Some aspects of codes over rings

Peter J. Cameron

Queen Mary University of London

p.j.cameron@qmul.ac.uk

Galway, July 2009

This is work by two of my students,
Josephine Kusuma and Fatma Al-Kharoosi


26

Summary

- Codes over rings and orthogonal arrays

Summary

- Codes over rings and orthogonal arrays
- $\mathbb{Z}_4$ codes and Gray map images

Summary

- Codes over rings and orthogonal arrays
- $\mathbb{Z}_4$ codes and Gray map images
- $\mathbb{Z}_4$ codes determined by two binary codes

Summary

- Codes over rings and orthogonal arrays
- $\mathbb{Z}_4$ codes and Gray map images
- $\mathbb{Z}_4$ codes determined by two binary codes
- Generalisation to $\mathbb{Z}_{p^n}$

Codes over rings

Rings will always be finite commutative rings with identity.

Codes over rings

Rings will always be finite commutative rings with identity.
A (linear) code of length n over R is a submodule of the free R-module R^n.

Codes over rings

Rings will always be finite commutative rings with identity. A (linear) code of length n over R is a submodule of the free R-module R^n.

We define the (Hamming) metric d_H, the inner product of words, and the dual of a code, over a ring R just as for codes over fields.

Orthogonal arrays

A code C over an alphabet R is an *orthogonal array of strength* t if, given any set of t coordinates $i_1, \ldots, i_t$, and any entries $r_1, \ldots, r_t \in R$, there is a constant number of codewords $c \in C$ such that $c_{i_k} = r_k$ for $k = 1, \ldots, t$.

Orthogonal arrays

A code C over an alphabet R is an *orthogonal array of strength* t if, given any set of t coordinates $i_1, \ldots, i_t$, and any entries $r_1, \ldots, r_t \in R$, there is a constant number of codewords $c \in C$ such that $c_{i_k} = r_k$ for $k = 1, \ldots, t$.
The strength of a code C is the largest t for which C is an orthogonal array of strength t.

A theorem

Theorem

The strength of the linear code C over R is one less than the Hamming weight of the dual code $C^{\perp}$.

A theorem

Theorem

The strength of the linear code C over R is one less than the Hamming weight of the dual code $C^\perp$.

This was proved by Delsarte for codes over fields. The generalisation is not completely straightforward. It depends on the following property of rings (which, here, mean finite commutative rings with identity).

A theorem about rings

Proposition

If I is a proper ideal of the ring R, then the annihilator of R is non-zero.

A theorem about rings

Proposition

If I is a proper ideal of the ring R, then the annihilator of R is non-zero.

This is false without the assumptions on R, of course. It is proved by reducing to the case of local rings, and using the fact that such a ring is equal to its completion.

A theorem about rings

Proposition

If I is a proper ideal of the ring R, then the annihilator of R is non-zero.

This is false without the assumptions on R, of course. It is proved by reducing to the case of local rings, and using the fact that such a ring is equal to its completion.

Now the theorem is the case $n = 1$ of the coding result: a code of length 1 is just an ideal of R and the dual code is its annihilator. The general case is then proved by a careful induction.

A theorem about rings

Proposition

If I is a proper ideal of the ring R, then the annihilator of R is non-zero.

This is false without the assumptions on R, of course. It is proved by reducing to the case of local rings, and using the fact that such a ring is equal to its completion.

Now the theorem is the case $n = 1$ of the coding result: a code of length 1 is just an ideal of R and the dual code is its annihilator. The general case is then proved by a careful induction.
It is not true that $|\mathrm{Ann}(I)| = |R|/|I|$ for any ideal I, and hence not true that $|C^{\perp}| = |R|^n/|C|$ for any code over the ring R.
However this does hold for rings such as the integers mod q for positive integers q, or for finite fields.

The Gray map

The Lee metric d_L on $\mathbb{Z}_4^n$ is defined coordinatewise:

$$d_L(v,w) = \sum_{i=1}^{n} d_L(v_i, w_i),$$

where the Lee metric on $\mathbb{Z}_4$ is given by the rule that $d_L(a,b)$ is the number of steps from a to b when the elements of $\mathbb{Z}_4$ are arranged round a circle.

