The Development of Coding Theory over Finite Rings

Jay A. Wood
Department of Mathematics
Western Michigan University
1903 W Michigan Ave
Kalamazoo MI 49008-5248
jay.wood@wmich.edu
http://unix.cc.wmich.edu/jwood

AMS Special Session
January 7, 2002

Outline:

- Preliminaries
- Some early papers: cyclic codes
- Equivalence problems I: generating characters
- MacWilliams identities
- Equivalence problems II: virtual codes

Acknowledgments

Much of the recent work on codes over rings has been motivated by the break-through work of Hammons, Kumar, Calderbank, Sloane, and Solé. In Russia, Nechaev had similar results.

Many people have been very helpful to me in my work, and I thank them all. I single out for special thanks Ed Assmus, Vera Pless, and Thann Ward.

Preliminaries

We fix a finite ring R with 1 (and usually commutative, for convenience).

A *linear code* C of block length n is an R-submodule of R^n, the free module of n-tuples over R.

Several notions of weight for $x \in R^n$:

- Hamming weight: $\mathrm{wt}(x)$.
- Weight compositions: $c_r(x) = |\{i : x_i = r\}|$.
- Weight functions: $w(x) = \sum a_r c_r(x)$.
- Can make certain identifications to reflect symmetry.

Some early papers: cyclic codes

MacWilliams observed that cyclic codes can be viewed as ideals in appropriate group algebras.

- I. F. Blake, Codes over certain rings, *Inform. and Control*, **20** (1972), 396–404. Over $\mathbb{Z}/m\mathbb{Z}$, assumes m is a product of distinct primes. Uses Chinese remainder theorem to reduce to case of fields. Length is prime to m.

- I. F. Blake, Codes over integer residue rings, *Inform. and Control*, **29** (1975), 295–300. Hamming, Reed-Solomon, and BCH codes over $\mathbb{Z}/p^r\mathbb{Z}$. Length is prime to p.

- E. Spiegel, Codes over $\mathbb{Z}_m$, *Inform. and Control*, **35** (1977), 48–51. Cyclic codes over $\mathbb{Z}/p^r\mathbb{Z}$; length is prime to p.

- E. Spiegel, Codes over $\mathbb{Z}_m$, revisited, *Inform. and Control*, **37** (1978), 100–104. A different treatment of BCH codes of length prime to p.

- S. K. Wasan, On codes over $\mathbb{Z}_m$, *IEEE Trans. Info. Theory*, **28** (1982), 117–120. Splitting the group ring. One correction: $K[G_1 \times G_2] \cong KG_1 \otimes KG_2$.

Post-HKCSS, a large number of papers have appeared discussing cyclic and quasi-cyclic codes over $\mathbb{Z}/m\mathbb{Z}$ and other finite rings. I will defer to Patrick Solé and his talk later this morning.

Equivalence problems I: generating characters

Fix a subgroup U of the group of units $\mathcal{U}$ of R.

Two linear codes $C_1, C_2 \subset R^n$ are U-*equivalent* if there exists a U-monomial transformation on R^n taking one code to the other.

Let w be a weight function on R^n; $w(x) = \sum a_r c_r(x)$. The *symmetry group* of w is

$$\mathrm{Sym}(w) = \{u \in \mathcal{U} : a_{ur} = a_r, r \in R\}.$$

If $U \subset \mathrm{Sym}(w)$, then every U-monomial transformation f is an isometry for w. That is, $w(f(x)) = w(x), x \in R^n$.

What about the converse?

Over finite fields with the Hamming weight, MacWilliams proved the converse in her thesis (1962).

In 1978, Bogart, Goldberg, and Gordon provided another proof. (Recently, Greferath and Schmidt have given a BGG-like proof, too. More on that later.)

Ward and I gave a character-theoretic proof in 1996. (Ward knew of this proof at least five years earlier, while working on divisible codes.)

In 1980, Goldberg proved a version of the converse for weight compositions over finite fields.

Let's look at a few details of the character-theoretic proof of the converse.

The setting: R is a finite field, and we use the Hamming weight. Given are two linear codes $C_1, C_2 \subset R^n$ and an isomorphism $f : C_1 \to C_2$, with $\mathrm{wt}(f(x)) = \mathrm{wt}(x), x \in C_1$.

The question is whether f extends to a monomial transformation of R^n.

Let $\lambda_1, \ldots, \lambda_n$ be the coordinate functionals of C_1, and let $\mu_1, \ldots, \mu_n$ be the coordinate functionals of C_2 composed with f.

If π is a non-trivial character of R, then every other character of R has the form $\chi(r) = \pi(ar)$, for some $a \in R$. Then $\sum_a \pi(ar) = |R|$ if $r = 0$, and equals 0 if $r \neq 0$.

The fact that f preserves Hamming weight then yields

$$\sum_{i=1}^{n} \sum_{a \in R} \pi(a\lambda_i(x)) = \sum_{j=1}^{n} \sum_{b \in R} \pi(b\mu_j(x)),$$

for all $x \in C_1$.

The summands are characters on C_1. Linear independence of characters then allows one to deduce the existence of a monomial transformation extending f.

What makes this argument work?

There are two key properties:

- Every character is of the form $\chi(r) = \pi(ar)$. ("Can be labelled in a symmetric way"—FJM.)

