Linear codes over finite rings and modules

Jay A. Wood

Department of Mathematics
Western Michigan University
http://homepages.wmich.edu/∼jwood/

Algebra for Secure and Reliable Communications Modeling
Morelia, Michoacán, Mexico
October 5, 2012

Acknowledgments

- Thanks to . . . the organizers for inviting me to speak
- . . . and to CIMPA and the other sponsors for supporting this school.

Why finite rings? (a)

- There was work in the 1970s and early 1980s on linear codes over $\mathbb{Z}/m\mathbb{Z}$ by Blake, Shankar, Spiegel, and Wasan, primarily trying to understand cyclic codes over those rings.
- As early as 1981, Nechaev used $\mathbb{Z}/4\mathbb{Z}$ to explain the cyclic structure of the nonlinear binary Kerdock code.

Why finite rings? (b)

- The 1994 paper "The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes," by Hammons, Kumar, Calderbank, Sloane, and Solé, took this further. This paper explained the seeming duality of the nonlinear binary Kerdock and Preparata codes by viewing them as Gray images of dual linear codes over $\mathbb{Z}/4\mathbb{Z}$.
- This sparked a lot of interest!

What types of questions?

- Can other finite rings be used to explain existing codes or to create new ones?
- How much of the basic infrastructure of linear coding theory over finite fields is still valid over finite rings?
- If not over all finite rings, perhaps over certain general classes of finite rings?
- Prof. Dinh will primarily discuss creating new codes, while I will primarily discuss infrastructure.

Cyclic codes (a)

- A linear code C of length n over the finite field $\mathbb{F}_q$ is *cyclic* if $(a_0, a_1, \ldots, a_{n-1}) \in C$ implies $(a_{n-1}, a_0, a_1, \ldots, a_{n-2}) \in C$.
- View $\mathbb{F}_q^n$ as the vector space underlying the $\mathbb{F}_q$-algebra $R = \mathbb{F}_q[X]/(X^n - 1)$, with $(a_0, a_1, \ldots, a_{n-1}) \in \mathbb{F}_q^n$ corresponding to $a_0 + a_1X + a_2X^2 + \cdots a_{n-1}X^{n-1} \bmod (X^n - 1)$.

Cyclic codes (b)

- The cyclic shift corresponds to multiplication by X in R, because $X \cdot a_{n-1}X^{n-1} = a_{n-1}X^n \equiv a_{n-1} \bmod (X^n - 1)$.
- A cyclic code is simply an ideal in $R = \mathbb{F}_q[X]/(X^n - 1)$.
- An ideal in R will be seen to be a linear code over R of length 1.

Usual setting

- Let R be a finite, associative ring with 1.
- We allow R to be noncommutative.
- Denote the group of units of R by $\mathcal{U}(R)$.
- Let A be a finite left R-module ("alphabet").
- We always assume that $1 \in R$ acts as the identity on R-modules.

Linear codes

- A left *R-linear code* over A of length n is a left R-submodule $C \subset A^n$.
- The entries in codewords come from the alphabet A.
- Important special case: $A = R$ itself. These are linear codes over R.
- Cyclic codes are linear codes of length 1 over $R = \mathbb{F}_q[X]/(X^n - 1)$.
- One can define right linear codes similarly.

Weights

- A *weight* on an alphabet A is a function $w : A \to \mathbb{C}$ with $w(0) = 0$.
- The *Hamming weight* has $\mathrm{wt}(a) = 1$ for all $a \neq 0$.
- The Lee and Euclidean weights on $\mathbb{Z}/m\mathbb{Z}$: $w_L(a) = |a|$, $w_E(a) = |a|^2$, for $-m/2 < a \leq m/2$.
- Homogeneous weight on any finite ring (later).
- For $x \in A^n$, define $w(x) = \sum w(x_i)$.

Symmetry groups

- Suppose A has weight w.
- The *left symmetry group* is $G_l := \{u \in \mathcal{U}(R) : w(ua) = w(a), a \in A\}$.
- The *right symmetry group* is $G_r := \{\phi \in \mathrm{Aut}(A) : w(a\phi) = w(a), a \in A\}$.
- $\mathrm{Aut}(A)$ is the group of invertible R-linear homomorphisms $A \longrightarrow A$, written on the right. (When $A = R$, $\mathrm{Aut}(A)$ is right multiplication by units in $\mathcal{U}(R)$.)

Monomial transformations (a)

- A *monomial transformation* is a homomorphism $T : A^n \longrightarrow A^n$ of left R-modules of the form

$$(a_1, \ldots, a_n)T = (a_{\sigma(1)}\phi_1, \ldots, a_{\sigma(n)}\phi_n),$$

where $\phi_i \in \mathrm{Aut}(A)$ and σ is a permutation of $\{1, \ldots, n\}$.