The Gray map

The Lee metric d_L on $\mathbb{Z}_4^n$ is defined coordinatewise:

$$d_L(v,w) = \sum_{i=1}^{n} d_L(v_i,w_i),$$

where the Lee metric on $\mathbb{Z}_4$ is given by the rule that $d_L(a,b)$ is the number of steps from a to b when the elements of $\mathbb{Z}_4$ are arranged round a circle.

The Gray map γ is a non-linear map from $\mathbb{Z}_4^n$ to $\mathbb{Z}_2^{2n}$, which is an isometry from the Lee metric on $\mathbb{Z}_4^n$ to $\mathbb{Z}_2^{2n}$. It is also defined coordinatewise: on $\mathbb{Z}_4$ we have

$$\gamma(0) = 00, \quad \gamma(1) = 01, \quad \gamma(2) = 11, \quad \gamma(3) = 10.$$

The Gray map

The Lee metric d_L on $\mathbb{Z}_4^n$ is defined coordinatewise:

$$d_L(v,w) = \sum_{i=1}^{n} d_L(v_i,w_i),$$

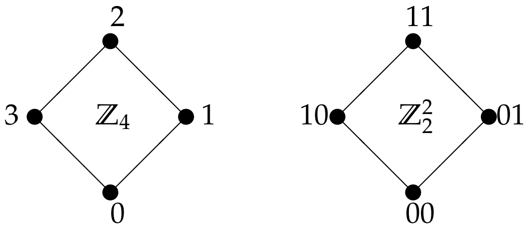
where the Lee metric on $\mathbb{Z}_4$ is given by the rule that $d_L(a,b)$ is the number of steps from a to b when the elements of $\mathbb{Z}_4$ are arranged round a circle.

The Gray map γ is a non-linear map from $\mathbb{Z}_4^n$ to $\mathbb{Z}_2^{2n}$, which is an isometry from the Lee metric on $\mathbb{Z}_4^n$ to $\mathbb{Z}_2^{2n}$. It is also defined coordinatewise: on $\mathbb{Z}_4$ we have

$$\gamma(0) = 00, \quad \gamma(1) = 01, \quad \gamma(2) = 11, \quad \gamma(3) = 10.$$

It was introduced by Hammons *et al.* in their classic paper showing that certain nonlinear binary codes such as the Nordstrom–Robinson, Preparata and Kerdock codes are Gray map images of linear $\mathbb{Z}_4$-codes.

The Gray map



A theorem and a conjecture

Conjecture

Let C be a linear code over $\mathbb{Z}_4$ and C' its Gray map image. Then the strength of C' is one less than the minimum Lee weight of $C^{\perp}$.

Note that the strength of C is one less than the minimum Hamming weight of $C^{\perp}$.

A theorem and a conjecture

Conjecture

Let C be a linear code over $\mathbb{Z}_4$ and C' its Gray map image. Then the strength of C' is one less than the minimum Lee weight of $C^\perp$.

Note that the strength of C is one less than the minimum Hamming weight of $C^\perp$.
Moreover, if C and C' have strength t and t' respectively, then it is known that $t \leq t' \leq 2t + 1$. (This would follow from the truth of the conjecture.)

A theorem and a conjecture

Conjecture

Let C be a linear code over $\mathbb{Z}_4$ and C' its Gray map image. Then the strength of C' is one less than the minimum Lee weight of $C^\perp$.

Note that the strength of C is one less than the minimum Hamming weight of $C^\perp$.
Moreover, if C and C' have strength t and t' respectively, then it is known that $t \leq t' \leq 2t + 1$. (This would follow from the truth of the conjecture.)

Theorem

Let C be a linear code over $\mathbb{Z}_4$ and C' its Gray map image. Then the strength of C' is at most the minimum Lee weight of $C^\perp$ minus one.

A classification of $\mathbb{Z}_4$-codes

With any $\mathbb{Z}_4$-code C, we can associate a pair (C_1, C_2) of binary codes as follows. (This is a special case of a construction due to Eric Lander).

A classification of $\mathbb{Z}_4$-codes

With any $\mathbb{Z}_4$-code C, we can associate a pair (C_1, C_2) of binary codes as follows. (This is a special case of a construction due to Eric Lander).

