Loose Ends

Paper for Chicago AMS Sectional Meeting, October 5–6, 2007

Harold N. Ward
Department of Mathematics, University of Virginia
Charlottesville, VA 22904

Most research projects produce generalizations to be pursued, conjectures to be proved, and special cases to be pondered–often meant to be dealt with at a later date. In this talk, I'll give examples of such postponements from my own work that I hope will be interesting.

Notation is pretty standard, I think. An $[n,k]_q$ code is a linear code of length n and dimension k over the finite field $\mathbb{F}_q$ of q elements. If the minimum weight is d, the code is labeled an $[n,k,d]_q$ code (with occasional liberties if the minimum weight is actually more than d).

1 Quadratic residue codes

The paper [28] describes codes constructed from the Weil representation for symplectic groups, building on my rediscovery of this representation in [27]. Most of [28] concerned two-dimensional symplectic groups, which are then the same as the special linear groups. The corresponding codes are generalizations of extended classical quadratic residue of length $p+1$, p an odd prime, to lengths $q+1$, q an odd prime power. Such generalizations were found at about the same time by Camion [5]. As the referee of [28] said, "No coding theorist is going to read this paper!"; accordingly, the generalizations to lengths $q+1$ were given a more accessible exposition in the paper by van Lint and MacWilliams [19]. In some ways, certain induced representations of the symplectic groups are at the heart of these generalizations, the basis of an approach suggested by Andrew Gleason; the exposition in [35, Chapter 9] follows out this suggestion.

One "loose end" here is the investigation of codes corresponding to symplectic groups of dimension larger than 2. I'll describe some of the ingredients when the field of the code (which is not the same as the field of the symplectic group–that interaction is another story) has characteristic 2.

Let V be a vector space of dimension $2m$ over $\mathbb{F}_q$, q a power of an odd prime p, and let V be endowed with a nondegenerate symplectic form φ. Let R be an integral

domain in which p is invertible and that contains a primitive p-th root of unity, ε. With $\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_p$ the trace function, define $f : V \times V \to R$ by

$$f(x, y) = \varepsilon^{\mathrm{Tr}(\varphi(x,y))}.$$

Then let A be the free R-module with basis elements indexed by the members of V; for $x \in V$, the corresponding basis element is denoted (x). Module A becomes an R-algebra with the definition

$$(x)(y) = f(x, y)(x + y).$$

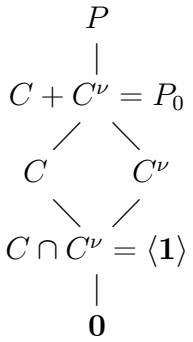
This is a twisted group algebra of the additive group of V. In [27] it is shown that A is a full matrix algebra over R and that the symplectic group $G = Sp(V)$ of φ embeds in A. If W is a maximal totally isotropic subspace in V (of dimension m), then $e = q^{-m} \sum_{x \in W}(x)$ is a primitive idempotent, called an **isotropic idempotent**. The number of these is $(q^m + 1)(q^{m-1} + 1) \cdots (q + 1)$. Thus left multiplication on Ae produces a representation of G; the Weil representations (and perhaps the trivial representation) are the components of this representation. If we replace ε by ε^ν, ν a nonsquare in $\mathbb{F}_p$, and let A^ν be the corresponding algebra, the Weil representation from A^ν is not equivalent to that from A.

Now let $\mathcal{I}_k$ be the set of isotropic subspaces of dimension k. Thus $\mathcal{I}_1$ is just the set of 1-dimensional subspaces of V, that is, the points of the corresponding projective space. Let $R\mathcal{I}_k$ be the free R-module with $\mathcal{I}_k$ as basis. For $k = m$, we can identify the isotropic idempotents with the members of $\mathcal{I}_m$. Let the basis element corresponding to e being denoted e^*. There is a monomial action of G on $R\mathcal{I}_m$ in which the coefficients are ± 1 for which there is a G-homomorphism $Ae \to R\mathcal{I}_m$. The image is an R-submodule of rank $(q^m + 1)/2$, and there is an analogous submodule produced from A^ν.

