Open Questions in Coding Theory

Steven T. Dougherty

July 4, 2013

Open Questions

The following questions were posed by:

S.T. Dougherty
J.L. Kim
P. Solé
J. Wood

Hilbert Style Problems

Fundamental Problem of Coding Theory

Open Question

For a fixed n and d, find largest M such that there exists a code $C \subset \mathbb{F}_q^n$ with $|C| = M$.

Fundamental Problem of Coding Theory (Linear Version)

Open Question

For a fixed n and d, find largest k such that there exists a linear code $C \subseteq \mathbb{F}_q^n$ with $dim(C) = k$.

Quote

Filling in a box for the best code with given parameters is just a game. – Felix Ulmer, Lens 2009.

Fundamental Problem of Coding Theory

In general, we want an algorithm (computable) that will give us the answer.

Fundamental question in its most general form

Open Question

Given an alphabet A and a metric D, fix n and d. Find the largest M such that there exists a code $C \subseteq A^n$, with minimum distance d, and $M = |C|$.

Fundamental question in its most general form

Example 1: What is the best $\mathbb{Z}_4$ code with respect to the Lee weight.

Fundamental question in its most general form

Example 1: What is the best $\mathbb{Z}_4$ code with respect to the Lee weight.

Example 2: What is the best $Mat_{n,s}(R)$ code with respect to the Rosenbloom-Tsfasman metric?

Fundamental question in its most general form

Example 1: What is the best $\mathbb{Z}_4$ code with respect to the Lee weight.

Example 2: What is the best $Mat_{n,s}(R)$ code with respect to the Rosenbloom-Tsfasman metric?

Example 3: What is the best code over a chain ring with respect to the homogeneous weight?

Fundamental question in its most general form

Example 1: What is the best $\mathbb{Z}_4$ code with respect to the Lee weight.

Example 2: What is the best $Mat_{n,s}(R)$ code with respect to the Rosenbloom-Tsfasman metric?

Example 3: What is the best code over a chain ring with respect to the homogeneous weight?

Example 4: What is the best additive code over $\mathbb{F}_4$? These codes are useful in terms of quantum communication.

Duality for Abelian groups

Note a character of G is a homomorphism from G to the multiplicative group of the Complex numbers.

Duality for Abelian groups

Note a character of G is a homomorphism from G to the multiplicative group of the Complex numbers.

Let G be a finite abelian group and fix a duality of G, i.e. a character table. We have a bijective correspondence between the elements of G and those of $\widehat{G} = \{\pi | \pi \text{ a character of } G\}$.

Duality for Abelian groups

Note a character of G is a homomorphism from G to the multiplicative group of the Complex numbers.

Let G be a finite abelian group and fix a duality of G, i.e. a character table. We have a bijective correspondence between the elements of G and those of $\widehat{G} = \{\pi | \pi \text{ a character of } G\}$.

For each $\alpha \in G$ denote the corresponding character by χ_α.

Duality for Abelian groups

A code C over G is a subset of G^n, the code is said to be linear if C is an additive subset of G^n.

Duality for Abelian groups

A code C over G is a subset of G^n, the code is said to be linear if C is an additive subset of G^n.

For C a code in over G, $C^\perp = \{(g_1, g_2, \dots, g_n) | \prod_{i=1}^{i=n} \chi_{g_i}(c_i) = 1$ for all $(c_1, \dots, c_n) \in C\}$.

Duality for Abelian groups

A code C over G is a subset of G^n, the code is said to be linear if C is an additive subset of G^n.

For C a code in over G, $C^\perp = \{(g_1, g_2, \ldots, g_n) | \prod_{i=1}^{i=n} \chi_{g_i}(c_i) = 1$ for all $(c_1, \ldots, c_n) \in C\}$.

We associate an element of $\widehat{G}^n$ with an element of G^n with the natural correspondence.

Duality for Abelian groups

A code C over G is a subset of G^n, the code is said to be linear if C is an additive subset of G^n.

For C a code in over G, $C^\perp = \{(g_1, g_2, \ldots, g_n) | \prod_{i=1}^{i=n} \chi_{g_i}(c_i) = 1$ for all $(c_1, \ldots, c_n) \in C\}$.

We associate an element of $\widehat{G}^n$ with an element of G^n with the natural correspondence.

