Coding Theory as Pure Mathematics

Steven T. Dougherty

July 1, 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.

Foundations

Shannon, C. E. A mathematical theory of communication. Bell System Tech. J. 27, (1948). 379 -423, 623 - 656. (Cited 612 times in MathSciNet).

Foundations

Shannon, C. E. A mathematical theory of communication. Bell System Tech. J. 27, (1948). 379 -423, 623 - 656. (Cited 612 times in MathSciNet).

R. W. Hamming, Error detecting and error correcting codes, Bell System Tech. J. 29 (1950), 147- 160.

Foundations

Shannon, C. E. A mathematical theory of communication. Bell System Tech. J. 27, (1948). 379 -423, 623 - 656. (Cited 612 times in MathSciNet).

R. W. Hamming, Error detecting and error correcting codes, Bell System Tech. J. 29 (1950), 147- 160.

Marcel J. E. Golay, Notes on digital coding [Proc. IRE 37 (1949), 657]

Foundations

To communicate you need:

- Efficiently encode the information.

Foundations

To communicate you need:

- Efficiently encode the information.
- Have a code where the distance between vectors is as large as possible so that errors can be corrected.

Foundations

To communicate you need:

- Efficiently encode the information.
- Have a code where the distance between vectors is as large as possible so that errors can be corrected.
- Have as many elements in the code as possible so that as much information as possible can be sent.

Foundations

To communicate you need:

- Efficiently encode the information.
- Have a code where the distance between vectors is as large as possible so that errors can be corrected.
- Have as many elements in the code as possible so that as much information as possible can be sent.
- An efficient algorithm to decode the information.

Classical Fundamental Question of Coding Theory

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

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

Classical Fundamental Question of Coding Theory

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, where the weight of $\mathbf{v}$ is $wt(\mathbf{v}) = |\{i \mid v_i \neq 0\}|$.

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.

My modified version: A very nice benefit of applied mathematics is that it enriches pure mathematics.

Basic Definitions

A code over an alphabet A of length n is a subset of A^n.

Basic Definitions

A code over an alphabet A of length n is a subset of A^n.
Initially, A was $\mathbb{F}_2$, then $\mathbb{F}_q$ was considered. More, recently A is allowed to be a ring, module or group.

Basic Definitions

A code over an alphabet A of length n is a subset of A^n.
Initially, A was $\mathbb{F}_2$, then $\mathbb{F}_q$ was considered. More, recently A is allowed to be a ring, module or group.
In general, we are concerned with any alphabet A but we are particularly concerned with A when it has an algebraic structure.

Basic Definitions

A code over an alphabet A of length n is a subset of A^n.
Initially, A was $\mathbb{F}_2$, then $\mathbb{F}_q$ was considered. More, recently A is allowed to be a ring, module or group.
In general, we are concerned with any alphabet A but we are particularly concerned with A when it has an algebraic structure.
We say the code is linear when the code itself has that algebraic structure, e.g. a code over $\mathbb{F}_q$ is linear when it is a vector space, and a code over a ring is linear if it is a submodule.

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

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

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

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

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.

Connection to Finite Geometry

The weight 3 vectors in the $[7, 4, 3]$ Hamming code correspond to the lines in a projective plane of order 2.

Connection to Finite Geometry

The weight 3 vectors in the $[7, 4, 3]$ Hamming code correspond to the lines in a projective plane of order 2.

The weight 4 vectors in the $[7, 4, 3]$ Hamming code correspond to the correspond to the hyperovals in the projecitve plane of order 2.

Hamming Code

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

Assume the vector received is $\mathbf{v} = (1010111)$, then $H\mathbf{v}^T = (110)$.

Hamming Code

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

Assume the vector received is $\mathbf{v} = (1010111)$, then $H\mathbf{v}^T = (110)$. So the correct vector is (1010101) which corresponds to a hyperoval in the projective plane of order 2.

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.
- Used in telephones, television, CDs, DVDs, computer to computer communication.

Classical Engineering Use of Coding Theory

- Construction of a communication system where errors in communication are not only detected but corrected.
- Used in telephones, television, CDs, DVDs, computer to computer communication.
- Cryptography and secret sharing schemes.