All of this can be read modulo 2–with some care! With ε now denoting the mod 2 image of the original ε, let $\mathbb{F} = \mathbb{F}_2(\varepsilon)$. Then $\mathbb{F}\mathcal{I}_m$ is effectively the binary permutation module for the action of G on the maximal totally isotropic subspaces of V (the monomial action of G becoming the permutation action by virtue of the ± 1 coefficients). For $a, b \in \mathcal{I}_m$, let $\dim(a \cap b)$ be the dimension of the intersection of the subspaces corresponding to a and b. Map $\mathbb{F}\mathcal{I}_m \to \mathbb{F}\mathcal{I}_m$ by

$$a^* \to \sum_{\dim(a \cap b) \equiv m \pmod 2} b^*.$$

The image is a G-module P of dimension $q^m + 1$ whose submodule lattice is:



The bottom module is the span of $\sum_{a \in \mathcal{I}_m} a^*$ (the all-1 word $\mathbf{1}$) and the top quotient P/P_0 has dimension 1; while $C/C \cap C^\nu$ and $C^\nu/C \cap C^\nu$ afford the two Weil representations. Both C and C^ν have dimension $(q^m + 1)/2$, and they are considered to be the analogues of quadratic residue codes in the ambient space $\mathbb{F}\mathcal{I}_m$; indeed, when $m = 1$, these are the codes taken to be the generalized quadratic residue codes.

When $m = 2$, $\mathcal{I}_1$ and $\mathcal{I}_2$ have the same size, $(q^2 + 1)(q + 1)$. The action of G on each of these sets is rank 3, but the actions are not equivalent. In their paper [4], Bagchi, Brouwer, and Wilbrink examine the G-submodule lattices of the two binary permutation modules $\mathbb{F}_2\mathcal{I}_1$ and $\mathbb{F}_2\mathcal{I}_2$, obtaining the dimensions of the various ingredients. However, the Weil representations can be written in $\mathbb{F}_2$ only when $q \equiv \pm 1 (\mathrm{mod}\, 8)$, so in the case $q \equiv \pm 3 (\mathrm{mod}\, 8)$, only the modules $\mathbf{0}$, $\langle \mathbf{1} \rangle$, and P_0 show up below P. Lataille, Sin, and Tiep [17] analyze the representation of G on $\overline{\mathbb{F}_2}\mathcal{I}_1$ over an algebraic closure $\overline{\mathbb{F}_2}$ of $\mathbb{F}_2$ for arbitrary m, as well as the one on $\overline{\mathbb{F}_2}\mathcal{I}_2$ when $m = 2$; they draw on the comprehensive work of Guralnick, Magaard, Saxl, and Tiep [9]. Two other papers dealing with codes involving the incidence structure having $\mathcal{I}_1$ for points and $\mathcal{I}_2$ for blocks (incidence being containment) are those by Kim, Peled, Perepelitsa, Pless, and Friedland [15]; and by Sin and Xiang [25].

But the codes C and C' have not been investigated for their coding properties for $m \geq 2$, to my knowledge. The lowest case with $m = 2$ and $q = 3$ has $\mathbb{F}_2(\varepsilon) = \mathbb{F}_4$. It is a $[40, 5, 24]_4$ code with weight distribution

$$A_0 = 1,\ A_{24} = 135,\ A_{30} = 480,\ A_{32} = 405,\ A_{40} = 3.$$

There are analogues of the square-root bound, but they are not as easy to use as when $m = 1$. The codes are in some sense amalgams of codes from lower values of m.