The code $C^\perp$ is associated with the set $\{\chi \in \widehat{G^n} | \chi(c) = 1 \text{ for all } c \in C\}$.

Duality for Abelian groups

A code C over G is a subset of G^n, the code is said to be linear if C is an additive subset of G^n.

For C a code in over G, $C^\perp = \{(g_1, g_2, \ldots, g_n) | \prod_{i=1}^{i=n} \chi_{g_i}(c_i) = 1$ for all $(c_1, \ldots, c_n) \in C\}$.

We associate an element of $\widehat{G}^n$ with an element of G^n with the natural correspondence.

The code $C^\perp$ is associated with the set $\{\chi \in \widehat{G^n} | \chi(c) = 1 \text{ for all } c \in C\}$.

This gives that $|C^\perp| = \frac{|\widehat{G}|^n}{|C|} = \frac{|G|^n}{|C|}$ and that $C = (C^\perp)^\perp$.

Duality for Abelian groups

Let $G = \{\alpha_i\}$ with α_0 the additive identity of the group.

The **complete weight enumerator** of a code C over a G is given by

$$W_C(x_0, x_1, \ldots, x_{s-1}) = \sum_{c \in C} wt(c)$$

where $wt(c) = \prod_{i=0}^{s-1} x_i^{\beta_i}$ where the element α_i appears β_i times in the vector c.

Duality for Abelian groups

Let T be defined as follows:

$$T_{\alpha_i,\alpha_j} = \chi_{\alpha_i}(\alpha_j)$$

Duality for Abelian groups

Let T be defined as follows:

$$T_{\alpha_i,\alpha_j} = \chi_{\alpha_i}(\alpha_j)$$

Theorem

Let C be a code over G, $|G| = s$, with weight enumerator $W_C(x_0, x_1, \ldots, x_{s-1})$ then the complete weight enumerator of the orthogonal is given by:

$$W_{C^\perp} = \frac{1}{|C|} W_C(T(x_0, x_1, \ldots, x_{s-1}))$$

and

$$H_{C^\perp} = \frac{1}{|C|} H_C(x + (s-1)y, x - y)$$

Duality for non-Abelian groups

This approach does not work for non-Abelian groups.

Duality for non-Abelian groups

This approach does not work for non-Abelian groups.

Open Question

Is there a duality and MacWilliams formula for codes over non-Abelian groups? Is there a subclass of non-Abelian groups for which a duality and a MacWilliams formula exists?

Difficulties for non-Abelian groups

Consider the non-Abelian Quaternion group of order 8. This group has elements $\{\pm 1, \pm i, \pm j, \pm k\}$.

Difficulties for non-Abelian groups

Consider the non-Abelian Quaternion group of order 8. This group has elements $\{\pm 1, \pm i, \pm j, \pm k\}$.

There are three subgroups of order 4 in this group, that is $\{\pm 1, \pm i\}$, $\{\pm 1, \pm j\}\{\pm 1, \pm k\}$. But there is only one group of order 2, that is $\{\pm 1\}$.

Difficulties for non-Abelian groups

Consider the non-Abelian Quaternion group of order 8. This group has elements $\{\pm 1, \pm i, \pm j, \pm k\}$.

There are three subgroups of order 4 in this group, that is $\{\pm 1, \pm i\}$, $\{\pm 1, \pm j\}\{\pm 1, \pm k\}$. But there is only one group of order 2, that is $\{\pm 1\}$.

If a linear code is defined as a subgroup (or even normal subgroup) of G^n then these are all linear codes. If we expect that $|C||C^\perp| = |G|^n$, then each subgroup of order 4 would need a subgroup of order 2 to be its orthogonal and the subgroup of order 2 would need a subgroup of order 4 to be its orthogonal. This would not be possible here, in other words we could not have $(C^\perp)^\perp = C$ in this scenario.

Duality for non-Abelian groups

Open Question

Is there a subclass of non-abelian groups for which a duality and a MacWilliams relations work?

General Duality Question

Open Question

What is the largest class of algebraic objects for which there exists a duality and a MacWilliams relation?

General Duality Question

Open Question

What is the largest class of algebraic objects for which there exists a duality and a MacWilliams relation?

For example, for rings the answer is Frobenius rings.

General Duality Question

Along with this question comes the question of what exactly should we call a linear code.

