Avenues of research for codes over rings

Steven Dougherty

June 6, 2011

Original Coding Question

What is the largest number of points in $\mathbb{F}_2^n$ such that any two of the points are at least d apart, where

$$d(\mathbf{v}, \mathbf{w}) = |\{i \mid \mathbf{v}_i \neq \mathbf{w}_i\}|?$$

Original Coding Question

What is the largest number of points in $\mathbb{F}_2^n$ such that any two of the points are at least d apart, where

$$d(\mathbf{v}, \mathbf{w}) = |\{i \mid \mathbf{v}_i \neq \mathbf{w}_i\}|?$$

Linear version: What is the largest dimension of a vector space in $\mathbb{F}_2^n$ such the weight of any non-zero vector is at least d, i.e. what is the largest k such that a $[n, k, d]$ binary code exists?

Modified Coding Question

What is the largest number of points in A^n, where A is some algebraic structure, such that the weight of any non-zero vector is at least d, where the weight is appropriate for the algebraic structure?

Examples

- $A = \mathbb{Z}_{2k}$ and weight is the Euclidean weight, $wt(\mathbf{c}) = \sum min\{\mathbf{c}_i, 2k - \mathbf{c}_i\}^2$.

Examples

- $A = \mathbb{Z}_{2k}$ and weight is the Euclidean weight, $wt(\mathbf{c}) = \sum min\{\mathbf{c}_i, 2k - \mathbf{c}_i\}^2$.
- A is any ring and the weight is Hamming weight, $wt(\mathbf{c}) = |\{i \mid \mathbf{c}_i \neq 0\}|$.

Examples

- $A = \mathbb{Z}_{2k}$ and weight is the Euclidean weight, $wt(\mathbf{c}) = \sum min\{\mathbf{c}_i, 2k - \mathbf{c}_i\}^2$.
- A is any ring and the weight is Hamming weight, $wt(\mathbf{c}) = |\{i \mid \mathbf{c}_i \neq 0\}|$.
- A is a ring and the weight is the Homegenous weight, that is a a function $w : R \to \mathbb{Q}$ such that
  - $w(0) = 0$
  - Whenever $R^\times x = R^\times y$ then $w(x) = w(y)$.
  - There is a constant $\gamma \in \mathbb{Q}$ such that

$$\frac{1}{|R|} \sum_{y \in Rx} w(y) = \gamma \text{ for all } x \in R\ \{0\}. \qquad (1)$$

Examples

- A is $\mathbb{Z}_4$ or $\mathbb{F}_2[u_1, u_2, \ldots, u_k]/\langle u_i^2 = 0, u_i u_j = u_j u_i \rangle$ or $\mathbb{F}_2[v_1, v_2, \ldots, v_k]/\langle v_i^2 = 0, v_i v_j = v_j v_i \rangle$ and weight is Lee weight, that is the Hamming weight of its image under the assoicated Gray map.

Gray Maps

$\mathbb{Z}_4$	$\mathbb{F}_2 + u\mathbb{F}_2$	$\mathbb{F}_2 + v\mathbb{F}_2$	$\mathbb{F}_2^2$
0	0	0	00
1	1	v	01
2	u	1	11
3	$1+u$	$1+v$	10

Big question 0

What algebraic structures do we allow A to be (modules, groups, rings etc.)?

Big question 0

What algebraic structures do we allow A to be (modules, groups, rings etc.)?
We want the MacWilliams Theorems to hold in order to apply the tools of Coding Theory.