1.1 Quadratic residue codes in their prime

An appropriate spanning set for an extended quadratic residue code of length $q + 1$, with $q = p^h$, can actually be read modulo p to produce a $[q+1, ((p+1)/2)^h, (q+3)/2]_p$

code. This code is invariant under a monomial action of $\Gamma\mathrm{L}(2,q)$ on the projective line over $\mathbb{F}_q$ (which labels the coordinate positions as for the standard codes). In [33], this code arose as the smallest code over $\mathbb{F}_p$ among those of length $q+1$ invariant under that same action. The lattice of the invariant codes was described in terms of certain sets of binary words, stemming from a realization of the codes as doubly extended cyclic codes. When h is odd, the "middle" code in this lattice is a self-dual code. The one for $q = 27$ is an extremal type III code, and it was given a geometric framework in [34]. However, these codes have not been studied in any depth. The paper [33] concluded with a recursive formula for the dimensions of the codes, but there may be a more direct method for computing them.

2 Divisibility

A linear code is **divisible by** Δ if all the codeword weights are divisible by Δ; if $\Delta > 1$, then the code is called **divisible**. There are many examples, perhaps the most prominent ones being the formally self-dual codes covered by the Gleason-Pierce theorem and the generalized Reed-Muller (GRM) codes. I first became interested in them from reviewing a paper that dealt with generalizing the MacWilliams theorem on the equivalence of cyclic codes, and I gave a divisible version of that theorem in [29]. One of the most important theorems on divisibility is that of Delsarte and McEliece regarding cyclic and Abelian codes (the joint paper [7] contains generalizations of earlier work of the two authors). Their theorem was in turn generalized in [31] for codes that are ideals in semisimple group algebras; the theorem related divisibility to the existence of invariant multilinear forms on the code. One hope for an application of the theorem was that somehow it would give extra information about representations of the corresponding groups.

Divisibility for GRM codes, on the other hand, regards the codes more naturally as being in a group algebra of a p-group over a field of characteristic p, a **modular** group algebra–quite the opposite of the semisimple case. Here the natural parameter for a divisible code is the **exponent** ε of the code, for which p^ε is the largest power of p that is a divisor of the code. The theorems in [32] were designed to cope with GRM codes, among others, and they have been applied by several authors. For example, they can be used to show this:

Proposition 1 *Suppose that $q = p^a$ and $q' = q^h$, p a prime. Let C be a code over $\mathbb{F}_q$ with exponent at least ε. Then if $C' = \mathbb{F}_{q'} \otimes C$, the code C with coefficients extended to $\mathbb{F}_{q'}$, the exponent of C' is at least $\varepsilon - (h-1)a$.*

Again there is a hope that the results of [32] could be used in the study of modular group algebras. Indeed, some work along that line has been done by Deirdre Smeltzer [26].

The recent papers by Katz [13, 14] contain summaries of various generalizing theorems on divisibility and further divisibility theorems for codes over Galois rings.

2.1 Griesmer codes

The famous Griesmer bound (more properly, Griesmer-Solomon-Stiffler bound) for linear codes says that if an $[n, k, d]_q$ code exists, then

$$n \geq g_q(k, d) = d + \left\lceil \frac{d}{q} \right\rceil + \cdots + \left\lceil \frac{d}{q^{k-1}} \right\rceil .$$

There has been a tremendous amount of research aimed at finding **length-optimal** (usually simply called **optimal**) linear codes, those with smallest n for prescribed q, k and d; that n is often denoted $n_q(k, d)$. For surveys, see those by Hill and by Hill and Kolev [10, 11]. A guiding aspect for the work is deciding whether **Griesmer codes** exist, codes for which indeed $n = n_q(k, d) = g_q(k, d)$. Fortunately, Baumert and McEliece showed that for fixed q and k, Griesmer codes exist for sufficiently large d [3].

Of course, in deciding whether an $[n, k, d]_q$ code exists, the MacWilliams identities are key to restricting the possibilities for the weight distribution. But any additional restrictions on the possible weights that can be imposed are welcome. One such restriction is this:

Theorem 2 *Suppose that q is actually the prime p. Then if $p^e | d$, a Griesmer $[g_p(k, d), k, d]_p$ code is divisible by p^e.*

The proof in [36] makes heavy use of the divisibility criteria from [32].

