\sum_{i=1}^{n}\lambda_i(x)^{q-1}$, we have $\overline{w}(c)\equiv w(c)\bmod(p)$ for $c\in C$. Let $P$ be an endpoint of $C$, with $P=\langle\lambda\rangle$. Change variables in $GF(q)[x_1,\dots,x_k]$ to make $\lambda(x)$ one of the new variables, and set $\overline{w}(x)=\sum\overline{w}_j(x)\lambda(x)^j$, where the coefficients $\overline{w}_j(x)$ involve the remaining new variables. Since $P$ is an endpoint, the shortening of

$C$ at $P$ is a Griesmer code of dimension $k-1$. This code is divisible by $p$, by induction. Thus $\overline{w}(c) = 0$ when $\lambda(c) = 0$, so that $\overline{w}_0(c) = 0$ for all $c$. The key point now is that since $\overline{w}_0(x)$ has degree at most $q-1$, it must be the 0 polynomial, and so $\lambda(x)$ is a divisor of $\overline{w}(x)$.

By Lemma 11, $C$ has at least $g_q(t,k)$ endpoints, where

$$t = d - (\left\lceil d/q^{k-1} \right\rceil - 1)q^{k-1}.$$

As $q|d$ and $k > 1$, we have $t \geq q$ and $g_q(t,k) \geq q+1$. Since $GF(q)[x_1, \ldots, x_k]$ is a unique factorization domain, $\overline{w}(x)$ must now be divisible by the product of at least $q+1$ distinct linear factors, and that violates the fact that $\overline{w}(x)$ has degree at most $q-1$. Consequently $\overline{w}(x) = 0$ and $p$ is a divisor of $C$. □

For example, Jones has used this result to show that there is no $[85,5,72]_8$ Griesmer code, as part of a research project with Angela Matney and me. By Proposition 13, the possible nonzero codeword weights of such a code are the even numbers from 72 to 84. Standard residual arguments rule out 74 and 82. If $w(c) = 78$, the residual at $c$ is a $[7,4,4]_8$ code. Producing a word of weight 4 in the residual requires a codeword $c'$ with $n(\langle c, c' \rangle) = 82$. Then *AWE* demands that $78+$ eight values from $\{72,76,78,80,84\} = 8 \times 82$. But $8 \times 82 = 78 + 7 \times 72 + 74$ shows no such combination exists, and $A_{78} = 0$ (with the usual weight enumerator notation of $A$s for the code and $B$s for the dual). Again by a standard argument from shortenings, one finds that $B_1 = B_2 = B_3 = 0$. The first four MacWilliams identities have $A_{72}, A_{76}, A_{80}$, and $A_{84}$ as unknowns; but the solution gives $A_{84} = -1470$.

**Theorem 14.** *Let $C$ be a $[g_4(k,d),k,d]_4$ code for which $2^e|d$, with $t \geq 2$. Then $2^{e-1}$ is a divisor of $C$.*

Proof. Induct on both $e$ and $k$: the theorem is true for $e = 2$ by Proposition 13, and it is true trivially for $k = 1$. First scale the columns of a generator matrix of $C$ so that for each point $P$, the $\mathcal{K}_C(P)$ columns corresponding to $P$ are all the same. Then let $c \in C, c \neq 0$, and rescale the columns of the generator matrix so that the nonzero entries in $c$ are all 1s. If $c$ has 0 entries in the columns for some endpoint, then $c$ can be regarded as a member of the shortening of $C$ at that endpoint. Since the shortening is a Griesmer code, $2^{e-1}|w(c)$ by induction. Thus assume that $c$ has 1s at each endpoint (that is, 1s in all the columns corresponding to endpoints). The strategy now is to find a minimum weight word $z$ that has each of the nonzero members $1, \alpha, \beta$ of $GF(4)$ appearing at some endpoint. If that can be done, we invoke *AWE* in the form that counts by rays:

$$w(c) + w(z) + w(z + c) + w(z + \alpha c) + w(z + \beta c) = 4n(\langle z, c\rangle).$$