Some Definitions

Let R be a ring. A linear code C over R of length n is a submodule of R^n.
$L(C) = \{v \mid [v, w] = 0 \text{ for all } w \in C$
$R(C) = \{v \mid [w, v] = 0 \text{ for all } w \in C$
If R is commutative then $R(C) = L(C) = C^{\perp}$.

$$W_C(x_0, x_1, \ldots, x_a) = \sum_{\mathbf{c} \in C} \prod_{i=1}^{n} x_{\mathbf{c}_i}$$

MacWilliams Theorems 1

Theorem

(**MacWilliams 1**) *(A) If R is a finite Frobenius ring and C is a linear code, then every hamming isometry $C \to R^n$ can be extended to a monomial transformation.*

MacWilliams Theorems 1

Theorem

(**MacWilliams 1**) *(A) If* R *is a finite Frobenius ring and* C *is a linear code, then every hamming isometry* $C \to R^n$ *can be extended to a monomial transformation.*
(B)If a finite commutative ring R *satisfies that all of its Hamming isometries between linear codes allow for monomial extensions, then* R *is a Frobenius ring.*

MacWilliams Theorems 1

Theorem

(**MacWilliams 1**) *(A) If R is a finite Frobenius ring and C is a linear code, then every hamming isometry $C \to R^n$ can be extended to a monomial transformation.*
(B)If a finite commutative ring R satisfies that all of its Hamming isometries between linear codes allow for monomial extensions, then R is a Frobenius ring.

By an example of Greferath and Schmidt MacWilliams I does not extend to quasi-Frobenius rings.

MacWilliams Theorems 2

Let χ be a generating character associated to the ring R and let $T_{a,b} = \chi(ab)$, with $C^{\perp}$ the standard orthogonal.

Theorem

(**MacWilliams 2**) *Let C be a linear code over a finite commutative Frobenius ring R then*

$$W_{C^{\perp}}(X_{\mathbf{a}}) = \frac{1}{|C|} W_C(T \cdot X_{\mathbf{a}})$$

MacWilliams Theorems 2

Let χ be a generating character associated to the ring R and let $T_{a,b} = \chi(ab)$, with $C^\perp$ the standard orthogonal.

Theorem

(**MacWilliams 2**) *Let C be a linear code over a finite commutative Frobenius ring R then*

$$W_{C^\perp}(X_{\mathbf{a}}) = \frac{1}{|C|} W_C(T \cdot X_{\mathbf{a}})$$

MacWilliams relations exists for non-commutative rings for the left and right orthogonal by a slight alteration of the matrix T.

J.A. Wood, Duality for modules over finite rings and applications to coding theory, American Journal of Mathematics, 121, 1999, 555-575.

Standard techniques for commutative rings

- Any commutative Frobenius ring is isomorphic via the Chinese Remainder Theorem to a product of Frobenius local rings.
- Any commutative principal ideal ring is isomorphic via the Chinese Remainder Theorem to a product of chain rings. For example, $\mathbb{Z}_k$ is isomorophic to $\mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_s^{e_s}}$.
- We describe by CRT this isomorphism so that $C = CRT(C_1, C_2, \ldots, C_s)$.

Singleton Bound

Let C be a subset of A^n where A is any alphabet, and $d(C)$ is the minimum Hamming distance between any two distinct vectors then

$$d(C) \leq n - \log_{|A|}(C) + 1.$$

Singleton Bound

Let C be a subset of A^n where A is any alphabet, and $d(C)$ is the minimum Hamming distance between any two distinct vectors then

$$d(C) \leq n - \log_{|A|}(C) + 1.$$

A code meeting this bound is said to be an MDS (Maximum Distance Separable Code).

Singleton Bound

Let C be a subset of A^n where A is any alphabet, and $d(C)$ is the minimum Hamming distance between any two distinct vectors then

$$d(C) \leq n - \log_{|A|}(C) + 1.$$

A code meeting this bound is said to be an MDS (Maximum Distance Separable Code).
This combinatorial bound is equivalent to a number of interesting combinatorial questions involving mutually orthogonal Latin squares (and hypercubes) and arcs of maximal size in projective geometry.

MDR Codes

Let C be a linear code over a PIR, then

$$d(C) \leq n - k + 1$$

where k is the rank of the code.

MDR Codes

Let C be a linear code over a PIR, then

$$d(C) \leq n - k + 1$$

where k is the rank of the code.
A code meeting this bound is said to be MDR (Maximum Distance with respect to Rank).