- C_1 is obtained by reading the entries in words of C mod 2, so that 0 and 2 become 0, 1 and 3 become 1.

A classification of $\mathbb{Z}_4$-codes

With any $\mathbb{Z}_4$-code C, we can associate a pair (C_1, C_2) of binary codes as follows. (This is a special case of a construction due to Eric Lander).

- C_1 is obtained by reading the entries in words of C mod 2, so that 0 and 2 become 0, 1 and 3 become 1.
- C_2 is obtained by considering just those words of C with entries 0 and 2 only, and replacing 0 by 0 and 2 by 1.

A classification of $\mathbb{Z}_4$-codes

With any $\mathbb{Z}_4$-code C, we can associate a pair (C_1, C_2) of binary codes as follows. (This is a special case of a construction due to Eric Lander).

- C_1 is obtained by reading the entries in words of C mod 2, so that 0 and 2 become 0, 1 and 3 become 1.
- C_2 is obtained by considering just those words of C with entries 0 and 2 only, and replacing 0 by 0 and 2 by 1.

Algebraically, there is a homomorphism from C to C_1 with kernel (isomorphic to) C_2; so C is an extension of C_2 by C_1.

A classification of $\mathbb{Z}_4$-codes

With any $\mathbb{Z}_4$-code C, we can associate a pair (C_1, C_2) of binary codes as follows. (This is a special case of a construction due to Eric Lander).

- C_1 is obtained by reading the entries in words of C mod 2, so that 0 and 2 become 0, 1 and 3 become 1.
- C_2 is obtained by considering just those words of C with entries 0 and 2 only, and replacing 0 by 0 and 2 by 1.

Algebraically, there is a homomorphism from C to C_1 with kernel (isomorphic to) C_2; so C is an extension of C_2 by C_1. So you should expect cohomology to come in somewhere …

The class $\mathcal{C}(C_1, C_2)$

We note that $C_1 \leq C_2$. For, given any word $c \in C_1$, let c' be a word in C mapping onto c; then $2c'$ has all entries 0 or 2 and produces the word $c \in C_2$.

The class $\mathcal{C}(C_1, C_2)$

We note that $C_1 \leq C_2$. For, given any word $c \in C_1$, let c' be a word in C mapping onto c; then $2c'$ has all entries 0 or 2 and produces the word $c \in C_2$.
Given binary codes $C_1 \leq C_2$, let $\mathcal{C}(C_1, C_2)$ be the set of all $\mathbb{Z}_4$-codes C corresponding as above to the pair C_1, C_2.

The class $\mathcal{C}(C_1, C_2)$

We note that $C_1 \leq C_2$. For, given any word $c \in C_1$, let c' be a word in C mapping onto c; then $2c'$ has all entries 0 or 2 and produces the word $c \in C_2$.
Given binary codes $C_1 \leq C_2$, let $\mathcal{C}(C_1, C_2)$ be the set of all $\mathbb{Z}_4$-codes C corresponding as above to the pair C_1, C_2.

Proposition

If the length is n, and $\dim(C_i) = k_i$ for $i = 1, 2$, then $|\mathcal{C}(C_1, C_2)| = 2^{k_1(n-k_2)}$.

The class $\mathcal{C}(C_1, C_2)$

We note that $C_1 \leq C_2$. For, given any word $c \in C_1$, let c' be a word in C mapping onto c; then $2c'$ has all entries 0 or 2 and produces the word $c \in C_2$.
Given binary codes $C_1 \leq C_2$, let $\mathcal{C}(C_1, C_2)$ be the set of all $\mathbb{Z}_4$-codes C corresponding as above to the pair C_1, C_2.

Proposition

If the length is n, and $\dim(C_i) = k_i$ for $i = 1, 2$, then $|\mathcal{C}(C_1, C_2)| = 2^{k_1(n-k_2)}$.

Given C_1 and C_2, what can we say about properties of the codes in $\mathcal{C}(C_1, C_2)$?

Generator matrices

The code C has a generator matrix of the form $\begin{pmatrix} I & X & Y \\ O & 2I & 2Z \end{pmatrix}$.

