Interesting alphabets and weights for algebraic coding theory

Steven T. Dougherty

February 24, 2013

Classical Fundamental Question of Coding Theory

Find the largest subset of $\mathbb{F}_2^n$ such that any two vectors are at least distance d apart, where the distance between two vectors is the number of coordinates in which they differ.

Linear Version

Find the largest subspace of $\mathbb{F}_2^n$ such that the minimum weight of any non-zero vector is at least d, where the weight of a vector is the number of non-zero coordinates in that vector.

Linear Version

Find the largest subspace of $\mathbb{F}_2^n$ such that the minimum weight of any non-zero vector is at least d, where the weight of a vector is the number of non-zero coordinates in that vector.

For vectors $\mathbf{v}, \mathbf{w}$, $d(\mathbf{v}, \mathbf{w}) = wt(\mathbf{v} - \mathbf{w})$ hence this is the linear version of the previous question.

Modified Fundamental Question of Coding Theory

Find the largest subset of A^n such that any two vectors are at least distance d apart, where the distance is a metric and A is an algebraic structure.

Basic Definitions

A code C over a ring R of length n is a subset of R^n. It is linear if it is also a submodule.

Basic Definitions

A code C over a ring R of length n is a subset of R^n. It is linear if it is also a submodule.

$$[\mathbf{v}, \mathbf{w}] = \sum \mathbf{v}_i \overline{\mathbf{w}_i}$$

Basic Definitions

A code C over a ring R of length n is a subset of R^n. It is linear if it is also a submodule.

$$[\mathbf{v}, \mathbf{w}] = \sum \mathbf{v}_i \overline{\mathbf{w}_i}$$

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

Basics

- R Frobenius $\Rightarrow |C||C^{\perp}| = |R|^n$.

Basics

- R Frobenius $\Rightarrow |C||C^\perp| = |R|^n$.
- $C \subseteq C^\perp$ – the code is self-orthogonal.

Basics

- R Frobenius $\Rightarrow |C||C^\perp| = |R|^n$.
- $C \subseteq C^\perp$ – the code is self-orthogonal.
- $C = C^\perp$ – the code is self-dual.

Basics

- R Frobenius $\Rightarrow |C||C^{\perp}| = |R|^n$.
- $C \subseteq C^{\perp}$ – the code is self-orthogonal.
- $C = C^{\perp}$ – the code is self-dual.
- $W_C(y) = \sum_{\mathbf{c} \in C} y^{wt(\mathbf{c})}$.

Basics

- R Frobenius $\Rightarrow |C||C^\perp| = |R|^n$.
- $C \subseteq C^\perp$ – the code is self-orthogonal.
- $C = C^\perp$ – the code is self-dual.
- $W_C(y) = \sum_{\mathbf{c} \in C} y^{wt(\mathbf{c})}$.
- $W_C(y) = W_{C^\perp}(y)$ the code is formally self-dual.

Basics

- R Frobenius $\Rightarrow |C||C^\perp| = |R|^n$.
- $C \subseteq C^\perp$ – the code is self-orthogonal.
- $C = C^\perp$ – the code is self-dual.
- $W_C(y) = \sum_{\mathbf{c} \in C} y^{wt(\mathbf{c})}$.
- $W_C(y) = W_{C^\perp}(y)$ the code is formally self-dual.
  Self-dual codes are of particular interest because of their connections to unimodular lattices and invariant theory.

Rings of Order 4

$$\mathbb{Z}_4 = \{0, 1, 2, 3\}$$

Rings of Order 4

$$\mathbb{Z}_4 = \{0, 1, 2, 3\}$$

$$\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$$

Rings of Order 4

$$\mathbb{Z}_4 = \{0, 1, 2, 3\}$$

$$\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$$

$$\mathbb{F}_2 + u\mathbb{F}_2 = \{0, 1, u, 1 + u\}, u^2 = 0$$

Rings of Order 4

$$\mathbb{Z}_4 = \{0, 1, 2, 3\}$$

$$\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$$

$$\mathbb{F}_2 + u\mathbb{F}_2 = \{0, 1, u, 1 + u\}, u^2 = 0$$

$$\mathbb{F}_2 + v\mathbb{F}_2 = \{0, 1, v, 1 + v\}, v^2 = v$$

Rings of Order 4

$\mathbb{Z}_4$ is a chain ring

Rings of Order 4

$\mathbb{Z}_4$ is a chain ring
$\mathbb{F}_4$ is a finite field and so it is within the area of classical coding theory.