MDR Codes

Let C be a linear code over a PIR, then

$$d(C) \leq n - k + 1$$

where k is the rank of the code.
A code meeting this bound is said to be MDR (Maximum Distance with respect to Rank).

MDR and MDS Codes

Theorem

Let $C_1, C_2, \ldots, C_k$ be codes over R_i, where the R_i are the component rings via the CRT. If C_i is an MDR code for each i, then $C = CRT(C_1, C_2, \ldots, C_k)$ is an MDR code. If C_i is an MDS code of the same rank for each i, then $C = CRT(C_1, C_2, \ldots, C_k)$ is an MDS code.

S.T. Dougherty, Jon-Lark Kim and Hamid Kulosman, MDS codes over finite principal ideal rings , Designs, Codes and Cryptography, Volume 50, 77-92, 2009.

MDS

Theorem

Let R be a finite principal ideal ring all of whose residue fields satisfy $|R/\mathfrak{m}_i| > \binom{n-1}{n-k-1}$ for some integers n, k with $n-k-1>0$. Then there exists an MDS $[n, k, n-k+1]$ code over R.

S.T. Dougherty, Jon-Lark Kim and Hamid Kulosman, MDS codes over finite principal ideal rings , Designs, Codes and Cryptography, Volume 50, 77-92, 2009.

Big Question 1

Construct and classify MDR codes over rings (commutative and non-commutative).
That is, determine precisely when they exist.

Self-Dual Codes

A code is self-dual if $C = C^{\perp}$.

Self-dual codes are related to unimodular lattices and combinatorial objects.

Self-Dual Codes

A code is self-dual if $C = C^{\perp}$.

Self-dual codes are related to unimodular lattices and combinatorial objects.

Self-dual codes are interesting algebraic objects in that their weight enumerators are held invariant by the MacWilliams relations.

Self-Dual Codes

Theorem

Let R be a finite Frobenius ring whose residue fields (with respect to the maximal ideals) are $\mathbb{F}_1, \ldots, \mathbb{F}_k$. Then
(1) If $\mathbb{F}_i$ has characteristic $1 \pmod 4$ for all i then there exist free self-dual codes of all even lengths.
(2) If for each i, $\mathbb{F}_i$ has characteristic 1 or $3 \pmod 4$, then there exist free self-dual codes of all lengths congruent to $0 \pmod 4$.

Self-Dual codes over Frobenius Rings, with J.L. Kim, H. Kulosman and Hongwei Liu, Finite Fields and their Applications, Volume 16, January 2010, 14-26.

Big Question 2

- Determine when self-dual codes exist over non-commutative rings.

Big Question 2

- Determine when self-dual codes exist over non-commutative rings.
- Find interesting algebraic and number theoretic connections for self-dual codes over non-commutative rings.

Big Question 2

- Determine when self-dual codes exist over non-commutative rings.
- Find interesting algebraic and number theoretic connections for self-dual codes over non-commutative rings.
- Give constructions of self-dual codes over non-commutative rings.

Big Question 3

Does there exist a binary $[72, 36, 16]$ Type II self-dual code (Type II means all the weights are $0 \pmod 4$)?

Big Question 3

Does there exist a binary $[72, 36, 16]$ Type II self-dual code (Type II means all the weights are $0 \pmod 4$)?
This question has been open for over 40 years, in reality close to 50 years. It is related to a number of combinatorial conjectures.
Every coding theory trick in the book has been tried – some new technique is necessary to solve it.

Big Question 3

Does there exist a binary $[72, 36, 16]$ Type II self-dual code (Type II means all the weights are $0 \pmod 4$)?
This question has been open for over 40 years, in reality close to 50 years. It is related to a number of combinatorial conjectures.
Every coding theory trick in the book has been tried – some new technique is necessary to solve it.
Monetary prizes and a complete description can be found at:
http://academic.scranton.edu/faculty/DOUGHERTYS1/72.htm

Cyclic Codes

Cyclic codes are an extremely important class of codes.