General Duality Question

Along with this question comes the question of what exactly should we call a linear code.

Open Question

Define linear codes when the alphabet is neither a ring, module nor an abelian group.

Designs and Codes

A block $t-(v,k,\lambda)$ design is an incidence structure of points and blocks such that the following hold:
1. There are v points,
2. Each block contains k points,
3. For any t points there are exactly λ blocks that contain all these points.

The Assmus-Mattson Theorem

Theorem

Assmus-Mattson Theorem *Let C be a code over $\mathbb{F}_q$ of length n with minimum weight d, and let $d^\perp$ denote the minimum weight of $C^\perp$. Let $w = n$ when $q = 2$ and otherwise the largest integer w satisfying $w - (\frac{w+q-2}{q-1}) < d$, define $w^\perp$ similarly. Suppose there is an integer t with $0 < t < d$ that satisfies the following condition: for $W_{C^\perp}(Z) = B_i Z^i$ at most $d - t$ of $B_1, B_2, \ldots, B_{n-t}$ are non-zero. Then for each i with $d \leq i \leq w$ the supports of the vectors of weight i of C, provided there are any, yield a t-design. Similarly, for each j with $d^\perp \leq j \leq min\{w^\perp, n - t\}$ the supports of the vectors of weight j in $C^\perp$, provided there are any, form a t-design.*

The Assmus-Mattson Theorem

Theorem

Assmus-Mattson Theorem *Let C be a code over $\mathbb{F}_q$ of length n with minimum weight d, and let $d^\perp$ denote the minimum weight of $C^\perp$. Let $w = n$ when $q = 2$ and otherwise the largest integer w satisfying $w - (\frac{w+q-2}{q-1}) < d$, define $w^\perp$ similarly. Suppose there is an integer t with $0 < t < d$ that satisfies the following condition: for $W_{C^\perp}(Z) = B_i Z^i$ at most $d - t$ of $B_1, B_2, \ldots, B_{n-t}$ are non-zero. Then for each i with $d \leq i \leq w$ the supports of the vectors of weight i of C, provided there are any, yield a t-design. Similarly, for each j with $d^\perp \leq j \leq min\{w^\perp, n - t\}$ the supports of the vectors of weight j in $C^\perp$, provided there are any, form a t-design.*

One of the most fruitful uses of this theorem is to find 5-designs in the extremal Type II codes of length 24 and 48. There would also be 5-designs in the putative $[24k, 12k, 4k + 4]$ codes.

Assmus-Mattson Theorem limit

Open Question

Find a theoretical limit for t such that the exists t-designs via the Assmus-Mattson theorem applied to a linear code, or prove that no such limit exists by finding codes with t-designs for arbitrary t.

Assmus-Mattson Theorem limit

Open Question

Find a theoretical limit for t such that the exists t-designs via the Assmus-Mattson theorem applied to a linear code, or prove that no such limit exists by finding codes with t-designs for arbitrary t.

Toward this very large question it would be interesting to solve the following.

Open Question

Find 5*-designs that are not in* $[24k, 12k, 4k + 4]$ *codes Type II codes or any* 6*-designs in codes.*

Assmus Mattson Theorem limit

In 2000 Janusz showed the following.

Theorem

Let C be a $[24m + 8\mu, 12m + 4\mu, 4m + 4]$ extremal Type II code for $\mu = 0, 1$, or 2, where $m \geq 1$ if $\mu = 0$, and $\mu \geq 0$ otherwise. Then only one of the following holds:

(a) *the codewords of any fixed weight $i \neq 0$ hold t*-designs for $t = 7 - 2\mu$, *or*

(b) *the codewords of any fixed weight $i \neq 0$ hold t*-designs for $t = 5 - 2\mu$ *and there is no i with $0 < i < 24m + 8\mu$ such that codewords of weight i hold a* $(6 - 2\mu)$-design.

MDS Codes

The Singleton Bound is as follows.

Theorem

Let C be a code over an alphabet A with length n, minimimum distance d and size $k = log_{|A|}(C)$. Then $d \leq n - k + 1$.

MDS Codes

The Singleton Bound is as follows.

Theorem

Let C be a code over an alphabet A with length n, minimimum distance d and size $k = log_{|A|}(C)$. Then $d \leq n - k + 1$.