Monomial transformations (b)

- A G_r-*monomial transformation* is one where each $\phi_i \in G_r$.
- Every G_r-monomial transformation preserves w: $w(aT) = w(a)$ for $a \in A^n$.

The Extension Problem

- Suppose $C_1, C_2 \subset A^n$ are two R-linear codes.
- If $C_1 T = C_2$, then $T : C_1 \longrightarrow C_2$ is a w-preserving isomorphism between the codes.
- Is the converse true? If $f : C_1 \longrightarrow C_2$ is a w-preserving isomorphism, does f extend to a G_r-monomial transformation?
- True for Hamming weight over finite fields (MacWilliams, 1961–1962).
- What happens over rings? (Later talks.)

Dot products

- Suppose the alphabet is $A = R$ itself.
- Define a *dot product* on R^n by

$$a \cdot b = \sum a_i b_i \in R.$$

Annihilators

- Let $C \subset R^n$ be a linear code.
- Define *annihilators*:

$$l(C) := \{b \in R^n : b \cdot a = 0, a \in C\},$$
$$r(C) := \{b \in R^n : a \cdot b = 0, a \in C\}.$$

- Do these annihilators behave like dual codes? (Later talks.)

MacWilliams identities

- For a linear code $C \subset R^n$, the *Hamming weight enumerator* is the generating function

$$W_C(X, Y) := \sum_{a \in C} X^{n-\mathrm{wt}(a)} Y^{\mathrm{wt}(a)}.$$

- Any relationship between W_C and $W_{l(C)}$ or $W_{r(C)}$?
- Yes, over finite fields (MacWilliams, 1962–1963).
- More generally? (Later talks.)

Parametrized codes (a)

- Another way to view linear codes is by abstracting the idea of a generator matrix. (Although one can still define generator matrices.)
- This abstraction is due to Assmus and Mattson, 1963.
- A left R-linear *parametrized code* over A is pair (M, Λ), where M is a finite left R-module, and $\Lambda : M \longrightarrow A^n$ is a homomorphism of left R-modules.
- Λ is given by an n-tuple $(\lambda_1, \lambda_2, \ldots, \lambda_n)$ of homomorphisms $\lambda_i : M \longrightarrow A$.

Parametrized codes (b)

- M generalizes "information bits."
- By choosing a set of generators for M, one can build a generator matrix.
- A linear code is the image $M\Lambda \subset A^n$.
- Note: homomorphisms of left R-modules are written on the right.

Jacobson radical

- Let R be a finite, associative ring with 1.
- The *Jacobson radical* J of R is the intersection of all the maximal left ideals of R.
- J is a two-sided ideal of R.
- R/J is a semisimple ring, isomorphic to a direct sum of matrix rings over finite fields.

Socles

- A left R-module M is *simple* if it has no nonzero proper submodules.
- The *socle* $\mathrm{Soc}(M)$ of M is the submodule generated by all the simple submodules of M.
- The left socle of a ring is its socle as a left module over itself.

$\mathbb{Z}/m\mathbb{Z}$

- Let $R = \mathbb{Z}/m\mathbb{Z}$, where m has prime factorization $m = p_1^{k_1} p_2^{k_2} \cdots p_l^{k_l}$.
- $J = (p_1 p_2 \cdots p_l)$ and $R/J \cong \mathbb{Z}/(p_1 p_2 \cdots p_l)\mathbb{Z} \cong \mathbb{Z}/p_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_l\mathbb{Z}$.
- $\mathrm{Soc}(R) = (p_1^{k_1-1} \cdots p_l^{k_l-1}) \cong \mathbb{Z}/p_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_l\mathbb{Z}$.

$M_n(\mathbb{F}_q)$

- Let $R = M_n(\mathbb{F}_q)$ be the ring of $n \times n$ matrices over $\mathbb{F}_q$.
- R has no nontrivial two-sided ideals, so $J = 0$.
- $\mathbb{F}_q^n$ is a simple module, and $R = \mathrm{Soc}(R) \cong n\mathbb{F}_q^n$.

Klemm's example

- Let $R = \mathbb{F}_2[X, Y]/(X^2, XY, Y^2)$. R is a 3-dimensional algebra over $\mathbb{F}_2$, with vector space basis $1, X, Y$.
- $J = (X, Y)$, with $R/J \cong \mathbb{F}_2$. R is a local ring.
- $\mathrm{Soc}(R) = J \cong 2\mathbb{F}_2$.