What if $q = p^h$ for $h > 1$? Examination of examples leads to this conjecture:

Conjecture 3 *If p^e divides the minimum weight d of a Griesmer code over $\mathbb{F}_q$, where $q = p^h$ and $e \geq h$, then the code is divisible by $p^{e+1-h} = p^{e+1}/q$.*

The conjecture is true for $q = 4$; proofs of the general conjecture have been offered, but none correct that I know of. Ivan Landjev gave a geometric proof of Theorem 2 in [16], and Ivan expressed the hope that his methods could be applied to the conjecture.

At the end of [36], the possibility of Griesmer codes over $\mathbb{F}_p$ with parameters $n = 3(p^2 + 1)/2$, $k = 4$, and $d = 3p(p - 1)/2$, p an odd prime, was raised. The code would be a two-weight code, with

$$\begin{aligned} A_d &= (p^2 + 1)(2p - 1)(p - 1)/2 \\ A_{d+p} &= 3(p^2 + 1)(p - 1)/2 = n(p - 1) \end{aligned}$$

These codes exist for $p = 3$ and 5, but others seem not to be known. Markus Grassl's tables at

`http://www.codetables.de/`

that continue Brouwer's, gives a code at $p = 7$ with minimum weight one less. Tatsuya Maruta maintains a web page devoted to the Griesmer bound at

`http://www.geocities.com/mars39.geo/griesmer.htm`

2.2 Divisible code bound

Let C be an $[n,k]_q$ code that is divisible by Δ, q being a power of the prime p. When p does not divide Δ, C is equivalent to a Δ-fold replicated code, perhaps extended by some 0-coordinates [30], and one has $k \le n/\Delta$. The divisible code bound is a replacement for this simple inequality when p divides Δ (although the bound still holds when p doesn't). Suppose that the nonzero codeword weights of C lie in the interval $(b-a+1)\Delta, \ldots, b\Delta$ containing a multiples of Δ. Then

$$kv_p(q) \le a(v_p(\Delta) + v_p(q)) + v_p\left(\binom{b}{a}\right),$$

where v_p is the p-adic valuation. This **divisible code bound** was first proved by character-theoretic methods, but later given a more combinatorial proof [37]. It was applied to type I self-dual codes for an asymptotic improvement of the bound of Conway and Sloane [6], and that improvement itself was made "non-asymptotic" later on by Rains [24]. The bound has always struck me as rather weak, although it has had some successful applications to type I self-dual codes other than in the transitional role just mentioned.

There is a more general bound that does not restrict the codeword weights to an interval [37, Proposition 4.1]. Several codes in the list in MacWilliams and Seery [21] meet this second bound. Perhaps it is worth exploring in more detail and finding examples for other characteristics. Notice that the code length does not show up explicitly in the divisible code bound (and not in the generalization as well).

If $n = 24m$ for an extremal type II self-dual code (where $\Delta = 4$), then $d = 4m+4$. On applying the divisible code bound to a once-shortened code (to eliminate the all-1 word), for which $k = n/2 - 1 = 12m - 1$, $a = 4m + 1$, and $b = 5m - 1$, one finds that

$$12m - 1 \le 12m - 3 + v_2\left(\binom{5m-1}{4m-1}\right),$$

requiring $v_2\left(\binom{5m-1}{m}\right) \ge 2$. But this is always true–often tantalizingly with equality! Can anything be done with this?

A couple of natural questions are: is there an analogue of the Griesmer bound for divisible codes? Can one classify codes meeting the divisible code bound? (The codes should probably be restricted in some way, however.)