Mathematical Use of Coding Theory

- Constructing lattices, e.g. recent construction of extremal lattice at length 72

Mathematical Use of Coding Theory

- Constructing lattices, e.g. recent construction of extremal lattice at length 72
- Connections to number theory (modular forms, etc.)

Mathematical Use of Coding Theory

- Constructing lattices, e.g. recent construction of extremal lattice at length 72
- Connections to number theory (modular forms, etc.)
- Connection to designs (constructing, proving non-existence and proving non-isomorphic), e.g. proof of the non-existence of the projective plane of order 10

Mathematical Use of Coding Theory

- Constructing lattices, e.g. recent construction of extremal lattice at length 72
- Connections to number theory (modular forms, etc.)
- Connection to designs (constructing, proving non-existence and proving non-isomorphic), e.g. proof of the non-existence of the projective plane of order 10
- Connections to algebraic geometry

Mathematical Use of Coding Theory

- Constructing lattices, e.g. recent construction of extremal lattice at length 72
- Connections to number theory (modular forms, etc.)
- Connection to designs (constructing, proving non-existence and proving non-isomorphic), e.g. proof of the non-existence of the projective plane of order 10
- Connections to algebraic geometry
- Connections to combinatorics, e.g. MDS codes and mutually orthogonal latin squares and arcs in projective geometry

Singleton Bound

Theorem

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

Singleton Bound

Theorem

Let C be an $[n, q^k, d]$ code over an alphabet of size q, 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 over an alphabet of size q, 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

Connection to combinatorics.

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

Extremely difficult question in pure mathematics.

Sphere Packing Bound

Theorem

*(**Sphere Packing Bound**) Let C be a code over $\mathbb{F}_q$ of length n with $M = |C|$ and minimum distance $2t + 1$. Then*

$$M(1 + (q-1)n + (q-1)^2 \binom{n}{2} + \cdots + (q-1)^t \binom{n}{t}) \leq q^n.$$

Sphere Packing Bound

Theorem

(**Sphere Packing Bound**) *Let C be a code over $\mathbb{F}_q$ of length n with $M = |C|$ and minimum distance $2t + 1$. Then*

$$M(1 + (q-1)n + (q-1)^2 \binom{n}{2} + \cdots + (q-1)^t \binom{n}{t}) \leq q^n.$$

A code meeting this bound is called a perfect code.

Perfect Codes

The $[7, 4, 3]$ Hamming code given before is a perfect code.

Perfect Codes

The $[7, 4, 3]$ Hamming code given before is a perfect code.

The $[23, 12, 7]$ binary Golay code is a perfect code.

Perfect Codes

The $[7, 4, 3]$ Hamming code given before is a perfect code.

The $[23, 12, 7]$ binary Golay code is a perfect code.

The $[11, 6, 5]$ ternary Golay code is a perfect code.

Perfect Code

Example of a connection to combinatorics. A Steiner system is a t-design with $\lambda = 1$. A $t - (v, k, \lambda)$ Steiner system is denoted $S(, t, v, k)$.

Perfect Code

Example of a connection to combinatorics. A Steiner system is a t-design with $\lambda = 1$. A $t - (v, k, \lambda)$ Steiner system is denoted $S(, t, v, k)$.

Theorem

*(**Assmus and Mattson**) If there exists a perfect binary t-error correcting code of length n, then there exists a Steiner system $S(t+1, 2t+1, n)$.*

Jessie MacWilliams (1917-1990)

Theorem

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

Jessie MacWilliams (1917-1990)

MacWilliams, Jessie A theorem on the distribution of weights in a systematic code. Bell System Tech. J. 42 1963 79-94.

Jessie MacWilliams (1917-1990)

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)

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*

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

Interesting Families of Codes

Cyclic Codes

Cyclic codes are an extremely important class of codes – initially because of an efficient decoding algorithm.

A code C is cyclic if
$(a_0, a_1, \ldots, a_{n-1}) \in C \implies (a_{n-1}, a_0, a_1, a_2, \ldots, a_{n-2}) \in C$.

Cyclic Codes

Cyclic codes are an extremely important class of codes – initially because of an efficient decoding algorithm.