Rings of Order 4

$\mathbb{Z}_4$ is a chain ring
$\mathbb{F}_4$ is a finite field and so it is within the area of classical coding theory.
$\mathbb{F}_2 + u\mathbb{F}_2$ is a local ring with maximal ideal $\langle u \rangle$ (it is also a chain ring but its generalization is not).

Rings of Order 4

$\mathbb{Z}_4$ is a chain ring
$\mathbb{F}_4$ is a finite field and so it is within the area of classical coding theory.
$\mathbb{F}_2 + u\mathbb{F}_2$ is a local ring with maximal ideal $\langle u \rangle$ (it is also a chain ring but its generalization is not).
$\mathbb{F}_2 + v\mathbb{F}_2$ is a principal ideal ring isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$

Gray Maps

The following are the distance preserving Gray maps from the rings of order 4 to $\mathbb{F}_2^2$.

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

Generalizations

- $\mathbb{Z}_4$ generalizes to $\mathbb{Z}_{2^k}$, $\mathbb{Z}_{2^k}$ is a chain ring.

Generalizations

- $\mathbb{Z}_4$ generalizes to $\mathbb{Z}_{2^k}$, $\mathbb{Z}_{2^k}$ is a chain ring.
- $\mathbb{F}_4$ generalizes to $\mathbb{F}_{2^s}$, $\mathbb{F}_{2^s}$ is a finite field.

Generalizations

- $\mathbb{Z}_4$ generalizes to $\mathbb{Z}_{2^k}$, $\mathbb{Z}_{2^k}$ is a chain ring.
- $\mathbb{F}_4$ generalizes to $\mathbb{F}_{2^s}$, $\mathbb{F}_{2^s}$ is a finite field.
- $\mathbb{F}_2 + u\mathbb{F}_2$ generalizes to R_k, $R_k = \mathbb{F}_2[u_1, v_2, \dots, u_k]$, $u_i^2 = 0$, which is a local ring.

Generalizations

- $\mathbb{Z}_4$ generalizes to $\mathbb{Z}_{2^k}$, $\mathbb{Z}_{2^k}$ is a chain ring.
- $\mathbb{F}_4$ generalizes to $\mathbb{F}_{2^s}$, $\mathbb{F}_{2^s}$ is a finite field.
- $\mathbb{F}_2 + u\mathbb{F}_2$ generalizes to R_k, $R_k = \mathbb{F}_2[u_1, v_2, \ldots, u_k]$, $u_i^2 = 0$, which is a local ring.
- $\mathbb{F}_2 + v\mathbb{F}_2$ generalizes to A_k, $A_k = \mathbb{F}_2[v_1, v_2, \ldots, v_k]$, $v_i^2 = v_i$, which is isomorphic to $\mathbb{F}_2^k$.

We begin by extending the Gray map (non-linear) to the chain ring $\mathbb{Z}_{2^k}$.

We begin by extending the Gray map (non-linear) to the chain ring $\mathbb{Z}_{2^k}$. Let $\mathbf{1}_i$ denote the all-one vector of length i and let $\mathbf{0}_i$ denote

the all zero vector of length i.