3 Codes and geometry

There are many connections between codes and geometry and I have worked with a number of people on them, especially Ray Hill, Jenny Key, and Gary McGuire. All of those collaborations produced work that can be viewed as ongoing, with lots of

unanswered questions. For example, Gary and I determined the weight enumerator of code of the projective plane of order 5 over $\mathbb{F}_5$ by hand [23], making use of theorems on self-dual codes over $\mathbb{F}_5$ [18]. Fortunately, our result was corroborated by Jenny using Magma! This is the largest order plane for which the enumerator has been determined, I believe. But the geometry of the words in codes of planes continues to be explored For surveys, see the two on Jenny's web page listed as "AMS SS06" and "VA07"; of course, her book with Ed Assmus [2] has a wealth of material on the subject. Gary and I found configurations associated with the words of small weight, but one could imagine finding those for higher weights. Some important progress on analogous questions has been made by Leo Storme and his collaborators [8].

The theorem on divisibility of Griesmer codes in Section 2.1 has been used a number of times and it has been my entry item to the general study of optimal codes. As implied, there are many unanswered questions. Tatsuya Maruta has written several papers describing intervals for d values for general q and k for which Griesmer codes exist, or for which the optimal length is $g_q(k,d)$ plus something small; see, for example, [22]. But specific possibilities have been dealt with regularly–the paper with Chris Jones and Angela Matney [12] is an example in which the geometric considerations were particularly fierce!

3.1 A divisible code catalog?

Simeon Ball once suggested cataloging divisible codes of small dimension. Here are some related "entry-level" problems:

1 Consider binary codes with specified divisor 2^δ. For a given dimension k, what is the length $s_\delta(k)$ of the shortest such code? When $\delta = 1$, the required code is simply the even subcode of $\mathbb{F}_2^{k+1}$: $s_1(k) = k+1$. At $\delta = 2$, the codes are self-orthogonal, and the relevant topic is type II self-dual codes and quadratic forms. The results are these:

$k \pmod 4$	0	1	2	3
$s_2(k)$	$2k$	$2k+2$	$2k+2$	$2k+1$

What about $\delta \geq 3$? Theorem 2 implies that if there is a Griesmer $[n,k]_2$ code with minimum weight 2^δ, then $s_\delta(k) = g_2(k, 2^\delta)$. Such Griesmer codes do exist for large enough δ (k fixed), by the theorem of Baumert and McEliece.

2 When q is even, how close is an $[n,k]_q$ code C that is divisible by 2 to being a replicated code? If $C^\perp$ contains a word of weight 2, then C punctured at the support of that word is also divisible by 2. Thus either C has a direct summand equivalent to the code with generator matrix $[1,1]$, or else C is obtained from an $[n-2,k]_q$ code C' that is divisible by 2 by adjoining one column twice to a generator matrix of C'. Call code C a **2-code** if C is divisible by 2 (q even) and C is **projective**: $C^\perp$ contains no word of weight 2. For a given $k \geq 2$, what is the length $t_q(k)$ of the shortest $[n,k]_q$ 2-code? It's not hard to show that $d \geq q$, whereby the Griesmer

bound implies that $t_q(k) \geq q + k - 1$. For $k = 2$, a Hamming dual (simplex code) gives $t_q(2) = q + 1$, and at $k = 3$, the code for which the columns of a generator matrix form a hyperoval in $\mathrm{PG}(2, q)$ implies that $t_q(3) = q + 2$. This latter code illustrates one standard connection between codes and geometry: the columns of the generating matrix are construed as representing points in a projective space, their configuration having properties reflecting those of the code. See Ivan's cited survey [16], for example.

An upper bound on $t_q(k)$ comes from taking direct sums of the codes for $k = 2$ or $k = 3$, so that if $k = 3l - r$, $0 \leq r \leq 2$, then $t_q(k) \leq (q + 2)l - r$. When $q = 4$, the codes in question are self-orthogonal, of course, and from [20] one can infer that $t_4(k) = 2k$. So we may take $q \geq 8$. If $t_q(4) = q + 3$, a $[q + 3, 4]_q$ code would have just the codeword weights q and $q + 2$, and the divisible code bound rules this out. Thus, $q + 4 \leq t_q(4) \leq 2q$. But what is the bound, and what holds for $k > 4$? In the spirit of [1], one might include a search for indecomposable 2-codes and other categorical properties.