In this equation, $z + c, z + \alpha c, z + \beta c$ all belong to Griesmer codes that are shortenings of $C$, and their weights are divisible by $2^{e-1}$ by induction. For the right side, $n(\langle z, c\rangle) - w(z)$ is the weight of the image of $c$ in the residual code $C/z$, a Griesmer code of minimum weight $d/4 = 2^{e-2}$ and thus divisible by $2^{e-3}$, by induction. Rewriting the equation as

$$w(c) = 4\{n(\langle z, c\rangle) - w(z)\} + 3w(z) - w(z + c) - w(z + \alpha c) - w(z + \beta c)$$

shows that, indeed, $2^{e-1}|w(c)$.

We are assuming that $e \geq 3$, so that any 2-dimensional Griesmer subcode is a replicated simplex code [32, Corollary 5] and any of its nonzero words has weight $d$. In particular, we may take $k \geq 3$. Let $D$ be a 3-dimensional Griesmer subcode, and let $D'$ be a 2-dimensional Griesmer subcode of $D$. If $d = 8m$, Lemma 12 shows that each endpoint of $D'$ contains at least $4-\{4\lceil m/2\rceil - 2m\} \geq 2$ endpoints of $D$. Set up three rows for a generator matrix of $C$ from words of $D$, with the first two rows from $D'$, in such a way that we see the submatrix

$$\begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & \gamma & 0 \\ 1 & 0 & \delta & 0 \end{bmatrix}$$

where $\gamma$ and $\delta$ are not 0. Here each column represents the $\lceil d/4^{k-1}\rceil$ columns of an endpoint of $C$ each of which is an endpoint of $D$. Moreover, the second and third columns are in two endpoints of $D$ contained in a single endpoint of $D'$. If a combination of these rows has a 0 anywhere in the displayed columns, then the combination will be in a 2-dimensional Griesmer subcode of $D$ (being 0 at an endpoint of $D$) and thus be a word of weight $d$.

First of all, we may assume that $\gamma = 1$. For if not, then if $1, \gamma, \gamma'$ are the three nonzero members of $GF(4)$, $\gamma' \times [row1] + [row2]$ displays $0, 1, \gamma, \gamma'$ and produces the needed $z$. The matrix above is now

$$\begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & \delta & 0 \end{bmatrix}$$

Then if $\delta = 1$, the combination $\alpha \times [row2] + \beta \times [row3]$ shows $\beta, \alpha, 1, 0$, again providing a desired $z$. Thus we may assume that $\delta \neq 1$. But now if $\delta\delta' = 1$, then $\delta \times [row1] + [row2] + \delta' \times [row3]$ gives $\delta', 1, 0, \delta$ and yields the needed $z$. □

Hill and Landjev [13] showed that $n_4(4,80) = g_4(4,80)+1 = 108$. To see that no $[107,4,80]_4$ code exists from Theorem 14, suppose that $C$ is such a code. Then $C$ is divisible by 8, and its possible word weights are $80, 88, 96, 104$. Known values of $n_4(3,d)$ rule out 96 and 104 by their residual parameters. Letting $A_i(D)$ and $B_j(D)$ refer to the enumerators involving code $D$ in what follows, we find from the MacWilliams identities that $A_{80}(C) = 237, A_{88}(C) = 18$, and $B_2(C) = 75$. Now with thanks to Ray Hill, we construct a $[6,4,2]$ code "dual" to $C$ in the sense of Brouwer and van Eupen [7]. The code space for the dual is indeed $C^*$. We identify $C^{**}$ and $C$ and take representatives $e_1, \ldots, e_6$ of the six rays of 88s in $C$ to be the coordinate functionals. Then the weight of a nonzero $\lambda$ in $C^*$ is $6 - e(\lambda)$, where