Gray Maps

Then we define the Gray map $\phi : \mathbb{Z}_{2^k} \to \mathbb{Z}_2^{2^{k-1}}$ by

$$\phi(i) = \begin{cases} \mathbf{0}_{2^{k-2}-i}\mathbf{1}_i & 0 \leq i \leq 2^{k-2} \\ \mathbf{1}_{2^{k-1}} + \phi(i - 2^{k-1}) & i > 2^{k-2} \end{cases} .$$

Example

$$\mathbb{Z}_8 \to \mathbb{F}_2^4$$

$$\begin{aligned}
0 &\to 0000\\
1 &\to 0001\\
2 &\to 0011\\
3 &\to 0111\\
4 &\to 1111\\
5 &\to 1110\\
6 &\to 1100\\
7 &\to 1000
\end{aligned}$$

Rank and Kernel

Let C a code over $\mathbb{Z}_{2^k}$. Define the rank of C, denoted $rank(C)$, as the minimum number of generators of the code C, and the kernel of C, denoted $K(C)$, as the set

$$K(C) = \{v | \ v \in C, v + C = C\}.$$

Singleton Bound

If C is a linear code over $\mathbb{Z}_{2^k}$ of length n then

$$\left\lfloor \frac{d_L(C)-1}{2^{k-1}} \right\rfloor \leq n - rank(C). \quad (1)$$

Singleton Bound

If C is a linear code over $\mathbb{Z}_{2^k}$ of length n then

$$\left\lfloor \frac{d_L(C) - 1}{2^{k-1}} \right\rfloor \leq n - rank(C). \tag{1}$$

A code meeting this bound is said to be Maximum Distance with respect to Rank with the Lee weight, or Lee MDR.

Singleton Bound

If C is a linear code over $\mathbb{Z}_{2^k}$ of length n then

$$\left\lfloor \frac{d_L(C) - 1}{2^{k-1}} \right\rfloor \leq n - rank(C). \quad (1)$$

A code meeting this bound is said to be Maximum Distance with respect to Rank with the Lee weight, or Lee MDR.

It is Lee MDS if it meets the stronger bound

$$\left\lfloor \frac{d_L(C) - 1}{2^{k-1}} \right\rfloor \leq n - log_{2^k}|C|. \quad (2)$$

Kernels

Theorem

Let C be a code over $\mathbb{Z}_{2^k}$ of type $\{\delta_0, \delta_1, \dots, \delta_{k-1}\}$. If $m = dim(K(\phi(C)))$, then

$$m \in \left\{ \sum_{i=0}^{k-1} \delta_i, \sum_{i=0}^{k-1} \delta_i + 1, \dots, \sum_{i=0}^{k-1} \delta_i + \delta_{k-2} - 2, \sum_{i=0}^{k-1} \delta_i + \delta_{k-2} \right\}.$$

Moreover, there exist such a code C for any m in the interval.

Linear Image

Theorem

Let C be a code over $\mathbb{Z}_{2^k}$, $k > 2$. Then $\phi(C)$ is linear if and only if C is permutation equivalent to a code with generator matrix of the form

$$\begin{pmatrix} 2^{k-2} I_{\delta_{k-2}} & 2^{k-2} A & 2^{k-2} B \\ \mathbf{0} & 2^{k-1} I_{\delta_{k-1}} & 2^{k-1} T \end{pmatrix}, \qquad (3)$$

where A, B and T are matrices over $\mathbb{Z}_{2^k}$ with all entries in $\{0, 1\} \subset \mathbb{Z}_{2^k}$.

Formally Self-Dual Codes over $\mathbb{Z}_4$

Theorem

Let C be a formally self-dual code over $\mathbb{Z}_4$ with respect to the Lee weight enumerator, then the image of C under the Gray map has the weight enumerator of a formally self-dual code.

Formally Self-Dual Codes over $\mathbb{Z}_4$

Theorem

Let C be a formally self-dual code over $\mathbb{Z}_4$ with respect to the Lee weight enumerator, then the image of C under the Gray map has the weight enumerator of a formally self-dual code.

Often self-dual codes will produce binary self-dual codes but not always.