3 If $q = 2^h$, and C is a binary code divisible by 2^h, then by Proposition 1, the field-extended code $\mathbb{F}_q \otimes C$ is divisible by 2. Thus if C is also projective, $\mathbb{F}_q \otimes C$ is a 2-code. This observation connects the two previous problems: we can produce 2-codes from codes uncovered in problem 1 if they are also projective. How does problem 1 change if we also require the minimal codes to be projective? Given δ, consider the first-order punctured Reed-Muller code $\mathcal{R}(1, k)^*$ (again a simplex code) with $k \geq \delta + 1$ [2, Chapter 5]. It has length $2^k - 1$, dimension k, and all its nonzero word weights are 2^{k-1}. Moreover, it is projective. So for $k \geq \delta + 1$, there certainly is a projective code of dimension k that is divisible by 2^δ; and therefore there is such a code of minimum length. Can the minimal codes be described neatly?

And–what about the analogous questions for field characteristics other than 2?

References

[1] E. F. Assmus, Jr., The category of linear codes. *IEEE Trans. Inform. Theory* **44** (1998), no. 2, 612–629.

[2] E. F. Assmus, Jr. and J. D. Key, *Designs and their codes.* Cambridge Tracts in Mathematics, 103. Cambridge University Press, Cambridge, 1992.

[3] L. D. Baumert and Robert. J. McEliece, A note on the Griesmer bound. *IEEE Trans. Information Theory* **IT-19** (1973), no. 1, 134–135.

[4] B. Bagchi, A. E. Brouwer, and H. A.Wilbrink, Notes on binary codes related to the $\mathrm{O}(5, q)$ generalized quadrangle for odd q. *Geom. Dedicata* **39** (1991), no. 3, 339–355.

[5] Paul Camion, Global quadratic Abelian codes, *Information Theory, CISM Courses and Lectures* **219**, G. Longo ed.,Springer-Verlag, Vienna (1975) 293–310.

[6] J. H. Conway and N. J. A. Sloane, A new upper bound on the minimal distance of self-dual codes. *IEEE Trans. Inform. Theory* **36** (1990), no. 6, 1319–1333.

[7] Philippe Delsarte and Robert J. McEliece, Zeros of functions in finite abelian group algebras. *Amer. J. Math.* **98** (1976), no. 1, 197–224.

[8] V. Fack, Sz. L. Fancsali, L. Storme, G. Van de Voorde, and J. Winne, Small weight codewords in the codes arising from Desarguesian projective planes. *Des. Codes Cryptogr.*, to appear.

[9] Robert M. Guralnick, Kay Magaard, Jan Saxl, and Pham Huu Tiep, Cross characteristic representations of symplectic and unitary groups. *J. Algebra* **257** (2002), no. 2, 291–347.

[10] Ray Hill, Optimal linear codes. *Cryptography and coding, II (Cirencester, 1989)*, 75–104, Inst. Math. Appl. Conf. Ser. New Ser., 33, Oxford Univ. Press, New York, 1992.

[11] Ray Hill and Emil Kolev, A survey of recent results on optimal linear codes. *Combinatorial designs and their applications (Milton Keynes, 1997)*, 127–152, Chapman & Hall/CRC *Res. Notes Math.*, **403**, Chapman & Hall/CRC, Boca Raton, FL, 1999.

[12] Chris Jones, Angela Matney, and Harold Ward, Optimal four-dimensional codes over GF(8). *Electron. J. Combin.* **13** (2006), no. 1, Research Paper 43, 21 pp.

[13] Daniel J. Katz, p-adic valuation of weights in abelian codes over $\mathbb{Z}_{p^d}$. *IEEE Trans. Inform. Theory* **51** (2005), no. 1, 281–305.

[14] Daniel J. Katz, p-adic estimates of Hamming weights in abelian codes over Galois rings. *IEEE Trans. Inform. Theory* **52** (2006), no. 3, 964–985.

