Coding Theory as Pure Mathematics

Steven T. Dougherty

February 24, 2013

Origins of Coding Theory

How does one communicate electronic information effectively?
Namely can one detect and correct errors made in transmission?

Origins of Coding Theory

How does one communicate electronic information effectively?
Namely can one detect and correct errors made in transmission?
Shannon's Theorem: You can always communicate effectively no matter how noisy the channel.

Classical Fundamental Question of Coding Theory

What is the largest (linear) subset of $\mathbb{F}_2^n$ you can have such that any two words are at least d apart, where two words are s units apart if they differ in s places.

Classical Fundamental Question of Coding Theory

What is the largest (linear) subset of $\mathbb{F}_2^n$ you can have such that any two words are at least d apart, where two words are s units apart if they differ in s places.
For linear codes minimum distance becomes minimum weight, where $wt(\mathbf{v})$ is the number of non-zero elements of $\mathbf{v}$, since $wt(\mathbf{v} - \mathbf{w}) = d(\mathbf{v}, \mathbf{w})$.

E.F. Assmus

The purpose of applied mathematics is to enrich pure mathematics. – E.F. Assmus 1931-1998.

E.F. Assmus

The purpose of applied mathematics is to enrich pure mathematics. – E.F. Assmus 1931-1998.
Modified version: A very nice benefit of applied mathematics is that it enriches pure mathematics.

Mathematical Foundations

A code C of length n is a subset of $\mathbb{F}_q^n$ of size M and minimum distance d, denoted $[n, M, d]$.

Mathematical Foundations

A code C of length n is a subset of $\mathbb{F}_q^n$ of size M and minimum distance d, denoted $[n, M, d]$.
If C is linear $M = q^k$, k the dimension, and it is denoted by $[n, k, d]$.

Mathematical Foundations

A code C of length n is a subset of $\mathbb{F}_q^n$ of size M and minimum distance d, denoted $[n, M, d]$.
If C is linear $M = q^k$, k the dimension, and it is denoted by $[n, k, d]$.
Attached to the ambient space is the inner-product

$$[\mathbf{v}, \mathbf{w}] = \sum v_i w_i.$$

Mathematical Foundations

A code C of length n is a subset of $\mathbb{F}_q^n$ of size M and minimum distance d, denoted $[n, M, d]$.
If C is linear $M = q^k$, k the dimension, and it is denoted by $[n, k, d]$.
Attached to the ambient space is the inner-product

$$[\mathbf{v}, \mathbf{w}] = \sum v_i w_i.$$

Define $C^\perp = \{\mathbf{v} \mid [\mathbf{v}, \mathbf{w}] = 0, \forall \mathbf{w} \in C\}$.

Mathematical Foundations

If C is a linear code in $\mathbb{F}_q^n$ then $dim(C) + dim(C^{\perp}) = n$.

Mathematical Foundations

If C is a linear code in $\mathbb{F}_q^n$ then $dim(C) + dim(C^{\perp}) = n$.
All codes have a minimal generating set (basis) so it has a generating matrix G. The code $C^{\perp}$ has a generating matrix H (parity check matrix) so

$$\mathbf{v} \in C \iff Hv^T = \mathbf{0}.$$

Mathematical Foundations

If C is a linear code in $\mathbb{F}_q^n$ then $dim(C) + dim(C^\perp) = n$.
All codes have a minimal generating set (basis) so it has a generating matrix G. The code $C^\perp$ has a generating matrix H (parity check matrix) so

$$\mathbf{v} \in C \iff Hv^T = \mathbf{0}.$$

The matrix H is used extensively in decoding.

Example: Hamming Code

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Example: Hamming Code

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Then C is a $[7, 4, 3]$ code such that any vector in $\mathbb{F}_2^n$ is at most distance 1 from a unique vector in the code.

Classical Engineering Use of Coding Theory

- Construction of a communication system where errors in communication are not only detected but corrected.