Examples

Table: Binary Images of Self-dual Codes over $\mathbb{Z}_4$

Code	Length	Binary Image	Orthogonality
$\mathcal{A}_1$	1	$[2,1,2]$ Linear Code	Self-Dual
$\mathcal{D}_4^{\oplus}$	4	$[8,4,4]$ Linear Code	Self-Dual
$\mathcal{D}_6^{\oplus}$	6	$[12,6,4]$ Linear Code	Not Self-Dual
$\mathcal{E}_7^{+}$	7	$(14,2^7,4)$ Non-linear Code	Not Self-Dual
$\mathcal{D}_8^{\oplus}$	8	$[16,8,4]$ Linear Code	Not Self-Dual
$\mathcal{E}_8$	8	$(16,2^8,4)$ Non-linear Code	Not Self-Dual
$\mathcal{K}_8$	8	$[16,8,4]$ Linear Code	Self-Dual
$\mathcal{K}_8'$	8	$[16,8,4]$ Linear Code	Self-Dual
$\mathcal{O}_8$	8	$(16,2^8,4)$ Non-linear Code	Not Self-Dual
$\mathcal{Q}_8$	8	$[16,8,4]$ Linear Code	Not Self-Dual

The ring R_k

$$R_k = \mathbb{F}_2[u_1, u_2, \ldots, u_k]/\langle u_i^2 = 0, u_i u_j = u_j u_i \rangle$$

The ring R_k

$$R_k = \mathbb{F}_2[u_1, u_2, \ldots, u_k]/\langle u_i^2 = 0, u_i u_j = u_j u_i \rangle$$

Theorem

The ring R_k is a local ring with unique maximal ideal $\mathfrak{m}_k = I_{u_1, u_2, \ldots, u_k}$. This ideal consists of all non-units and has $|\mathfrak{m}_k| = \frac{|R_k|}{2}$.

Representation of Elements

Let $u_A = \prod_{1 \in A} u_i$. Any element in R_k can be written as

$$\sum_{A \subseteq \{1,2,\ldots,k\}} c_A u_A, c_A \in \mathbb{F}_2.$$

The ring R_k

The ring R_k has cardinality:

$$|R_k| = 2^{(2^k)}$$

The ring R_k

The ring R_k has cardinality:

$$|R_k| = 2^{(2^k)}$$

The rings is neither principal nor a chain ring for $k \geq 2$, but it is Frobenius.

Gray Map

$$\phi_{R_1}(a + bu_1) = (b, a + b)$$

$$\phi_{R_k}(a + bu_k) = (\phi_{R_{k-1}}(b), \phi_{R_{k-1}}(a) + \phi_{R_{k-1}}(b))$$

Gray Map

$$\phi_{R_1}(a + bu_1) = (b, a + b)$$

$$\phi_{R_k}(a + bu_k) = (\phi_{R_{k-1}}(b), \phi_{R_{k-1}}(a) + \phi_{R_{k-1}}(b))$$

The map is linear.

Alternate Gray Map

View R_k as a vector space over $\mathbb{F}_2$ with basis $\{u_A : A \subseteq \{1, 2, \ldots, k\}\}$.

Alternate Gray Map

View R_k as a vector space over $\mathbb{F}_2$ with basis $\{u_A : A \subseteq \{1, 2, \ldots, k\}\}$.
Define the Gray map of each u_A and then extend it linearly to all of R_k.

Alternate Gray Map

View R_k as a vector space over $\mathbb{F}_2$ with basis $\{u_A : A \subseteq \{1, 2, \ldots, k\}\}$.
Define the Gray map of each u_A and then extend it linearly to all of R_k.
Fix an ordering on the subsets of $\{1, 2, \ldots, k\}$, that will be defined recursively as follows:

$$\{1, 2, \ldots, k\} = \{1, 2, \ldots, k-1\} \cup \{k\}.$$

Alternate Gray Map

View R_k as a vector space over $\mathbb{F}_2$ with basis $\{u_A : A \subseteq \{1, 2, \ldots, k\}\}$.
Define the Gray map of each u_A and then extend it linearly to all of R_k.
Fix an ordering on the subsets of $\{1, 2, \ldots, k\}$, that will be defined recursively as follows:

$$\{1, 2, \ldots, k\} = \{1, 2, \ldots, k-1\} \cup \{k\}.$$

Denote by $\psi_k : R_k \to \mathbb{F}_2^{2^k}$ and define it as follows:

$$\psi_k(u_A) = (c_B)_{B \subseteq \{1,2,\ldots,k\}},$$

where

$$c_B = \begin{cases} 1 & \text{if} B \subseteq A \\ 0 & \text{otherwise.} \end{cases}$$