[15] Jon-Lark Kim, Uri N. Peled, Irina Perepelitsa, Vera Pless, and Shmuel Friedland, Explicit construction of families of LDPC codes with no 4-cycles. *IEEE Trans. Inform. Theory* **50** (2004), no. 10, 2378–2388.

[16] I. N. Landjev, The geometric approach to linear codes. *Finite geometries*, 247–256, *Dev. Math.*, **3**, Kluwer Acad. Publ., Dordrecht, 2001.

[17] J. M. Lataille, Peter Sin, and Pham Huu Tiep, The modulo 2 structure of rank 3 permutation modules for odd characteristic symplectic groups. *J. Algebra* **268** (2003), no. 2, 463–483.

[18] J. S. Leon, V. Pless, and N. J. A. Sloane, Self-dual codes over GF(5). *J. Combin. Theory Ser. A* **32** (1982), no. 2, 178–194.

[19] Jacobus H. van Lint and F. Jessie MacWilliams, Generalized quadratic residue codes. *IEEE Trans. Inform. Theory* **24** (1978), no. 6, 730–737.

[20] F. J. MacWilliams, A. M. Odlyzko, N. J. A. Sloane, and H. N. Ward, Self-dual codes over GF(4). *J. Combin. Theory Ser. A* **25** (1978), no. 3, 288–318.

[21] Jessie MacWilliams and Judith Seery, The weight distributions of some minimal cyclic codes. *IEEE Trans. Inform. Theory* **27** (1981), no. 6, 796–806.

[22] Tatsuya Maruta, On the minimum length of q-ary linear codes of dimension four. *Combinatorics (Assisi, 1996). Discrete Math.* **208/209** (1999), 427–435.

[23] Gary McGuire and Harold N. Ward, A determination of the weight enumerator of the code of the projective plane of order 5. *Note Mat.* **18** (1998), no. 1, 71–99 (1999).

[24] Eric M. Rains, Shadow bounds for self-dual codes. *IEEE Trans. Inform. Theory* **44** (1998), no. 1, 134–139.

[25] Peter Sin and Qing Xiang, On the dimension of certain LDPC codes based on q-regular bipartite graphs. *IEEE Trans. Inform. Theory* **52** (2006), no. 8, 3735–3737.

[26] Deirdre Longacher Smeltzer, Properties of codes from difference sets in 2-groups. *Des. Codes Cryptogr.* **16** (1999), no. 3, 291–306.

[27] Harold N. Ward, Representations of symplectic groups. *J. Algebra* **20** (1972) 182–195.

[28] Harold N. Ward, Quadratic residue codes and symplectic groups. *J. Algebra* **29** (1974) 150–171.

[29] Harold N. Ward, Combinatorial polarization. *Discrete Math.* **26** (1979), no. 2, 185–197.

[30] Harold N. Ward, Divisible codes. *Arch. Math. (Basel)* **36** (1981), no. 6, 485–494.

[31] Harold N. Ward, Multilinear forms and divisors of codeword weights. *Quart. J. Math. Oxford Ser. (2)* **34** (1983), no. 133, 115–128.

[32] Harold N. Ward, Weight polarization and divisibility. *Discrete Math.* **83** (1990), no. 2-3, 315–326.

[33] Harold N. Ward, Quadratic residue codes in their prime. *J. Algebra* **150** (1992), no. 1, 87–100.

[34] Harold N. Ward, Quadratic residue codes of length 27. *IEEE Trans. Inform. Theory* **36** (1990), no. 4, 950–953.

[35] Harold N. Ward, Quadratic residue codes and divisibility. *Handbook of coding theory, Vol. I, II*, 827–870, North-Holland, Amsterdam, 1998.

[36] Harold N. Ward, Divisibility of codes meeting the Griesmer bound. *J. Combin. Theory Ser. A* **83** (1998), no. 1, 79–93.

[37] Harold N. Ward, The divisible code bound revisited. *J. Combin. Theory Ser. A* **94** (2001), no. 1, 34–50.