Codes meeting this bound are called MDS codes. Finding such codes is largely a combinatorial problem.

MDS Codes

This combinatorial bound is equivalent to a number of interesting combinatorial questions involving mutually orthogonal Latin squares (and hypercubes) and arcs of maximal size in projective geometry.

Theorem

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

MDS Codes

This combinatorial bound is equivalent to a number of interesting combinatorial questions involving mutually orthogonal Latin squares (and hypercubes) and arcs of maximal size in projective geometry.

Theorem

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

The search for mutually orthogonal squares has been suggested as the next Fermat question, owing to its ease of statement and its intractability over centuries.

MDS Codes

There is a corresponding bound for codes over a principal ideal ring.

Theorem

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

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

where k is the rank of the code.

MDS Codes

There is a corresponding bound for codes over a principal ideal ring.

Theorem

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

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

where k is the rank of the code.

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

MDS and MDR Codes

Open Question

Find and classify all MDS and MDR codes.

MDS and MDR Codes

Open Question

Find and classify all MDS and MDR codes.

Open Question

Prove or disprove that if C is an $[n, k, n-k+1]$ MDS code over $\mathbb{F}_p$ then $n \leq p+1$.

Gleason-Pierce-Ward

Theorem

(**Gleason-Pierce-Ward**) *Let p be a prime, m, n be integers and $q = p^m$. Suppose C is a linear $[n, \frac{n}{2}]$ divisible code over $\mathbb{F}_q$ with divisor $\Delta > 1$. Then one (or more) of the following holds:*
I. $q = 2$ and $\Delta = 2$,
II. $q = 2$, $\Delta = 4$, and C is self-dual,
III. $q = 3$, $\Delta = 3$, and C is self-dual,
IV. $q = 4$, $\Delta = 2$, and C is Hermitian self-dual,
V. $\Delta = 2$ and C is equivalent to the code over $\mathbb{F}_q$ with generator matrix $[I_{\frac{n}{2}} I_{\frac{n}{2}}]$, where $I_{\frac{n}{2}}$ is the identity matrix of size $\frac{n}{2}$ over $\mathbb{F}_q$.

Generalization of Gleason-Pierce-Ward

Theorem

Suppose that C is a self-dual code over $\mathbb{Z}_{2k}$ which has the property that every Euclidean weight is a multiple of a positive integer. Then the largest positive integer c is either $2k$ or $4k$.

Generalization of Gleason-Pierce-Ward

Open Question

Find the largest class of codes over algebraic structures for which there exists such a divisibility condition for self-dual code for a given weight.

Generalization of Gleason, Nebe-Rains-Sloane

Self-Dual Codes and Invariant Theory G. Nebe, E. M. Rains and N. J. A. Sloane Springer-Verlag, 2006, xxvii+430 pp. ISBN 3-540-30729-x

Generalization of Gleason, Nebe-Rains-Sloane

Open Question

(Suggested By Jay Wood) Find the largest class of codes for which a generalization of these theorems exist.

Non-existence

Open Question

Develop tools for proving the non-existence of codes for a given set of parameters.

Non-existence

Open Question

Develop tools for proving the non-existence of codes for a given set of parameters.

Numerous constructions exist for codes, but in comparison we have relatively few techniques for proving that codes do not exist.

Non-existence

Open Question

Develop tools for proving the non-existence of codes for a given set of parameters.

Numerous constructions exist for codes, but in comparison we have relatively few techniques for proving that codes do not exist.

Recall that the non-existence of the projective plane of order 10 was proven by showing that a certain code did not exist.

Self-dual codes

Numerous papers have been written trying to find optimal self-dual codes for a given length using many different constructions and techniques.

Self-dual codes

Numerous papers have been written trying to find optimal self-dual codes for a given length using many different constructions and techniques.

As of now, we still do not know the complete answer for lengths under 100.

Self-dual codes

Numerous papers have been written trying to find optimal self-dual codes for a given length using many different constructions and techniques.

As of now, we still do not know the complete answer for lengths under 100.

Open Question

Determine an algorithm (or theorem) for efficiently determining the parameters of an optimal self-dual code (over a ring or field).

Open Questions for Ring Theorists

Cyclic Codes

We know that in general, we associate cyclic codes (which are useful both in theory and practice) with ideals in $R[x]/\langle x^n - 1\rangle$.