$$e(\lambda) = |\{j|\lambda(e_j)=0\}| = A_{88}(\ker\lambda)/3.$$

Using the fact that $\dim(\ker\lambda) = 3$ and $n(\ker\lambda) = 107 - \mathcal{K}_C(\langle\lambda\rangle)$, the first two MacWilliams identities determine the $A_{88}(\ker\lambda)$:

| $\mathcal{K}_C(\langle\lambda\rangle)$ | number of such $\lambda$ | $A_{88}(\ker\lambda)$ | $e(\lambda)$ |
|---|---|---|---|
| 2 | $75\ (= B_2)$ | 0 | 0 |
| 1 | $171\ (= 3(107 - 2B_2/3))$ | 6 | 2 |
| 0 | $9\ (= 255 - 75 - 171)$ | 12 | 4 |

(notice that since no $e(\lambda)$ is 6, the coding axiom is satisfied for $C^*$). Thus $A_2(C^*) = 9, A_4(C^*) = 171, A_6(C^*) = 75$. But now more MacWilliams identities yield $B_3(C^*) = -6$, which will not do!

We close by calling attention to the problem discussed at the end of [32], which may be expanded to this: for odd $q$, does there exist a $[3(q^2+1)/2, 4, 3(q^2-q)/2]_q$ two-weight code, the second weight being $(3q^2-q)/2$? For $q > 3$, such a code would meet the Griesmer bound. When $q = 3$, the $[15,4,9]_3$ sporadic code discovered by van Lint and Schrijver [21] is such a code. Moreover a $[39,4,30]_5$ code arises in the construction of certain difference sets cited in [32]. For $q > 5$, however, the existence of such a code seems to be unknown.

## REFERENCES

[1] E. F. Assmus, Jr., J. D. Key. Designs and Their Codes, Cambridge Univ. Press, Cambridge, 1992; MR **93j**:51003.

[2] E. F. Assmus, Jr., H. F. Mattson, Jr. Error-correcting codes: an axiomatic approach. *Information and Control* **6** (1963), 315–330; MR **31** #3251.

[3] J. Ax. Zeroes of polynomials over finite fields. *Amer. J. Math.* **86** (1964), 255–261; MR **28** #3986.

[4] S. Ball, R. Hill, I. Landjev, H. Ward. On $(q^2+q+2, q+2)$-arcs in the projective plane $\mathrm{PG}(2,q)$. *Des. Codes Cryptogr.* **24** (2001), 205–224.

[5] C. M. Boner. Characterization of Absolute Summands of Categories of Divisible Codes. PhD thesis, University of Virginia, 1999.

[6] C. M. Boner. Maximal weight divisors of projective Reed-Muller codes. *Des. Codes Cryptogr.* **24** (2001), 43–47.

[7] A. E. Brouwer, M. van Eupen. The correspondence between projective codes and 2-weight codes. *Des. Codes Cryptogr.* **11** (1997), 261–266; MR **98a**:94031.

[8] A. R. Calderbank, W.-C. W. Li, B. Poonen. A 2-adic approach to the analysis of cyclic codes. *IEEE Trans. Inform. Theory* **43** (1997), 977–986; MR **98m**:94049.

[9] P. Delsarte, R. J. McEliece. Zeros of functions in finite abelian group algebras. *Amer. J. Math.* **98** (1976), 197–224; MR **53** #2908.

[10] S. M. Dodunekov, N. L. Manev. Minimum possible block length of a linear binary code for some distances. *Problems Inform. Transmission* **20** (1984), 8–14; MR **86i**:94048.

[11] P. P. Greenough, R. Hill. Optimal linear codes over GF(4). *Discrete Math.* **125** (1994), 187–199; MR **94m**:94020.

[12] R. Hill, M. van Eupen. An optimal ternary $[69, 5, 45]$ code and related codes. *Des. Codes Cryptogr.* **4** (1994), 271–282; MR **95g**:94020.