A code C is cyclic if
$(a_0, a_1, \ldots, a_{n-1}) \in C \implies (a_{n-1}, a_0, a_1, a_2, \ldots, a_{n-2}) \in C$.

Let $\pi((a_0, a_1, \ldots, a_{n-1})) = (a_{n-1}, a_0, a_1, a_2, \ldots, a_{n-2})$. So a cyclic code C has $\pi(C) = C$.

Cyclic Codes

There is a natural connection from vectors in a cyclic code to polynomials:

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

Cyclic Codes

There is a natural connection from vectors in a cyclic code to polynomials:

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

Notice that $\pi((a_0, a_1, \ldots, a_{n-1}))$ corresponds to $x(a_0 + a_1 x + a_2 x^2 \ldots a_{n-1} x^{n-1}) \pmod{x^n - 1}$.

Cyclic Codes

Then if C is linear over F and invariant under π then a cyclic code corresponds to an ideal in $F[x]/\langle x^n - 1\rangle$.

Cyclic Codes

Then if C is linear over F and invariant under π then a cyclic code corresponds to an ideal in $F[x]/\langle x^n - 1 \rangle$.

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

Cyclic Codes

Then if C is linear over F and invariant under π then a cyclic code corresponds to an ideal in $F[x]/\langle x^n - 1\rangle$.

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

Easily done when the length of the code is relatively prime to the characteristic of the field, that is we factor $x^n - 1$ uniquely in $F[x]$.

Constacyclic Codes

A code C is constacyclic if
$(a_0, a_1, \ldots, a_{n-1}) \in C \implies (\lambda_{n-1}, a_0, a_1, a_2, \ldots, a_{n-2}) \in C$ for some $\lambda \in F$.

Constacyclic Codes

A code C is constacyclic if $(a_0, a_1, \ldots, a_{n-1}) \in C \implies (\lambda_{n-1}, a_0, a_1, a_2, \ldots, a_{n-2}) \in C$ for some $\lambda \in F$.

If $\lambda = -1$ the codes are said to be negacyclic.

Constacyclic Codes

A code C is constacyclic if $(a_0, a_1, \ldots, a_{n-1}) \in C \implies (\lambda_{n-1}, a_0, a_1, a_2, \ldots, a_{n-2}) \in C$ for some $\lambda \in F$.

If $\lambda = -1$ the codes are said to be negacyclic.

Under the same reasoning, constacyclic codes corresponds to ideals in $F[x]/\langle x^n - \lambda \rangle$.

Hamming Codes

Let H be the matrix whose columns consist of the $(q^r - 1)/(q - 1)$ distinct non-zero vectors of $\mathbb{F}_q^r$ modulo scalar multiples. Then let $C = \langle H \rangle^\perp$.

Hamming Codes

Let H be the matrix whose columns consist of the $(q^r - 1)/(q - 1)$ distinct non-zero vectors of $\mathbb{F}_q^r$ modulo scalar multiples. Then let $C = \langle H \rangle^\perp$.

Then C is a $[(q^r - 1)/(q - 1), (q^r - 1)/(q - 1) - r, 3]$ perfect code.

Hamming Codes

Let H be the matrix whose columns consist of the $(q^r - 1)/(q - 1)$ distinct non-zero vectors of $\mathbb{F}_q^r$ modulo scalar multiples. Then let $C = \langle H \rangle^{\perp}$.

Then C is a $[(q^r - 1)/(q - 1), (q^r - 1)/(q - 1) - r, 3]$ perfect code.

These codes are the Generalized Hamming Codes.

Hamming Codes

For example $r = 3, q = 3$,

$$H = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 1 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \end{pmatrix}$$

Hamming Codes

For example $r = 3, q = 3$,

$$H = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 1 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \end{pmatrix}$$

C is a $[13, 10, 3]$ perfect code over $\mathbb{F}_3$.

Simplex Codes

The Simplex Codes are $[2^r - 1, r, 2^{r-1}]$ codes and are the orthogonals to the binary Hamming Codes.

BCH Codes

Let $\mathbb{F}_q = \{0, b_1, \ldots, b_{q-1}\}$, let $a_i = b_j$ for some j and $a_i \neq a_j$ if $i \neq j$.