Generator matrices

The code C has a generator matrix of the form $\begin{pmatrix} I & X & Y \\ O & 2I & 2Z \end{pmatrix}$.

The generator matrices of C_1 and C_2 are respectively $\begin{pmatrix} I & X & Y \end{pmatrix}$ and $\begin{pmatrix} I & X & Y \\ O & I & Z \end{pmatrix}$ (where the entries are read mod 2).

Generator matrices

The code C has a generator matrix of the form $\begin{pmatrix} I & X & Y \\ O & 2I & 2Z \end{pmatrix}$.
The generator matrices of C_1 and C_2 are respectively $\begin{pmatrix} I & X & Y \end{pmatrix}$ and $\begin{pmatrix} I & X & Y \\ O & I & Z \end{pmatrix}$ (where the entries are read mod 2).
We can assume that X is a zero-one matrix. Then Y is only determined mod 2 by C_1 and C_2, so the codes in $\mathcal{C}(C_1, C_2)$ are found by adding 0 or 2 to the elements of Y.

Generator matrices

The code C has a generator matrix of the form $\begin{pmatrix} I & X & Y \\ O & 2I & 2Z \end{pmatrix}$.
The generator matrices of C_1 and C_2 are respectively $\begin{pmatrix} I & X & Y \end{pmatrix}$ and $\begin{pmatrix} I & X & Y \\ O & I & Z \end{pmatrix}$ (where the entries are read mod 2).
We can assume that X is a zero-one matrix. Then Y is only determined mod 2 by C_1 and C_2, so the codes in $\mathcal{C}(C_1, C_2)$ are found by adding 0 or 2 to the elements of Y.
Since Y is $k_1 \times (n - k_2)$, where $k_i = \dim(C_i)$, this gives the formula for $|\mathcal{C}(C_1, C_2)|$.

Weight enumerators

The symmetrized weight enumerator of a $\mathbb{Z}_4$-code C is the three-variable homogeneous polynomial

$$\sum_{c \in C} x^{n_0(c)} y^{n_2(c)} z^{n_1(c)+n_3(c)}.$$

Weight enumerators

The symmetrized weight enumerator of a $\mathbb{Z}_4$-code C is the three-variable homogeneous polynomial

$$\sum_{c \in C} x^{n_0(c)} y^{n_2(c)} z^{n_1(c)+n_3(c)}.$$

Apart from renormalisation, we obtain the weight enumerators of C_1 and C_2 by the substitutions $x \to x, y \to x, z \to y$ and $x \to x, y \to y$ and $z \to 0$ respectively.

Weight enumerators

The symmetrized weight enumerator of a $\mathbb{Z}_4$-code C is the three-variable homogeneous polynomial

$$\sum_{c \in C} x^{n_0(c)} y^{n_2(c)} z^{n_1(c)+n_3(c)}.$$

Apart from renormalisation, we obtain the weight enumerators of C_1 and C_2 by the substitutions $x \to x, y \to x, z \to y$ and $x \to x, y \to y$ and $z \to 0$ respectively.
The Lee weight enumerator of C, and hence the weight enumerator of the Gray map image, is obtained by the substitution $x \to x^2, y \to y^2, z \to xy$.

Weight enumerators

The symmetrized weight enumerator of a $\mathbb{Z}_4$-code C is the three-variable homogeneous polynomial

$$\sum_{c \in C} x^{n_0(c)} y^{n_2(c)} z^{n_1(c)+n_3(c)}.$$

Apart from renormalisation, we obtain the weight enumerators of C_1 and C_2 by the substitutions $x \to x, y \to x, z \to y$ and $x \to x, y \to y$ and $z \to 0$ respectively.
The Lee weight enumerator of C, and hence the weight enumerator of the Gray map image, is obtained by the substitution $x \to x^2, y \to y^2, z \to xy$.

Theorem

The average of the symmetrized weight enumerators of the codes in $\mathcal{C}(C_1, C_2)$ *is*

$$\frac{|C_2|}{2^n} \left(W_{C_1}(x+y, 2z) - (x+y)^n \right) + W_{C_2}(x, y).$$

Weight enumerators, continued

Carrie Rutherford and I are currently trying to obtain further global information about this; in particular, the "variance" of the weight enumerators of codes in $\mathcal{C}(C_1, C_2)$.