Cyclic Codes

We know that in general, we associate cyclic codes (which are useful both in theory and practice) with ideals in $R[x]/\langle x^n - 1\rangle$.

Open Question

Classify all ideals in $R[x]/\langle x^n - 1\rangle$, where R is a Frobenius ring and n is any integer.

Cyclic Codes

We know that in general, we associate cyclic codes (which are useful both in theory and practice) with ideals in $R[x]/\langle x^n - 1\rangle$.

Open Question

Classify all ideals in $R[x]/\langle x^n - 1\rangle$, where R is a Frobenius ring and n is any integer.

Numerous cases are known, however, even for $\mathbb{Z}_m$ with n not relatively prime to m, there is a lot to be studied.

Skew Cyclic Codes

Open Question

Give the most general setting for skew cyclic codes, that is give a description of an algebraic setting and a determination of the ideals in that setting where the alphabet and automorphism are as general as possible.

Skew Cyclic Codes

Open Question

Give the most general setting for skew cyclic codes, that is give a description of an algebraic setting and a determination of the ideals in that setting where the alphabet and automorphism are as general as possible.

Of course, there are numerous steps that can be done on the path of this problem.

Skew Cyclic Codes

One might even generalize this to where the permutation acting is not simply the cyclic permutations.

Skew Cyclic Codes

One might even generalize this to where the permutation acting is not simply the cyclic permutations.

Open Question

Give an algebraic description of all skew codes that are held invariant by some finite group of permutations G.

Non-Commutative Rings

While a great deal has been done where the alphabet is a commutative ring, very little has been done where the alphabet is a non-commutative ring.

Non-Commutative Rings

While a great deal has been done where the alphabet is a commutative ring, very little has been done where the alphabet is a non-commutative ring.

Open Question

Develop the theory for any family of codes where the alphabet is a non-commutative ring.

Non-Commutative Rings

Open Question

Find connections for codes over rings (commutative and non-commutative) to other branches of mathematics (combinatorics, number theory, design theory).

Non-Commutative Rings

Open Question

Find connections for codes over rings (commutative and non-commutative) to other branches of mathematics (combinatorics, number theory, design theory).

Open Question

Find connections for codes over rings (commutative and non-commutative) to engineering applications.

Fermat Style Problems

My favorite open problem

Open Question

Does there exist a Type II $[72, 36, 16]$ *code?*

My favorite open problem

Monetary prizes:

- N.J.A. Sloane \$10 (1973),
- S.T. Dougherty \$100 for the existence (2000),
- M. Harada \$200 for the nonexistence (2000).

The putative $[72, 36, 16]$ code

If C is a self-dual code then the weight enumerator is held invariant by the MacWilliams relations and hence by the following matrix:

$$M = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

The putative $[72, 36, 16]$ code

If C is a self-dual code then the weight enumerator is held invariant by the MacWilliams relations and hence by the following matrix:

$$M = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

If the code is doubly-even, that is the Hamming weights of all vectors are $0 \pmod 8$, then it is also held invariant by the following matrix:

$$A = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

The putative $[72, 36, 16]$ code

The group $G = \langle G, A \rangle$ has order 192. The series $\Phi(\lambda) = \sum a_i \lambda^i$ where there are a_i independent polynomials held invariant by the group G. Next we apply the classic theorem of Molien.

The putative [72, 36, 16] code

The group $G = \langle G, A \rangle$ has order 192. The series $\Phi(\lambda) = \sum a_i \lambda^i$ where there are a_i independent polynomials held invariant by the group G. Next we apply the classic theorem of Molien.

Theorem

(Molien) For any finite group G of complex m by m matrices, $\Phi(\lambda)$ is given by

$$\Phi(\lambda) = \frac{1}{|G|} \sum_{A \in G} \frac{1}{det(I - \lambda A)} \tag{1}$$

where I is the identity matrix.

The putative [72, 36, 16] code

The group $G = \langle G, A \rangle$ has order 192. The series $\Phi(\lambda) = \sum a_i \lambda^i$ where there are a_i independent polynomials held invariant by the group G. Next we apply the classic theorem of Molien.