BCH Codes

Let $\mathbb{F}_q = \{0, b_1, \ldots, b_{q-1}\}$, let $a_i = b_j$ for some j and $a_i \neq a_j$ if $i \neq j$. The let

$$H = \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ a_1 & a_2 & a_3 & \ldots & a_n \\ a_1^2 & a_2^2 & a_3^2 & \ldots & a_n^2 \\ \vdots & & & & \\ a_1^{d-2} & a_2^{d-2} & a_3^{d-2} & \ldots & a_n^{d-2} \end{pmatrix}$$

BCH Codes

The matrix H is a Vandermonde matrix and as such has a non-zero determinant. Hence the $d-1$ rows and $d-1$ columns are linearly independent.

BCH Codes

The matrix H is a Vandermonde matrix and as such has a non-zero determinant. Hence the $d-1$ rows and $d-1$ columns are linearly independent.

Let $C = \langle H \rangle^{\perp}$. Then C is a $[n, n-(d-1), d]$ code.

BCH Codes

The matrix H is a Vandermonde matrix and as such has a non-zero determinant. Hence the $d-1$ rows and $d-1$ columns are linearly independent.

Let $C = \langle H \rangle^{\perp}$. Then C is a $[n, n-(d-1), d]$ code.

Then $n-k+1 = n-(n-(d-1))+1 = d$ and the code meets the Singleton bound.

BCH Codes

As an example, let

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 \\ 1 & 4 & 4 & 1 \end{pmatrix}$$

BCH Codes

As an example, let

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 \\ 1 & 4 & 4 & 1 \end{pmatrix}$$

Then C is a $[4, 1, 4]$ code and $4 - 1 + 1 = 4$ and the code is MDS over $\mathbb{F}_5$.

BCH Codes

As an example, let

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 \\ 1 & 4 & 4 & 1 \end{pmatrix}$$

Then C is a $[4, 1, 4]$ code and $4 - 1 + 1 = 4$ and the code is MDS over $\mathbb{F}_5$.

In this case $C = \langle (1, 2, 3, 4) \rangle$.

Important Texts for Classical Coding Theory

- F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, Amsterdam, The Netherlands: North-Holland, 1977.

Important Texts for Classical Coding Theory

- F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, Amsterdam, The Netherlands: North-Holland, 1977.
- W.C. Huffman and V.S. Pless, Fundamentals of Error-correcting Codes, Cambridge: Cambridge University Press, 2003.

Important Texts for Classical Coding Theory

- F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, Amsterdam, The Netherlands: North-Holland, 1977.
- W.C. Huffman and V.S. Pless, Fundamentals of Error-correcting Codes, Cambridge: Cambridge University Press, 2003.
- Handbook of Coding Theory, V.S. Pless and W.C. Huffman, eds., 177–294, Elsevier:Amsterdam, 1998.

Important Texts for Connections to Classical Coding Theory

- Conway, J. H.; Sloane, N. J. A. Sphere packings, lattices and groups. Third edition. With additional contributions by E. Bannai, R. E. Borcherds, J. Leech, S. P. Norton, A. M. Odlyzko, R. A. Parker, L. Queen and B. B. Venkov. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], 290. Springer-Verlag, New York, 1999.

Important Texts for Connections to Classical Coding Theory

- Conway, J. H.; Sloane, N. J. A. Sphere packings, lattices and groups. Third edition. With additional contributions by E. Bannai, R. E. Borcherds, J. Leech, S. P. Norton, A. M. Odlyzko, R. A. Parker, L. Queen and B. B. Venkov. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], 290. Springer-Verlag, New York, 1999.
- Assmus, E. F., Jr.; Key, J. D. Designs and their codes. Cambridge Tracts in Mathematics, 103. Cambridge University Press, Cambridge, 1992.

Quote

We do not have to pretend that what we are doing has anything to do with information transfer any more. – Sasha Barg, University of Cincinnati, Cincinnati Ohio, Oct 2006.

Expansion of Coding Theory

In MacWilliams and Sloane, there are around 1500 cited works from 1948 to 1977.

Expansion of Coding Theory

In MacWilliams and Sloane, there are around 1500 cited works from 1948 to 1977.