Classical Engineering Use of Coding Theory

- Construction of a communication system where errors in communication are not only detected but corrected.
- Cryptography and secret sharing schemes

Mathematical Use of Coding Theory

- Constructing lattices

Mathematical Use of Coding Theory

- Constructing lattices
- Connections to number theory (modular forms, etc.)

Mathematical Use of Coding Theory

- Constructing lattices
- Connections to number theory (modular forms, etc.)
- Connection to designs (constructing, proving non-existence and proving non-isomorphic)

Mathematical Use of Coding Theory

- Constructing lattices
- Connections to number theory (modular forms, etc.)
- Connection to designs (constructing, proving non-existence and proving non-isomorphic)
- Connections to algebraic geometry

Mathematical Use of Coding Theory

- Constructing lattices
- Connections to number theory (modular forms, etc.)
- Connection to designs (constructing, proving non-existence and proving non-isomorphic)
- Connections to algebraic geometry
- Connections to combinatorics

Singleton Bound

Theorem

Let C be an $[n, q^k, d]$ code, then $d \leq n - k + 1$.

Singleton Bound

Theorem

Let C be an $[n, q^k, d]$ *code, then* $d \leq n - k + 1$.

Proof.

Consider the first $n - (d - 1)$ coordinates. These must all be distinct, otherwise the distance between two vectors would be less than d. Hence $k \leq n - (d - 1) = n - d + 1$. □

Singleton Bound

Theorem

Let C be an $[n, q^k, d]$ code, then $d \leq n - k + 1$.

Proof.

Consider the first $n - (d - 1)$ coordinates. These must all be distinct, otherwise the distance between two vectors would be less than d. Hence $k \leq n - (d - 1) = n - d + 1$. □

If C meets this bound the code is called a Maximum Distance Separable (MDS) code.

Singleton Bound

Theorem

A set of s MOLS of order q is equivalent to an MDS an $[s+2, q^2, s+1]$ MDS code.

Extremely difficult question in pure mathematics.

Jessie MacWilliams (1917-1990)

Theorem

(**MacWilliams I**) *Let C be a linear code over a finite field, then every Hamming isometry $C \to R^n$ can be extended to a monomial transformation.*

Jessie MacWilliams (1917-1990)

Theorem

(**MacWilliams I**) *Let* C *be a linear code over a finite field, then every Hamming isometry* $C \to R^n$ *can be extended to a monomial transformation.*

Hamming Weight Enumerator:

$$W_C(x, y) = \sum_{\mathbf{c} \in C} x^{n - wt(\mathbf{c})} y^{wt(\mathbf{c})}$$

Jessie MacWilliams (1917-1990)

Theorem

(**MacWilliams I**) *Let C be a linear code over a finite field, then every Hamming isometry $C \to R^n$ can be extended to a monomial transformation.*

Hamming Weight Enumerator:

$$W_C(x, y) = \sum_{\mathbf{c} \in C} x^{n - wt(\mathbf{c})} y^{wt(\mathbf{c})}$$

Theorem

(**MacWilliams Relations**) *Let C be a linear code over $\mathbb{F}_q$ then*

$$W_{C^\perp}(x, y) = \frac{1}{|C|} W_C(x + (q-1)y, x - y).$$

A big step forward – Gray Map

Classical Coding Theory gets a shock!

A big step forward – Gray Map

Classical Coding Theory gets a shock!

$$\phi : \mathbb{Z}_4 \to \mathbb{F}_2^2$$

$$\begin{array}{ccc} 0 & \to & 00 \\ 1 & \to & 01 \\ 2 & \to & 11 \\ 3 & \to & 10 \end{array}$$

A big step forward – Gray Map

Classical Coding Theory gets a shock!

$$\phi : \mathbb{Z}_4 \to \mathbb{F}_2^2$$

$$\begin{array}{ccc} 0 & \to & 00 \\ 1 & \to & 01 \\ 2 & \to & 11 \\ 3 & \to & 10 \end{array}$$

A non-linear distance preserving map. Many interesting non-linear binary codes are actually images of linear codes (modules) over $\mathbb{Z}_4$.