Theorem

(Molien) For any finite group G of complex m by m matrices, $\Phi(\lambda)$ is given by

$$\Phi(\lambda) = \frac{1}{|G|} \sum_{A \in G} \frac{1}{det(I - \lambda A)} \tag{1}$$

where I is the identity matrix.

For our group G we get

$$\Phi(\lambda) = \frac{1}{(1-\lambda^8)(1-\lambda^{24})} = 1 + \lambda^8 + \lambda^{16} + 2\lambda^{24} + 2\lambda^{32} + \ldots \tag{2}$$

The putative $[72, 36, 16]$ code

$$W_1(x, y) = x^8 + 14x^4y^4 + y^8 \tag{3}$$

and

$$W_2(x, y) = x^4y^4(x^4 - y^4)^4 \tag{4}$$

The putative $[72, 36, 16]$ code

$$W_1(x,y) = x^8 + 14x^4y^4 + y^8 \tag{3}$$

and

$$W_2(x,y) = x^4y^4(x^4 - y^4)^4 \tag{4}$$

Theorem

(Gleason) The weight enumerator of an Type II self-dual code is a polynomial in $W_1(x,y)$ and $W_2(x,y)$, i.e. if C is a Type II code then $W_C(x,y) \in \mathbb{C}[W_1(x,y), W_2(x,y)]$.

Bound

It follows that if C is a Type II $[n, k, d]$ code then

$$d \leq 4\lfloor \frac{n}{24} \rfloor + 4 \tag{5}$$

Bound

It follows that if C is a Type II $[n, k, d]$ code then

$$d \leq 4\lfloor \frac{n}{24} \rfloor + 4 \tag{5}$$

Codes meeting this bound are called extremal. We investigate those with parameters $[24k, 12k, 4k + 4]$. It is not known whether these codes exist until $24k \geq 3720$ at which a coefficient becomes negative.

General Form of the Question

Open Question

For which k does there exists a doubly-even self-dual binary $[24k, 12k, 4k+4]$ code?

Length 24 and 48

For length 24, there is a $[24, 12, 8]$ code, namely the well known Golay code.

Length 24 and 48

For length 24, there is a $[24, 12, 8]$ code, namely the well known Golay code.

For length 48, there is also a code namely the Pless code.

Length 24 and 48

For length 24, there is a $[24, 12, 8]$ code, namely the well known Golay code.

For length 48, there is also a code namely the Pless code.

Hence the first unknown case is whether there exists a $[72, 36, 16]$ code.

Weight Enumerator

C_i	i
1	0, 72
249849	16, 56
18106704	20, 52
462962955	24, 48
4397342400	28, 44
16602715899	32, 40
25756721120	36

Shadows

Lemma

Let C be a self-dual code with C_0 the subcode of doubly-even vectors. The subcode C_0 is linear and of codimension 1.

Shadows

Lemma

Let C be a self-dual code with C_0 the subcode of doubly-even vectors. The subcode C_0 is linear and of codimension 1.

Proof.

If $\mathbf{v}$ and $\mathbf{w}$ are doubly-even vectors then

$$wt(\mathbf{v}+\mathbf{w}) = wt(\mathbf{v}) + wt(\mathbf{w}) - 2|v \wedge w| \equiv 0 \pmod 4, \tag{6}$$

since both $wt(\mathbf{v})$ and $wt(\mathbf{w})$ are $0 \pmod 4$ and $|\mathbf{v} \wedge \mathbf{w}|$ is even since the vectors are orthogonal. Then the map $\psi : C \to \mathbb{F}_2$ with $\psi(c) = 0$ if it is doubly-even and 1 if it is singly even, is linear and C_0 is the kernel, which gives that $2|C_0| = |C|$ and so the code is of codimension 1. $\square$

Shadows

Then $C_0^\perp = C_0 \cup C_1 \cup C_2 \cup C_3$ with $C = C_0 \cup C_2$. Let $S = C_1 \cup C_3$ be the shadow of C with respect to the subcode C_0. Note that the shadow is a non-linear code.

Shadows

$$W_{C_0}(x, y) = (\frac{1}{2})(W_C(x, y) + W_C(x, iy)) \tag{7}$$

where i is the complex number with $i^2 = -1$.