Alternate Gray Map

It follows immediately that

$$w_L(u_A) = 2^{|A|}. \tag{4}$$

Alternate Gray Map

It follows immediately that

$$w_L(u_A) = 2^{|A|}. \tag{4}$$

The map ψ_k is equivalent to ϕ_k

Gray Image

Theorem

If C is a binary code that is the Gray image of a linear code over R_k then its automorphism group contains k distinct automorphisms which are involutions corresponding to multiplying by the units $1 + u_i$, for $i = 1, 2, \cdots, k$.

Gray Image

Theorem

If C is a binary code that is the Gray image of a linear code over R_k then its automorphism group contains k distinct automorphisms which are involutions corresponding to multiplying by the units $1 + u_i$, for $i = 1, 2, \cdots, k$.

Theorem

If C is a self-dual code over R_k, then $\phi_k(C)$ is a binary self-dual code of length $2^k n$.

Reed Muller Codes

Theorem

The Reed-Muller codes $RM(r, m)$ are the images of linear codes over the ring R_k of length 2^{m-k} under the Gray map ϕ_k for all $m \geq k$ and for all r with $0 \leq r \leq m$.

Lifts

Define $\Pi_{j,k} : R_j \to R_k$ by $\Pi_{j,k}(u_i) = 0$ if $i > k$ and the identity elsewhere. That is $\Pi_{j,k}$ is the projection of R_j to R_k. Note that if $j \leq k$, then $\Pi_{j,k}$ is the identity map on R_j.

Lifts

Define $\Pi_{j,k} : R_j \to R_k$ by $\Pi_{j,k}(u_i) = 0$ if $i > k$ and the identity elsewhere. That is $\Pi_{j,k}$ is the projection of R_j to R_k. Note that if $j \leq k$, then $\Pi_{j,k}$ is the identity map on R_j.

If $C = \Pi_{j,k}(C')$ for some C' and $j \geq k$, then C' is said to be a lift of C.

Lifts and Projections of Self-Dual Codes

Theorem

If C is a self-dual code over R_k then there exists a self-dual code C' over R_j, for $j > k$, with $\Pi_{j,k}(C') = C$.

Self-Dual Codes

Theorem

Self-dual codes over R_k exist for all lengths and for all k.

Self-Dual Codes

Theorem

Self-dual codes over R_k exist for all lengths and for all k.

A self-dual code over R_k is Type II if the Lee weights are all multiples of 4.

Self-Dual Codes

Theorem

Self-dual codes over R_k exist for all lengths and for all k.

A self-dual code over R_k is Type II if the Lee weights are all multiples of 4. A self-dual code over $\mathbb{F}_2$ is Type II if the Hamming weights are all multiples of 4.

Self-Dual Codes

Theorem

Let C be a self-dual code over R_k then $\psi_k(C)$ is a binary self-dual code of length 2^k. If C is a Type II code then $\psi_k(C)$ is Type II and if C is Type I then $\psi_k(C)$ is Type I.

Cyclic Codes

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

Cyclic Codes

A code C is cyclic if $(a_0, a_1, \ldots, a_{n-1}) \in C$ implies $(a_{n-1}, a_0, a_1, \ldots, a_{n-2}) \in C$.
A code C is b-quasi-cyclic if $(a_0, a_1, \ldots, a_{n-1}) \in C$ implies $(a_{0-b}, a_{1-b}, \ldots, a_{n-1-b}) \in C$.

Cyclic Codes

Theorem

Let C be a cyclic code of length n over the ring R_k. Then $\psi_k(C)$ is a 2^k- quasi-cyclic binary linear code of length $2^k n$.

Good Codes

Using cyclic codes and self-dual codes we have found many good binary codes as images under the Gray maps.