Weight enumerators, continued

Carrie Rutherford and I are currently trying to obtain further global information about this; in particular, the “variance” of the weight enumerators of codes in $\mathcal{C}(C_1, C_2)$.

Fatma Al-Kharoosi examined this situation locally, and showed that there are only a limited number of possibilities for the way that the s.w.e. changes in moving from one code in the class to a neighbouring one.

Weight enumerators, continued

Carrie Rutherford and I are currently trying to obtain further global information about this; in particular, the “variance” of the weight enumerators of codes in $\mathcal{C}(C_1, C_2)$.

Fatma Al-Kharoosi examined this situation locally, and showed that there are only a limited number of possibilities for the way that the s.w.e. changes in moving from one code in the class to a neighbouring one.
A detailed example is given later.

$\mathcal{C}(C_1, C_2)$ as an affine space

The fact that $|\mathcal{C}(C_1, C_2)|$ is a power of 2 is not a coincidence: the group $C_1^* \otimes (\mathbb{Z}_2^n / C_2)$ acts on this set by translation. (C_1^* is the dual space of C_1.)

$\mathcal{C}(C_1, C_2)$ as an affine space

The fact that $|\mathcal{C}(C_1, C_2)|$ is a power of 2 is not a coincidence: the group $C_1^* \otimes (\mathbb{Z}_2^n / C_2)$ acts on this set by translation. (C_1^* is the dual space of C_1.)
For $C_1^* \otimes \mathbb{Z}_2^n$ acts on $\mathcal{C}$ by the rule

$$(f \otimes w)(c) = c + d(f(c \bmod 2))w$$

where d is the "doubling" map $0 \to 0, 1 \to 2$ from $\mathbb{Z}_2$ to $\mathbb{Z}_4$, and the kernel of the action is $C_1^* \otimes C_2$.

$\mathcal{C}(C_1, C_2)$ as an affine space

The fact that $|\mathcal{C}(C_1, C_2)|$ is a power of 2 is not a coincidence: the group $C_1^* \otimes (\mathbb{Z}_2^n / C_2)$ acts on this set by translation. (C_1^* is the dual space of C_1.)
For $C_1^* \otimes \mathbb{Z}_2^n$ acts on $\mathcal{C}$ by the rule

$$(f \otimes w)(c) = c + d(f(c \bmod 2))w$$

where d is the "doubling" map $0 \to 0, 1 \to 2$ from $\mathbb{Z}_2$ to $\mathbb{Z}_4$, and the kernel of the action is $C_1^* \otimes C_2$.
So if we fix a reference code in $\mathcal{C}$ to act as origin, there is a bijection between $\mathcal{C}$ and $C_1^* \otimes (\mathbb{Z}_2^n / C_2)$.

Another group action

It is clear that $\mathcal{C}$ is invariant under $\mathrm{Aut}(C_1) \cap \mathrm{Aut}(C_2)$, the common automorphisms of C_1 and C_2.

Another group action

It is clear that $\mathcal{C}$ is invariant under $\mathrm{Aut}(C_1) \cap \mathrm{Aut}(C_2)$, the common automorphisms of C_1 and C_2.
Also, 3 is a unit in $\mathbb{Z}_4$, so multiplying any set of coordinate by 3 maps each code in $\mathcal{C}$ to another with the same symmetrized weight enumerator.

Another group action

It is clear that $\mathcal{C}$ is invariant under $\mathrm{Aut}(C_1) \cap \mathrm{Aut}(C_2)$, the common automorphisms of C_1 and C_2.
Also, 3 is a unit in $\mathbb{Z}_4$, so multiplying any set of coordinate by 3 maps each code in $\mathcal{C}$ to another with the same symmetrized weight enumerator.
Multiplying all coordinates by 3 fixes all the codes, so the group $\mathbb{Z}_2^{n-1}$ acts.