A code C is cyclic if
$(a_0, a_1, \ldots, a_{n-1}) \in C \implies (a_1, a_2, \ldots, a_{n-1}, a_0) \in C$.

Cyclic Codes

Cyclic codes are an extremely important class of codes.

A code C is cyclic if
$(a_0, a_1, \ldots, a_{n-1}) \in C \implies (a_1, a_2, \ldots, a_{n-1}, a_0) \in C$.

$$(a_0, a_1, \ldots, a_{n-1}) \leftrightarrow a_0 + a_1 x + a_2 x^2 \ldots a_{n-1} x^{n-1}$$

Cyclic Codes

Cyclic codes are an extremely important class of codes.

A code C is cyclic if
$(a_0, a_1, \ldots, a_{n-1}) \in C \implies (a_1, a_2, \ldots, a_{n-1}, a_0) \in C$.

$$(a_0, a_1, \ldots, a_{n-1}) \leftrightarrow a_0 + a_1x + a_2x^2 \ldots a_{n-1}x^{n-1}$$

A cyclic code is an ideal in $R[x]/\langle x^n - 1\rangle$.

Cyclic Codes

Cyclic codes are classified by finding all ideals in $R[x]/\langle x^n - 1\rangle$.

Generally easy for codes over fields, namely find the divisors of $x^n - 1$. Much harder for codes over rings, for example, cyclic codes over $\mathbb{Z}_4$ of even length (i.e. length not relatively prime to characteristic of the ring) is quite complicated.

S.T. Dougherty and San Ling, Cyclic codes over $\mathbb{Z}_4$ of even length, Designs, Codes and Cryptography, May 2006, 127-153.

Big Question 4

There is a wealth of open problems here for the talented ring theorist. That is, determine the ideals in $R[x]/\langle x^n - 1\rangle$.

Big Question 4

There is a wealth of open problems here for the talented ring theorist. That is, determine the ideals in $R[x]/\langle x^n - 1\rangle$.
A lot has been done in the commutative case, but very little for the non-commutative case. Even for the commutative case it has only been done for a handful of rings.

Big Question 4

There is a wealth of open problems here for the talented ring theorist. That is, determine the ideals in $R[x]/\langle x^n - 1\rangle$.

A lot has been done in the commutative case, but very little for the non-commutative case. Even for the commutative case it has only been done for a handful of rings.

More generally, determine the ideals in $R[x]/\langle x^n - a\rangle$, where a is some constant. This is classifying constacyclic codes.

Big Question 4

In complete generality, study the group ring. For example, the the cyclic group gives cyclic codes. This is only started to be studied in the commutative case.

Non-Hamming Metric

Example: Rosenbloom-Tsfasman Metric

$$\begin{array}{cccc} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{array}$$

Distance to $\mathbf{0}$ is $3 + 4 + 1 + 2 = 9$.

Rosenbllom-Tsfasman

MDS codes with respect to this metric are related to uniform distributions and (T, M, S)-nets.

Rosenbllom-Tsfasman

MDS codes with respect to this metric are related to uniform distributions and (T, M, S)-nets.
This notion has been generalized to using a poset to determine the metric.

Big Question 5

Find corresponding coding theoretic results for non-Hamming metrics. As usual most results are for a commutative alphabet.

Infinite rings

Codes have also been defined over the p-adics. The benefit here is that they can then be projected down to codes over the finite ring $\mathbb{Z}_{p^e}$.

Infinite rings

Codes have also been defined over the p-adics. The benefit here is that they can then be projected down to codes over the finite ring $\mathbb{Z}_{p^e}$.

This notion has been further generalized to other infinite rings where there is a natural projection to a family of finite rings.

Big Question 6

Find interesting infinite rings with canonical projections to finite rings and develop coding theory over these rings.

Questions