A search on MathSciNet for titles with the word code, there are 12,267 items.

What constitutes coding theory

- An algebraic structure to linear codes.

What constitutes coding theory

- An algebraic structure to linear codes.
- A well defined orthogonal inner-product which gives an orthogonal $C^{\perp}$ with

$$|C||C^{\perp}| = |R|^n$$

What constitutes coding theory

- An algebraic structure to linear codes.
- A well defined orthogonal inner-product which gives an orthogonal $C^{\perp}$ with

$$|C||C^{\perp}| = |R|^n$$

- MacWilliams Theorem 1

What constitutes coding theory

- An algebraic structure to linear codes.
- A well defined orthogonal inner-product which gives an orthogonal $C^{\perp}$ with

$$|C||C^{\perp}| = |R|^n$$

- MacWilliams Theorem 1
- MacWilliams Theorem 2

A big step forward – Gray Map

Classical Coding Theory gets a shock!

A big step forward – Gray Map

Classical Coding Theory gets a shock!

A.R. Hammons, P.V. Kumar, A.R. Calderbank, N.J.A. Sloane and P. Solé, The $\mathbb{Z}_4$-linearity of kerdock, preparata, goethals and related codes, *IEEE Trans. Inform. Theory*, vol. 40, pp. 301-319, 1994. (Cited 221 times).

A big step forward – Gray Map

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

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

A big step forward – Gray Map

The map ϕ is a non-linear distance preserving map.

A big step forward – Gray Map

The map ϕ is a non-linear distance preserving map.

Important weight in $\mathbb{Z}_4$ is Lee weight, i.e. the weight of the binary image.

A big step forward – Gray Map

The map ϕ is a non-linear distance preserving map.

Important weight in $\mathbb{Z}_4$ is Lee weight, i.e. the weight of the binary image.

The authors show that the Kerdock, the Preparata and the Nordstrom-Robinson codes, while non-linear binary codes, are the images of linear quaternary codes.

A big step forward – Gray Map

In retrospect, the following paper should have helped understand this earlier.

Delsarte, P., An algebraic approach to the association schemes of coding theory. Philips Res. Rep. Suppl., Vol. 10, (1973). (Cited 216 times).

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?

Quote

Why should we care about codes over Frobenius rings anyway? – Vera Pless. AMS Special Topic Session, Notre Dame University, April 2000.

Jay Wood

Wood, J.: Duality for modules over finite rings and applications to coding theory, Amer. J. Math., Vol. 121, No. 3, pp. 555-575 (1999).

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 an algebraic structure to linear codes and a well defined orthogonal inner-product which gives an orthogonal $C^{\perp}$ with $|C||C^{\perp}| = |R|^n$. You also 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 an algebraic structure to linear codes and a well defined orthogonal inner-product which gives an orthogonal $C^{\perp}$ with $|C||C^{\perp}| = |R|^n$. You also want both MacWilliams Theorems to be true in order to use most of the tools of coding theory.

Answer: Frobenius Rings

Nakayama's Definition of Frobenius Rings

We are concerned with finite rings so all of the rings we consider are Artinian but the definitions apply to all Artinian rings.

Nakayama's Definition of Frobenius Rings

We are concerned with finite rings so all of the rings we consider are Artinian but the definitions apply to all Artinian rings.

A left module M is irreducible if it contains no non-trivial left submodule.

Nakayama's Definition of Frobenius Rings

We are concerned with finite rings so all of the rings we consider are Artinian but the definitions apply to all Artinian rings.

A left module M is irreducible if it contains no non-trivial left submodule.

A left module M is indecomposable if it has no non-trivial left direct summands. (N.B. every irreducible module is indecomposable, but not the converse).

Nakayama's Definition of Frobenius Rings

An Artinian ring (as a left module over itself) admits a finite direct sum decomposition:

$$ {}_R R = Re_{1,1} \oplus \ldots Re_{1,\mu_1} \oplus \cdots \oplus Re_{n,1} \oplus \cdots \oplus R_e n, \mu_n, $$

where the $e_{i,j}$ are primitive orthogonal idempotents with $1 = \sum e_{i,j}$.

Nakayama's Definition of Frobenius Rings

This is the principal decomposition of ${}_R R$.