Another group action

It is clear that $\mathcal{C}$ is invariant under $\mathrm{Aut}(C_1) \cap \mathrm{Aut}(C_2)$, the common automorphisms of C_1 and C_2.
Also, 3 is a unit in $\mathbb{Z}_4$, so multiplying any set of coordinate by 3 maps each code in $\mathcal{C}$ to another with the same symmetrized weight enumerator.
Multiplying all coordinates by 3 fixes all the codes, so the group $\mathbb{Z}_2^{n-1}$ acts.
These two groups generate their semidirect product $(\mathbb{Z}_2^{n-1}) : (\mathrm{Aut}(C_1) \cap \mathrm{Aut}(C_2))$.

First cohomology

Let A be an abelian group, and G a group acting on A.

First cohomology

Let A be an abelian group, and G a group acting on A.
A derivation is a map $d : G \longrightarrow A$ satisfying $d(g_1 g_2) = d(g_1)^{g_2} + d(g_2)$. It is inner if there is an element $a \in A$ such that $d(g) = a^g - a$.

First cohomology

Let A be an abelian group, and G a group acting on A.
A derivation is a map $d : G \to A$ satisfying $d(g_1 g_2) = d(g_1)^{g_2} + d(g_2)$. It is inner if there is an element $a \in A$ such that $d(g) = a^g - a$.
The derivations modulo inner derivations form a group, the first cohomology group $H^1(G, A)$, whose elements correspond bijectively to the conjugacy classes of complements of the normal subgroup A in the semidirect product $A : G$.

First cohomology

Let A be an abelian group, and G a group acting on A.
A derivation is a map $d : G \to A$ satisfying $d(g_1g_2) = d(g_1)^{g_2} + d(g_2)$. It is inner if there is an element $a \in A$ such that $d(g) = a^g - a$.
The derivations modulo inner derivations form a group, the first cohomology group $H^1(G, A)$, whose elements correspond bijectively to the conjugacy classes of complements of the normal subgroup A in the semidirect product $A : G$.
If A is a vector space and G a linear group, then $A : G$ is a group of affine transformations of A; the stabilizer of the zero vector is a complement, and a complement is conjugate to G if and only if it fixes a vector.

A case study

A very interesting case is that in which $C_1 = C_2$ is the extended Hamming code of length 8. The class $\mathcal{C}(C_1, C_2)$ includes the "octacode" whose Gray map image is the non-linear Nordstrom–Robinson code of length 16.

A case study

A very interesting case is that in which $C_1 = C_2$ is the extended Hamming code of length 8. The class $\mathcal{C}(C_1, C_2)$ includes the "octacode" whose Gray map image is the non-linear Nordstrom–Robinson code of length 16.
The class $\mathcal{C}$ in this case admits the group $G = (\mathbb{Z}_2^7) : \mathrm{AGL}(3, 2)$ (the first factor corresponds to coordinate sign changes, the second is the common automorphism group of C_1 and C_2).

A case study

A very interesting case is that in which $C_1 = C_2$ is the extended Hamming code of length 8. The class $\mathcal{C}(C_1, C_2)$ includes the "octacode" whose Gray map image is the non-linear Nordstrom–Robinson code of length 16.
The class $\mathcal{C}$ in this case admits the group $G = (\mathbb{Z}_2^7) : \mathrm{AGL}(3, 2)$ (the first factor corresponds to coordinate sign changes, the second is the common automorphism group of C_1 and C_2).
The cohomology group $H^1(G, W)$ is non-zero, and indeed the class $\mathcal{C}$ realises an outer derivation.

A case study, continued

The table gives the orbit lengths of G on $\mathcal{C}$, the symmetrized weight enumerator of a code in each orbit, and the number of orbits of the subgroup $\mathrm{AGL}(3,2)$ (the automorphism group of the extended Hamming code). Here

$$F(x,y,z) = x^8 + 14x^4y^4 + y^8 + 16z^8 + 112xyz^4(x^2+y^2)$$

is the weight enumerator of the octacode, and

$$E(x,y,z) = 4z^4(x-y)^4.$$

The data

Orbit	SWE	#perm orbits
7168	F+5E	19
896	F+6E	7
21504	F+4E	24
21504	F+3E	27
3584	F+4E	14
896	F+4E	4
7168	F+2E	8
2688	F+2E	8
128	F	3

The data

Orbit	SWE	#perm orbits
7168	F+5E	19
896	F+6E	7
21504	F+4E	24
21504	F+3E	27
3584	F+4E	14
896	F+4E	4
7168	F+2E	8
2688	F+2E	8
128	F	3

The orbit of size 128 consists of octacodes.