- If $\pi(\lambda(x)) = 1$ for all x, then $\lambda(x) = 0$ for all x.

The same proof will work over a finite ring possessing such a character π. These are the Frobenius rings, and π is called a generating character. (Use the character module itself as the alphabet: Greferath, Nechaev, Wisbauer.)

The name comes from Klemm, who used generating characters to prove the MacWilliams identities. Claasen and Goldberg also studied these characters.

The MacWilliams extension theorem is now known over finite Frobenius rings with the Hamming weight or with symmetrized weight compositions.

Results valid for more general weight functions are more restrictive. Constantinescu, Heise, and Honold, as well as Greferath and Schmidt, have results for homogeneous weights. I have a very general sufficient condition that applies in a number of situations (such as Lee and Euclidean weights over $\mathbb{Z}/m\mathbb{Z}$ for $m \leq 256$).

MacWilliams identities

There are several proofs of the MacWilliams identities over finite fields. (Honold and Ward have elegant elementary proofs.) My favorite is Gleason's proof using the Poisson summation formula.

Since the Poisson summation formula involves the discrete Fourier transform, it is ultimately based on characters. An essential ingredient is the ability to identify a character-theoretic annihilator with an orthogonal. Once again, a generating character π in a Frobenius ring makes such an identification possible.

Many people have made observations along these lines: MacWilliams, Klemm, Nechaev, ...

Equivalence problems II: virtual codes

Another early paper, which explicitly states that rings can underlie linear codes, is

- E. F. Assmus, H. F. Mattson, Error-correcting codes: an axiomatic approach, *Inform. and Control* **6** (1963), 315–330.

Assmus and Mattson also take a linear functional point of view. With that in mind, I will re-define linear codes.

A *linear code* C is a pair (M, η), where M is a finitely generated R-module, and

$$\eta : M^\sharp := \mathrm{Hom}_R(M, R) \to \mathbb{N}$$

is a *multiplicity function*.

Think of columns of a generator matrix. Compare with the "modular representation" in Peterson's book.

Non-degenerate: $\eta(0) = 0$.

A *weight function* w on R assigns weights a_r to $r \in R$; $a_0 = 0$. We assume $a_r \in \mathbb{Q}$.

For a code $C = (M, \eta)$, $x \in M$ has *weight*

$$w_\eta(x) = \sum_{\lambda \in M^\sharp} \eta(\lambda) a_{\lambda(x)}.$$

Let U denote the symmetry group of w. Then U acts on M and $M^\sharp$ by scalar multiplication. Denote the sets of *non-zero* orbits by $\mathcal{O}$ and $\mathcal{O}^\sharp$, respectively.

If $x, y \in M$ lie in the same orbit, then $w_\eta(x) = w_\eta(y)$.

For any $\lambda \in M^\sharp$, define

$$\eta_S(\lambda) = \sum_{\mu \in \mathsf{orb}(\lambda)} \eta(\mu).$$

If $\lambda, \mu \in M^\sharp$ lie in the same orbit, then $\eta_S(\lambda) = \eta_S(\mu)$.

Two linear codes $C = (M, \eta)$, $C' = (M, \eta')$ are *scale equivalent* if $\eta_S = \eta'_S$. Denote the set of functions $\mathcal{O}^\sharp \to \mathbb{N}$ by $\mathbb{N}[\mathcal{O}^\sharp]$.

There is a bijection between the set of all nondegenerate linear codes (M, η), up to scale equivalence, and the function space $\mathbb{N}[\mathcal{O}^\sharp]$.

Two linear codes $C' = (M', \eta')$, $C = (M, \eta)$, are *equivalent* if there exists an isomorphism $f : M' \to M$ such that $(M, \eta' \circ f^\sharp)$ and (M, η) are scale equivalent. If C' and C are equivalent, then $w_{\eta'}(x) = w_\eta(f(x))$ for all $x \in M'$.

Compare to equivalence via generator matrices.

Fix the R-module M. Define $W : \mathbb{N}[\mathcal{O}^\sharp] \to \mathbb{Q}[\mathcal{O}]$, $g \mapsto w_g$, where

$$w_g(\text{orb}(x)) = \sum_{\lambda:\text{rep}} g(\text{orb}(\lambda))\, a_{\lambda(x)},$$

and the summation is over one representative λ of each Sym(w)-orbit.

Comments:

- The extension theorem is equivalent to W being injective.

- W can be found in work of MacDonald and Slepian (see Peterson's book).

- The map W is the same as the map T used by Bogart, Goldberg, and Gordon and by Greferath and Schmidt.

Virtual codes: allow the multiplicity function $\eta : M^\sharp \to \mathbb{Q}$ to have rational values. *Classical* codes have values in $\mathbb{N}$.

There is a bijection between the set of nondegenerate virtual linear codes (M, η), up to scale equivalence, and the function space $\mathbb{Q}[\mathcal{O}^\sharp]$.

The weight mapping $W : \mathbb{Q}[\mathcal{O}^\sharp] \to \mathbb{Q}[\mathcal{O}]$ then becomes an isomorphism, if the extension theorem holds.

This isomorphism allows one to understand completely those linear codes having only one nonzero weight.