A big step forward – Gray Map

Classical Coding Theory gets a shock!

$$\phi : \mathbb{Z}_4 \to \mathbb{F}_2^2$$

$$\begin{array}{ccc} 0 & \to & 00 \\ 1 & \to & 01 \\ 2 & \to & 11 \\ 3 & \to & 10 \end{array}$$

A non-linear distance preserving map. Many interesting non-linear binary codes are actually images of linear codes (modules) over $\mathbb{Z}_4$. Important weight in $\mathbb{Z}_4$ is Lee weight, i.e. the weight of the binary image.

A New Beginning

It now becomes interesting to study codes over a larger class of alphabets with an algebraic structure, namely rings.

Codes over Rings

New Definitions

$$\begin{aligned} \text{field} &\rightarrow \textit{ring} \\ \text{dimension} &\rightarrow \textit{rank}, \textit{type}, \textit{other} \\ \text{Hamming weight} &\rightarrow \textit{appropriate metric} \\ \text{vector space} &\rightarrow \textit{module} \end{aligned}$$

Modified Fundamental Question of Coding Theory

What is the largest (linear) subspace of R^n, R a ring, such that any two vectors are at least d units apart, where d is with respect to the appropriate metric?

Jay Wood

What is the largest class of codes you can use for coding theory?

Jay Wood

What is the largest class of codes you can use for coding theory? You want both MacWilliams Theorems to be true in order to use most of the tools of coding theory.

Jay Wood

What is the largest class of codes you can use for coding theory? You want both MacWilliams Theorems to be true in order to use most of the tools of coding theory.

Answer: Frobenius Rings

Frobenius Rings

Definition of Frobenius Rings

A module M over a ring R is injective if, for every pair of left R-modules $B_1 \subset B_2$ and every R-linear mapping $f : B_1 \to M$, the mapping f extends to an R-linear mapping $\overline{f} : B_2 \to M$.

Frobenius Rings

Definition of Frobenius Rings

A module M over a ring R is injective if, for every pair of left R-modules $B_1 \subset B_2$ and every R-linear mapping $f : B_1 \to M$, the mapping f extends to an R-linear mapping $\overline{f} : B_2 \to M$.

For a commutative ring R, R is Frobenius if and only if the R module R is injective.

MacWilliams I revisted

Theorem

*(**MacWilliams I**) (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 I revisted

Theorem

(**MacWilliams I**) *(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.

Frobenius Rings

For Frobenius rings R, $\widehat{R}$ has a generating character χ, such that $\chi_a(b) = \chi(ab)$.

MacWilliams relations revisited

Complete Weight Enumerator:
Define $W_C(x_0, x_1, \ldots, x_k) = \sum_{\mathbf{c} \in C} x_i^{n_i(\mathbf{c})}$ where $n_i(c)$ is the number of occurences of the i-th element of R in $\mathbf{c}$.

MacWilliams relations revisited

Complete Weight Enumerator:
Define $W_C(x_0, x_1, \ldots, x_k) = \sum_{\mathbf{c} \in C} x_i^{n_i(\mathbf{c})}$ where $n_i(c)$ is the number of occurences of the i-th element of R in $\mathbf{c}$. The matrix T_i is given by:

$$(T_i)_{a,b} = (\chi_a(b)) \tag{1}$$

where a and b are in R.

MacWilliams relations revisited

Complete Weight Enumerator:
Define $W_C(x_0, x_1, \ldots, x_k) = \sum_{\mathbf{c} \in C} x_i^{n_i(\mathbf{c})}$ where $n_i(c)$ is the number of occurences of the i-th element of R in $\mathbf{c}$. The matrix T_i is given by:

$$(T_i)_{a,b} = (\chi_a(b)) \tag{1}$$

where a and b are in R.