The data

Orbit	SWE	#perm orbits
7168	F+5E	19
896	F+6E	7
21504	F+4E	24
21504	F+3E	27
3584	F+4E	14
896	F+4E	4
7168	F+2E	8
2688	F+2E	8
128	F	3

The orbit of size 128 consists of octacodes.

The average SWE is $F + \frac{7}{2}E$, in agreement with Theorem 6.

Problems

- In the example, the symmetrized weight enumerators of the codes in $\mathcal{C}(C_1, C_2)$ lie on a line in the space of polynomials. In general, Fatma's work shows that they always lie on a relatively low-dimensional space. Can one calculate this dimension, in terms of C_1 and C_2?

Problems

- In the example, the symmetrized weight enumerators of the codes in $\mathcal{C}(C_1, C_2)$ lie on a line in the space of polynomials. In general, Fatma's work shows that they always lie on a relatively low-dimensional space. Can one calculate this dimension, in terms of C_1 and C_2?
- Can one give lower bounds for the number of different SWEs that occur?

Problems

- In the example, the symmetrized weight enumerators of the codes in $\mathcal{C}(C_1, C_2)$ lie on a line in the space of polynomials. In general, Fatma's work shows that they always lie on a relatively low-dimensional space. Can one calculate this dimension, in terms of C_1 and C_2?
- Can one give lower bounds for the number of different SWEs that occur?
- Can one give necessary and sufficient conditions for the element of $H^1(\mathbb{Z}_2^{n-1} : \mathrm{Aut}(C_1) \cap \mathrm{Aut}(C_2), C_1^* \otimes (\mathbb{Z}_2^n / C_2))$ to be non-zero?

Problems

- In the example, the symmetrized weight enumerators of the codes in $\mathcal{C}(C_1, C_2)$ lie on a line in the space of polynomials. In general, Fatma's work shows that they always lie on a relatively low-dimensional space. Can one calculate this dimension, in terms of C_1 and C_2?
- Can one give lower bounds for the number of different SWEs that occur?
- Can one give necessary and sufficient conditions for the element of $H^1(\mathbb{Z}_2^{n-1} : \mathrm{Aut}(C_1) \cap \mathrm{Aut}(C_2), C_1^* \otimes (\mathbb{Z}_2^n / C_2))$ to be non-zero?
- Can one calculate the number of orbits of $\mathbb{Z}_2^{n-1} : \mathrm{Aut}(C_1) \cap \mathrm{Aut}(C_2)$ on $\mathcal{C}(C_1, C_2)$? (This number is not greater than the number of orbits on $C_1^* \otimes (\mathbb{Z}_2^n / C_2)$, and is equal if the cohomology element is zero.)

More generally ...

Following Eric Lander's method, we can associate a chain of r codes over $\mathbb{Z}_p$ with any code over $\mathbb{Z}_{p^r}$. The ith code consists of words of C with all entries divisible by p^{i-1}, read modulo p^i and then "divided" by p^{i-1} to give a $\mathbb{Z}_p$-code.

More generally . . .

Following Eric Lander's method, we can associate a chain of r codes over $\mathbb{Z}_p$ with any code over $\mathbb{Z}_{p^r}$. The ith code consists of words of C with all entries divisible by p^{i-1}, read modulo p^i and then "divided" by p^{i-1} to give a $\mathbb{Z}_p$-code.
One can ask the inverse question: Given a chain of $\mathbb{Z}_p$-codes, how many $\mathbb{Z}_{p^r}$ codes give rise to this chain, and what can be said about their properties?

More generally ...

Following Eric Lander's method, we can associate a chain of r codes over $\mathbb{Z}_p$ with any code over $\mathbb{Z}_{p^r}$. The ith code consists of words of C with all entries divisible by p^{i-1}, read modulo p^i and then "divided" by p^{i-1} to give a $\mathbb{Z}_p$-code.

One can ask the inverse question: Given a chain of $\mathbb{Z}_p$-codes, how many $\mathbb{Z}_{p^r}$ codes give rise to this chain, and what can be said about their properties?

Almost nothing is known about this!

… for your attention!