The Ring A_k

$$A_k = \mathbb{F}_2[v_1, v_2, \ldots, v_k]/\langle v_i^2 = v_i, v_i v_j = v_j v_i \rangle$$

Gray Maps

$$\phi_{A_1}(a + bv_1) = (a, a + b)$$

$$\phi_{A_k}(a + bu_k) = (\phi_{A_{k-1}}(a), \phi_{A_{k-1}}(a) + \phi_{A_{k-1}}(b))$$

Gray Maps

Order$\mathbb{F}_2^{2^k}$ again.

Gray Maps

Order$\mathbb{F}_2^{2^k}$ again. Let $\Psi_k : A_k \to \mathbb{F}_2^{2^k}$.

Gray Maps

Order$\mathbb{F}_2^{2^k}$ again. Let $\Psi_k : A_k \to \mathbb{F}_2^{2^k}$. Define

$$\Psi_k(v_B) = \sum_{E \subseteq B} w_E \tag{5}$$

where $F \in \mathcal{P}_k$ and

$$(w_E)_F = \begin{cases} 1 & E \subseteq F \\ 0 & \text{otherwise.} \end{cases} \tag{6}$$

Gray Maps

Order$\mathbb{F}_2^{2^k}$ again. Let $\Psi_k : A_k \to \mathbb{F}_2^{2^k}$. Define

$$\Psi_k(v_B) = \sum_{E \subseteq B} w_E \tag{5}$$

where $F \in \mathcal{P}_k$ and

$$(w_E)_F = \begin{cases} 1 & E \subseteq F \\ 0 & \text{otherwise.} \end{cases} \tag{6}$$

Then $\Psi_k(\sum \alpha_B v_B) = \sum \alpha_B \Psi_k(v_B)$.

Gray Maps

The two Gray maps are equivalent.

Inner Products

Over A_k, the Euclidean inner product is:

$$[\mathbf{v}, \mathbf{w}] = \sum \mathbf{v}_i \mathbf{w}_i$$

and the Hermitian is

$$[\mathbf{v}, \mathbf{w}]_H = \sum \mathbf{v}_i \overline{\mathbf{w}_i}$$

where $\overline{v_i} = 1 + v_i$.

Elements of A_k

Each element of A_k is of the form $\sum_{B \in \mathcal{P}_k} \alpha_B v_B$ where $\alpha_B \in \mathbb{F}_2$, and $\mathcal{P}_k$ is the power set of the set $\{1, 2, 3, \ldots, k\}$.

Elements of A_k

Each element of A_k is of the form $\sum_{B \in \mathcal{P}_k} \alpha_B v_B$ where $\alpha_B \in \mathbb{F}_2$, and $\mathcal{P}_k$ is the power set of the set $\{1, 2, 3, \ldots, k\}$.

For $A, B \subseteq \{1, 2, \ldots, k\}$ we have that $v_A v_B = v_{A \cup B}$ which gives that

$$\sum_{B \in \mathcal{P}_k} \alpha_B v_B \cdot \sum_{C \in \mathcal{P}_k} \beta_C v_C = \sum_{D \in \mathcal{P}_k} \Big(\sum_{B \cup C = D} \alpha_B \beta_C \Big) v_D.$$

The Ring A_k

Theorem

The ring A_k has characteristic 2 and cardinality 2^{2^k}. The ring A_k is not a local ring.

Chinese Remainder Theorem

Theorem

The ideal $\langle w_1, w_2, \ldots, w_k \rangle$*, where* $w_i \in \{v_i, 1 + v_i\}$*, is a maximal ideal of cardinality* 2^{2^k-1}*. Denote these maximal ideals by* $\mathfrak{m}_i$*. There are* 2^k *such ideals and* $\mathfrak{m}_i^e = \mathfrak{m}_i$ *for all* i *and* $e \geq 1$*. Hence its index of stability is 1. Moreover the direct sum of any two of these ideals is* A_k*.*