Theorem

(Generalized MacWilliams Relations) Let C be a linear code over a Frobenius rings R then

$$W_{C^\perp}(x_0, x_1, \ldots, x_k) = \frac{1}{|C|} W_C(T \cdot (x_0, x_1, \ldots, x_k)) \tag{2}$$

Corollary

Corollary

If C is a linear code over a Frobenius ring then $|C||C^\perp| = |R|^n$.

Corollary

Corollary

If C is a linear code over a Frobenius ring then $|C||C^{\perp}| = |R|^n$.

This often fails for codes over non-Frobenius rings.

Non Frobenius Example

For example:
Let

$$R = \mathbf{F}_2[X, Y]/(X^2, Y^2, XY) = \mathbf{F}_2[x, y],$$

where $x^2 = y^2 = xy = 0$.
$R = \{0, 1, x, y, 1 + x, 1 + y, x + y, 1 + x + y\}$.
The maximal ideal is $\mathfrak{m} = \{0, x, y, x + y\}$.
$\mathfrak{m}^\perp = \mathfrak{m} = \{0, x, y, x + y\}$.
$\mathfrak{m}$ is a self-dual code of length 1.
But $|\mathfrak{m}||\mathfrak{m}^\perp| \neq |R|$.

Useful rings

- Principal Ideal Rings – all ideals generated by a single element

Useful rings

- Principal Ideal Rings – all ideals generated by a single element
- Local rings – rings with a unique maximal ideal

Useful rings

- Principal Ideal Rings – all ideals generated by a single element
- Local rings – rings with a unique maximal ideal
- chain ring – a local rings with ideals ordered by inclusion

Examples

- Principal Ideal Rings – $\mathbb{Z}_n$

Examples

- Principal Ideal Rings – $\mathbb{Z}_n$
- chain ring – $\mathbb{Z}_{p^e}$, p prime

Examples

- Principal Ideal Rings – $\mathbb{Z}_n$
- chain ring – $\mathbb{Z}_{p^e}$, p prime
- Local rings – $\mathbb{F}_2[u, v]$, $u^2 = v^2 = 0$, $uv = vu$

Chinese Remainder Theorem

Let R be a finite commutative ring and let $\mathfrak{a}$ be an ideal of R.

Chinese Remainder Theorem

Let R be a finite commutative ring and let $\mathfrak{a}$ be an ideal of R.
Let $\Psi_{\mathfrak{a}} : R \to R/\mathfrak{a}$ denote the canonical homomorphism $x \mapsto x + \mathfrak{a}$.

Chinese Remainder Theorem

Let R be a finite commutative ring and let $\mathfrak{a}$ be an ideal of R. Let $\Psi_{\mathfrak{a}} : R \rightarrow R/\mathfrak{a}$ denote the canonical homomorphism $x \mapsto x + \mathfrak{a}$. Let R be a finite commutative ring and let $\mathfrak{m}_1, \ldots, \mathfrak{m}_k$ be the maximal ideals of R. Let $e_1, \ldots, e_k$ be their indices of stability. Then the ideals $\mathfrak{m}_1^{e_1}, \ldots, \mathfrak{m}_k^{e_k}$ are relatively prime in pairs and $\prod_{i=1}^k \mathfrak{m}_i^{e_i} = \cap_{i=1}^k \mathfrak{m}_i^{e_i} = \{0\}$.

Chinese Remainder Theorem

Theorem

(Chinese Remainder Theorem) The canonical ring homomorphism $\Psi : R \to \prod_{i=1}^{k} R/\mathfrak{m}_i^{e_i}$, *defined by* $x \mapsto (x \pmod{\mathfrak{m}_1^{e_1}}, \ldots, x \pmod{\mathfrak{m}_k^{e_k}})$, *is an isomorphism.*

Chinese Remainder Theorem

Theorem

(Chinese Remainder Theorem) The canonical ring homomorphism $\Psi : R \to \prod_{i=1}^{k} R/\mathfrak{m}_i^{e_i}$*, defined by* $x \mapsto (x \pmod{\mathfrak{m}_1^{e_1}}, \ldots, x \pmod{\mathfrak{m}_k^{e_k}})$*, is an isomorphism.*