Nakayama's Definition of Frobenius Rings

This is the principal decomposition of ${}_R R$.

The $Re_{i,j}$ are indexed so that $Re_{i,j}$ is isomorphic to $Re_{k,l}$ if and only if $i = k$.

Nakayama's Definition of Frobenius Rings

This is the principal decomposition of ${}_R R$.

The $Re_{i,j}$ are indexed so that $Re_{i,j}$ is isomorphic to $Re_{k,l}$ if and only if $i = k$.

Set $e_i = e_{i,1}$ then we can write:

$${}_R R \cong \oplus \mu_i Re_i$$

Nakayama's Definition of Frobenius Rings

The socle of a module M is the sum of the simple (no non-zero submodules) submodules of M.

Nakayama's Definition of Frobenius Rings

The socle of a module M is the sum of the simple (no non-zero submodules) submodules of M.

The radical of a module M is the intersection of all maximal submodules of M.

Nakayama's Definition of Frobenius Rings

$Re_{i,j}$ has a unique maximal left submodule

$$Rad(R)e_{i,j} = Re_{i,j} \cap Rad(R)$$

Nakayama's Definition of Frobenius Rings

$Re_{i,j}$ has a unique maximal left submodule

$$Rad(R)e_{i,j} = Re_{i,j} \cap Rad(R)$$

and a unique irreducible "top quotient"

$$T(Re_{i,j}) = Re_{i,j}/Rad(R)e_{i,j}.$$

Nakayama's Definition of Frobenius Rings

$Re_{i,j}$ has a unique maximal left submodule

$$Rad(R)e_{i,j} = Re_{i,j} \cap Rad(R)$$

and a unique irreducible "top quotient"

$$T(Re_{i,j}) = Re_{i,j}/Rad(R)e_{i,j}.$$

The socle $S(R_{e,j})$ is the left submodule generated by the irreducible left submodule of $Re_{i,j}$.

Nakayama's Definition of Frobenius Rings

Let ${}_RR = \oplus \mu_i Re_i$. Then an Artinian ring R is quasi-Frobenius if there exists a permutation σ of $\{1, 2, \ldots, n\}$. such that

$$T(Re_i) \cong S(Re_{\sigma(i)})$$

and

$$S(Re_i) \cong T(Re_{\sigma(i)})$$

Nakayama's Definition of Frobenius Rings

Let ${}_RR = \oplus \mu_i Re_i$. Then an Artinian ring R is quasi-Frobenius if there exists a permutation σ of $\{1, 2, \ldots, n\}$. such that

$$T(Re_i) \cong S(Re_{\sigma(i)})$$

and

$$S(Re_i) \cong T(Re_{\sigma(i)})$$

The ring is Frobenius if, in addition, $\mu_{\sigma(i)} = \mu_i$.

Nakayama's 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 $\overline{f} : B_2 \to M$.

Nakayama's 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 $\overline{f} : B_2 \to M$.

Theorem

An Artinian ring R is quasi-Frobenius if and only if R is self-injective, i.e. R is injective as a left(right) module over itself.

Frobenius Rings

For a commutative ring R, R is Frobenius if and only if it is quasi-Frobenius.

Frobenius Rings

For a module M let $\widehat{M}$ be the character module of M.

Frobenius Rings

For a module M let $\widehat{M}$ be the character module of M.

If M is a left module then $\widehat{M}$ is a right module.

Frobenius Rings

For a module M let $\widehat{M}$ be the character module of M.

If M is a left module then $\widehat{M}$ is a right module.

If M is a right module then $\widehat{M}$ is a left module.

Frobenius Rings

Theorem

Let R be a finite quasi-Frobenius ring, with ${}_R R = \oplus \mu_i R e_i$ and with permutation σ as inthe definition of quasi-Frobenius. Then, as left R modules,

$$\widehat{R} \cong \oplus \mu_i R e_{\sigma(i)}$$

and as right modules

$$\widehat{R} \cong \oplus \mu_i e_{\sigma^{-1}(i)} R.$$

Frobenius Rings

Theorem

Suppose R is a finite ring. If $\widehat{R}$ is a free left R-module, then $\widehat{R} \cong_R R$ and R is quasi-Frobenius.