Chinese Remainder Theorem

Theorem

The ideal $\langle w_1, w_2, \ldots, w_k \rangle$*, where* $w_i \in \{v_i, 1 + v_i\}$*, is a maximal ideal of cardinality* $2^{2^k - 1}$*. Denote these maximal ideals by* $\mathfrak{m}_i$*. There are* 2^k *such ideals and* $\mathfrak{m}_i^e = \mathfrak{m}_i$ *for all* i *and* $e \geq 1$*. Hence its index of stability is 1. Moreover the direct sum of any two of these ideals is* A_k*.*

Theorem

The ring A_k *is isomorphic via the Chinese Remainder Theorem to* $\mathbb{F}_2^{2^k}$*. Consequently, the ring* A_k *is a principal ideal ring.*

Euclidean Self-Dual Codes

Theorem

Euclidean self-dual codes exist if and only if the length is congruent to $0 \pmod 2$.

Euclidean Self-Dual Codes

Theorem

Euclidean self-dual codes exist if and only if the length is congruent to $0 \pmod 2$.

Theorem

The image under the Gray map of a Euclidean self-dual code is a binary self-dual code.

Hermitian Self-Dual Codes

Theorem

The code I_{v_i} is a Hermitian self-dual code of length 1.

Hermitian Self-Dual Codes

Theorem

The code I_{v_i} is a Hermitian self-dual code of length 1.

Theorem

Hermitian self-dual codes exist over A_k for all lengths.

Hermitian Self-Dual Codes

Theorem

Let C be a Hermitian self-dual code over A_k, then, with the proper arrangement of indices, C is isomorphic to

$$C_1 \times C_1^{\perp} \times C_2 \times C_2^{\perp} \times \cdots \times C_{2^{k-1}} \times C_{2^{k-1}}^{\perp}$$

where C_i is any binary code.

Hermitian Self-Dual Codes

Theorem

Let C be a Hermitian self-dual code over A_k, then, with the proper arrangement of indices, C is isomorphic to

$$C_1 \times C_1^{\perp} \times C_2 \times C_2^{\perp} \times \cdots \times C_{2^{k-1}} \times C_{2^{k-1}}^{\perp}$$

where C_i is any binary code.

Theorem

Let C be a Hermitian self-dual code over A_k of length n then $\Phi_k(C)$ is a formally self-dual binary code of length $2^k n$.

Cyclic and Quasi-Cyclic Codes

Theorem

The Gray image a cyclic code over A_k of length n is a quasi-cyclic code of index 2^k over $\mathbb{F}_2$ with length $2^k n$.

Cyclic and Quasi-Cyclic Codes

Theorem

The Gray image a cyclic code over A_k of length n is a quasi-cyclic code of index 2^k over $\mathbb{F}_2$ with length $2^k n$.

Theorem

The Gray image of a quasi-cyclic code over A_k of length n with index l is a l quasi-cyclic code of index 2^k over $\mathbb{F}_2$ with length $2^k n$.

Odd formally self-dual codes

- There exist odd formally self-dual codes of all lengths over A_k for all k.

Odd formally self-dual codes

- There exist odd formally self-dual codes of all lengths over A_k for all k.
- Linear odd formally self-dual codes exist over $\mathbb{Z}_4$ and R_k for all lengths greater than 1.

What we have done

- Each of the rings of order 4 has been generalized in a natural way with a corresponding Gray map.

What we have done

- Each of the rings of order 4 has been generalized in a natural way with a corresponding Gray map.
- The standard classes of codes have been examined over these rings and their Gray images examined.

What we have done

- Each of the rings of order 4 has been generalized in a natural way with a corresponding Gray map.
- The standard classes of codes have been examined over these rings and their Gray images examined.
- These rings have been used to produce interesting (good) binary codes.

What we have done

- Each of the rings of order 4 has been generalized in a natural way with a corresponding Gray map.
- The standard classes of codes have been examined over these rings and their Gray images examined.
- These rings have been used to produce interesting (good) binary codes.
- Computationally rich example. If C is a formally self-dual code over $\mathbb{Z}_4, R_k$ or A_k then the image under the corresponding Gray map is a binary formally self-dual code.