Given codes C_i of length n over $R/\mathfrak{m}_i^{e_i} \quad (i = 1, \ldots, k)$, we define the code $C = \mathrm{CRT(C_1, \ldots, C_k)}$ of length n over R as:

$$
\begin{aligned}
C &= \{\Psi^{-1}(\mathbf{v_1}, \ldots, \mathbf{v_k}) : \mathbf{v_i} \in C_i \, (i = 1, \ldots, k)\} \\
&= \{\mathbf{v} \in R^n : \Psi_{\mathfrak{m}_i^{t_i}}(\mathbf{v}) \in C_i \, (i = 1, \ldots, k)\}.
\end{aligned}
$$

Chinese Remainder Theorem

Theorem

If R is a finite commutative Frobenius ring, then R is isomorphic via the Chinese Remainder Theorm to $R_1 \times R_2 \times \cdots \times R_s$ where each R_i is a local Frobenius ring.

Chinese Remainder Theorem

Theorem

If R is a finite commutative Frobenius ring, then R is isomorphic via the Chinese Remainder Theorm to $R_1 \times R_2 \times \cdots \times R_s$ where each R_i is a local Frobenius ring.

Theorem

If R is a finite commutative principal ideal ring then then R is isomorphic to $R_1 \times R_2 \times \cdots \times R_s$ where each R_i is a chain ring.

MDR Codes

Theorem
Let C be a linear code over a principal ideal ring, then

$$d_H(C) \leq n - rank(C) + 1.$$

MDR Codes

Theorem

Let C be a linear code over a principal ideal ring, then

$$d_H(C) \leq n - rank(C) + 1.$$

Codes meeting this bound are called *MDR (Maximum Distance with respect to Rank) codes*.

MDR Codes

Theorem

Let C be a linear code over a principal ideal ring, then

$$d_H(C) \leq n - rank(C) + 1.$$

Codes meeting this bound are called *MDR (Maximum Distance with respect to Rank) codes*.

Theorem

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

Generating vectors

Over $\mathbb{Z}_6$, $\langle (2,3) \rangle = \{(0,0),(2,3),(4,0),(0,3),(2,0),(4,3)\}$.

Generating vectors

Over $\mathbb{Z}_6$, $\langle(2,3)\rangle = \{(0,0),(2,3),(4,0),(0,3),(2,0),(4,3)\}$.
This is strange since we would rather have say it is generated by
$\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$.

Generator Matrices over Chain Rings

Let R be a finite chain ring with maximal ideal $\mathfrak{m} = R\gamma$ with e its nilpotency index.

The generator matrix for a code C over R is permutation equivalent to a matrix of the following form:

$$\begin{pmatrix} I_{k_0} & A_{0,1} & A_{0,2} & A_{0,3} & \cdots & \cdots & A_{0,e} \\ 0 & \gamma I_{k_1} & \gamma A_{1,2} & \gamma A_{1,3} & \cdots & \cdots & \gamma A_{1,e} \\ 0 & 0 & \gamma^2 I_{k_2} & \gamma^2 A_{2,3} & \cdots & \cdots & \gamma^2 A_{2,e} \\ \vdots & \vdots & 0 & \ddots & \ddots & & \vdots \\ \vdots & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & \gamma^{e-1} I_{k_{e-1}} & \gamma^{e-1} A_{e-1,e} \end{pmatrix} \tag{3}$$

Generator Matrices over Chain Rings

Let R be a finite chain ring with maximal ideal $\mathfrak{m} = R\gamma$ with e its nilpotency index.