[13] R. Hill, I. Landgev. On the nonexistence of some quaternary codes. In:Applications of Finite Fields (Egham, 1994), Inst. Math. Appl. Conf. Ser. New Ser., **59**, Oxford Univ. Press, New York, 1996, 85–98; MR **98c**:11139.

[14] H. D. L. Hollmann, Q. Xiang. A proof of the Welch and Niho conjectures on cross-correlations of binary $m$-sequences. *Finite Fields Appl.* **7** (2001), 253–286.

[15] H. D. L. Hollmann, Q. Xiang. On binary cyclic codes with few weights. In: Finite Fields and Applications, Proceedings of Fq5, Augsburg, 1999 (Eds D. Jungnickel, H. Niederreiter), Springer-Verlag, New York, 2001, 251–275.

[16] B. Huppert, N. Blackburn. Finite Groups II. Springer-Verlag, Berlin–Heidelberg–New York, 1982; MR **84i**:20001a.

[17] S. A. Jennings. The structure of the group ring of a $p$-group over a modular field. *Trans. Amer. Math. Soc.* **50** (1941), 175–185; MR **3**,34f.

[18] C. M. Jones. Optimal Ternary Linear Codes. PhD thesis, University of Salford, 2000.

[19] I. Landjev. The geometric approach to linear codes. *J. Geom.*, to appear.

[20] P. Landrock, O. Manz. Classical codes as ideals in group algebras. *Des. Codes Cryptogr.* **2** (1992), 273–285; MR **93i**:94017.

[21] J. H. van Lint, A. Schrijver. Construction of strongly regular graphs, two-weight codes and partial geometries by finite fields. *Combinatorica* **1**(1981), 63–73; MR **82d**:05041.

[22] R. J. McEliece. Weight congruences for $p$-ary cyclic codes. *Discrete Math.* **3** (1972), 177–192; *Zbl* **251**.94008.

[23] A. Prószyński. $m$-applications over finite fields. *Fund. Math.* **112** (1981), 205–214; MR **82k**:13014.

[24] E. M. Rains, N. J. A. Sloane. Self-dual codes, Handbook of Coding Theory (Eds V. S. Pless, W. C. Huffman; Asst. Ed. R. A. Brualdi), Chapter 3, Elsevier, Amsterdam, 1998.

[25] D. L. Smeltzer. Properties of codes from difference sets in 2-groups. *Des. Codes Cryptogr.* **16** (1999), 291–306; MR **2000g**:94049.

[26] H. N. Ward. Combinatorial polarization. *Discrete Math.* **26** (1979), 185–197; MR **80m**:05012.

[27] H. N. Ward. Divisible codes. *Arch. Math. (Basel)* **36** (1981), 485–494; MR **83e**:94052.

[28] H. N. Ward. Multilinear forms and divisors of codeword weights. *Quart. J. Math. Oxford Ser. (2)* **34** (1983), 115–128; MR **84h**:94013.

[29] H. N. Ward. Weight polarization and divisibility. *Discrete Math.* **83** (1990), 315–326; MR **91i**:94034.

[30] H. N. Ward. A bound for divisible codes. *IEEE Trans. Inform. Theory* **38** (1992), 191–194; MR **92i**:94024.

[31] H. N. Ward. Divisors of codes of Reed-Muller type. *Discrete Math.* **131** (1994), 311–323; MR **95h**:94042.

[32] H. N. Ward. Divisibility of codes meeting the Griesmer bound. *J. Combin. Theory Ser. A* **83** (1998), 79–93; MR **2000e**:94057.

[33] H. N. Ward. The divisible code bound revisited. *J. Combin. Theory Ser. A* **94** (2001), 34–50.

*Department of Mathematics*
*University of Virginia*
*Charlottesville, V A 22903, USA*
hnw@virginia.edu

*Received August 23, 2001*