Frobenius Rings

Theorem

Suppose R is a finite ring. The following are equivalent.

- *R is a Frobenius ring.*
- *As a left module, $\widehat{R} \cong {}_R R$.*
- *As a right module $\widehat{R} \cong R_R$.*

Frobenius Rings

Let R be a Frobenius ring, so that $\widehat{R} \cong RR$ as both left and right modules. Let $\phi : R \to \widehat{R}$ be the right module isomorphism.

Frobenius Rings

Let R be a Frobenius ring, so that $\widehat{R} \cong RR$ as both left and right modules. Let $\phi : R \to \widehat{R}$ be the right module isomorphism.

Let $\chi = \phi(1)$ then $\phi(r) = \chi^r$. We call χ a right generating character.

Frobenius Rings

Let R be a Frobenius ring, so that $\widehat{R} \cong {}_RR$ as both left and right modules. Let $\phi : R \to \widehat{R}$ be the right module isomorphism.

Let $\chi = \phi(1)$ then $\phi(r) = \chi^r$. We call χ a right generating character.

Theorem

Let R be any finite ring. Then a character χ on R is a left generating character if and only if it is a right generating character.

MacWilliams I revisited

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 revisited

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.

MacWilliams I revisited

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

M. Greferath, S.E. Schmidt, Finite-ring combinatorics and MacWilliams equivalence theorem, J. Combin. Theory A, 92, 2000, 17-28.

MacWilliams I revisited

Theorem

Suppose R is a finite **commutative** *ring, and suppose that the extension theorem hold over R, that is every weight-preserving linear homomorphism $f : C \to R^n$ from a linear code $C \subseteq R^n$ to R^n extends to a monomial transformation of R^n. 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 $cwe_C(x_0, x_1, \ldots, x_k) = \sum_{\mathbf{c} \in C} x_i^{n_i(\mathbf{c})}$ 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 $cwe_C(x_0, x_1, \ldots, x_k) = \sum_{\mathbf{c} \in C} x_i^{n_i(\mathbf{c})}$ where $n_i(c)$ is the number of occurences of the i-th element of R in $\mathbf{c}$.

The matrix T_i is a $|R|$ by $|R|$ matrix given by:

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

where a and b are in R.

MacWilliams relations revisited

For a code C in R^n define

$$\mathcal{L}(C) = \{\mathbf{v} \mid [\mathbf{v}, \mathbf{w}] = 0, \forall \mathbf{w} \in C\}$$

MacWilliams relations revisited

For a code C in R^n define

$$\mathcal{L}(C) = \{\mathbf{v} \mid [\mathbf{v}, \mathbf{w}] = 0, \forall \mathbf{w} \in C\}$$

and

$$\mathcal{R}(C) = \{\mathbf{v} \mid [\mathbf{w}, \mathbf{v}] = 0, \forall \mathbf{w} \in C\}.$$

MacWilliams relations revisited

Theorem

(Generalized MacWilliams Relations) Let R be a Frobenius ring. If C is a left submodule of R^n, then

$$cwe_C(x_0, x_1, \ldots, x_k) = \frac{1}{|\mathcal{R}(C)|} cwe_{\mathcal{R}(C)}(T^t \cdot (x_0, x_1, \ldots, x_k)).$$

If C is a right submodule of R^n, then

$$cwe_C(x_0, x_1, \ldots, x_k) = \frac{1}{|\mathcal{L}(C)|} cwe_{\mathcal{L}(C)}(T \cdot (x_0, x_1, \ldots, x_k)).$$

MacWilliams relations revisited

For commutative rings $\mathcal{L}(C) = \mathcal{R}(C) = C^{\perp}$.

MacWilliams relations revisited

For commutative rings $\mathcal{L}(C) = \mathcal{R}(C) = C^{\perp}$.

Theorem

Let C be a linear code over a commutaive Frobenius rings R then

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

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 $\Psi_{\mathfrak{a}} : R \to R/\mathfrak{a}$ 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* $x \mapsto (x \pmod{\mathfrak{m}_1^{e_1}}, \dots, x \pmod{\mathfrak{m}_k^{e_k}})$, *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:

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

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.