The generator matrix for a code C over R is permutation equivalent to a matrix of the following form:

$$\begin{pmatrix} I_{k_0} & A_{0,1} & A_{0,2} & A_{0,3} & \cdots & \cdots & A_{0,e} \\ 0 & \gamma I_{k_1} & \gamma A_{1,2} & \gamma A_{1,3} & \cdots & \cdots & \gamma A_{1,e} \\ 0 & 0 & \gamma^2 I_{k_2} & \gamma^2 A_{2,3} & \cdots & \cdots & \gamma^2 A_{2,e} \\ \vdots & \vdots & 0 & \ddots & \ddots & & \vdots \\ \vdots & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & \gamma^{e-1} I_{k_{e-1}} & \gamma^{e-1} A_{e-1,e} \end{pmatrix} \tag{3}$$

A code with generator matrix of this form is said to have type $\{k_0, k_1, \ldots, k_{e-1}\}$. It is immediate that a code C with this generator matrix has

$$|C| = |R/\mathfrak{m}|^{\sum_{i=0}^{e-1}(e-i)k_i}. \tag{4}$$

Minimal Generating Sets

Definition

Let R_i be a local ring with unique maximal ideal $\mathfrak{m}_i$, and let $\mathbf{w}_1, \cdots, \mathbf{w}_s$ be vectors in R_i^n. Then $\mathbf{w}_1, \cdots, \mathbf{w}_s$ are modular independent if and only if $\sum \alpha_j \mathbf{w}_j = \mathbf{0}$ implies that $\alpha_j \in \mathfrak{m}_i$ for all j.

Minimal Generating Sets

Definition

Let R_i be a local ring with unique maximal ideal $\mathfrak{m}_i$, and let $\mathbf{w}_1, \cdots, \mathbf{w}_s$ be vectors in R_i^n. Then $\mathbf{w}_1, \cdots, \mathbf{w}_s$ are modular independent if and only if $\sum \alpha_j \mathbf{w}_j = \mathbf{0}$ implies that $\alpha_j \in \mathfrak{m}_i$ for all j.

Definition

The vectors $\mathbf{v}_1, \cdots, \mathbf{v}_k$ in R^n are modular independent if $\Phi_i(\mathbf{v}_1), \cdots, \Phi_i(\mathbf{v}_k)$ are modular independent for some i, where $R = CRT(R_1, R_2, \ldots, R_s)$ and Φ_i is the canonical map.

Minimal Generating Sets

Definition

Let $\mathbf{v}_1, \cdots, \mathbf{v}_k$ be vectors in R^n. Then $\mathbf{v}_1, \cdots, \mathbf{v}_k$ are independent if $\sum \alpha_j \mathbf{v}_j = \mathbf{0}$ implies that $\alpha_j \mathbf{v}_j = \mathbf{0}$ for all j.

Minimal Generating Sets

Definition

Let $\mathbf{v}_1, \cdots, \mathbf{v}_k$ be vectors in R^n. Then $\mathbf{v}_1, \cdots, \mathbf{v}_k$ are independent if $\sum \alpha_j \mathbf{v}_j = \mathbf{0}$ implies that $\alpha_j \mathbf{v}_j = \mathbf{0}$ for all j.

Definition

Let C be a code over R. The codewords $\mathbf{c}_1, \mathbf{c}_2, \cdots, \mathbf{c}_k$ is called a *basis* of C if they are independent, modular independent and generate C. In this case, each $\mathbf{c}_i$ is called a generator of C.

Minimal Generating Sets

Theorem

All linear codes over a Frobenius ring have a basis.

Coding Theory over Rings

- MacWilliams I and II still hold.

Coding Theory over Rings

- MacWilliams I and II still hold.
- We have a new algebraic Singleton bound.

Coding Theory over Rings

- MacWilliams I and II still hold.
- We have a new algebraic Singleton bound.
- We have a new notion of a basis.

Works in Progress

- Work towards answering the modified fundamental question of Coding Theory.

Works in Progress

- Work towards answering the modified fundamental question of Coding Theory.
- Find interesting connections to number theory, algebra, and combinatorics in this setting.

Works in Progress

- Work towards answering the modified fundamental question of Coding Theory.
- Find interesting connections to number theory, algebra, and combinatorics in this setting.
- Find applications outside of mathematics.