Shadows

Lemma

Let C be a Type I self-dual code with S its shadow then

$$W_S(x, y) = W_C\left(\frac{x+y}{\sqrt{2}}, \frac{i(x-y)}{\sqrt{2}}\right). \tag{8}$$

Shadows

Proof.
Let T be the action of the MacWilliams transform.

$$\begin{aligned}
W_S(x,y) &= W_{C_0^\perp}(x,y) - W_C(x,y) \\
&= \frac{1}{|C_0|} T \cdot W_{C_0}(x,y) - W_C(x,y) \\
&= \frac{1}{2|C_0|} T \cdot (W_C(x,y) + W_C(x,iy)) - W_C(x,y) \\
&= \frac{1}{|C|} T \cdot W_C(x,y) + \frac{1}{|C|} T \cdot W_C(x,iy) - W_C(x,y) \\
&= \frac{1}{|C|} T \cdot W_C(x,iy)
\end{aligned}$$

□

Shadows

Theorem (Brualdi and Pless)

Let C be a self-dual code of length n, C_0 be any subcode of codimension 1, and S be the shadow with respect to that subcode, with $C_0^\perp = C_0 \cup C_1 \cup C_2 \cup C_3$ as described above. Then if $\mathbf{j} \notin C_0$, where $\mathbf{j}$ is the all-one vector, the code $C' = (0, 0, C_0) \cup (1, 1, C_2) \cup (1, 0, C_1) \cup (0, 1, C_3)$ is a self-dual code of length $n+2$ with weight enumerator: $W_{C'} = x^2 W_{C_0}(x, y) + y^2 W_{C_2}(x, y) + xyW_S(x, y)$ If $\mathbf{j} \in C_0$ then the code $C' = (0, 0, 0, 0, C_0) \cup (1, 1, 0, 0, C_2) \cup (1, 0, 1, 0, C_1) \cup (0, 1, 1, 0, C_3)$ is self-orthogonal and the code $C^* = \langle v, C' \rangle$, where $v = (1, 1, 1, 1, 0, \dots, 0)$, is a self-dual code of length $n+4$ with weight enumerator: $(x^4 + y^4) W_{C_0}(x, y) + (2x^2y^2)(W_{C_1}(x, y) + W_{C_2}(x, y) + W_{C_3}(x, y))$

Shadows

Theorem (Brualdi and Pless)

Let C be a self-dual code of length n, C_0 be any subcode of codimension 1, and S be the shadow with respect to that subcode, with $C_0^\perp = C_0 \cup C_1 \cup C_2 \cup C_3$ as described above. Then if $\mathbf{j} \notin C_0$, where $\mathbf{j}$ is the all-one vector, the code $C' = (0,0,C_0) \cup (1,1,C_2) \cup (1,0,C_1) \cup (0,1,C_3)$ is a self-dual code of length $n+2$ with weight enumerator: $W_{C'} = x^2 W_{C_0}(x,y) + y^2 W_{C_2}(x,y) + xyW_S(x,y)$ If $\mathbf{j} \in C_0$ then the code $C' = (0,0,0,0,C_0) \cup (1,1,0,0,C_2) \cup (1,0,1,0,C_1) \cup (0,1,1,0,C_3)$ is self-orthogonal and the code $C^* = \langle v, C' \rangle$, where $v = (1,1,1,1,0,\ldots,0)$, is a self-dual code of length $n+4$ with weight enumerator: $(x^4+y^4)W_{C_0}(x,y) + (2x^2y^2)(W_{C_1}(x,y) + W_{C_2}(x,y) + W_{C_3}(x,y))$

In either case we refer to the larger code as the parent code and the smaller code as the child.

Building Up

Let C be a self-dual code of length $n+2$. We can take as a generator matrix, a matrix of the following form:

$$\left(\ I\ ,\ G\ \right)$$

where I is the identity matrix. It follows that we can then take a generator matrix to be

$$\begin{pmatrix} 0 & 0 & H_1 \\ 0 & 0 & H_2 \\ 0 & 0 & H_3 \\ & & . \\ & & . \\ & & . \\ 0 & 0 & H_{\frac{n}{2}-1} \\ 1 & 1 & v \\ 0 & 1 & u \end{pmatrix}$$

where the matrix H with rows $H_1, ..., H_{\frac{n}{2}-1}$ generates a self-orthogonal code D_0.

Building Up

Theorem

If C is a self-dual code of length $n+2$ with minimum weight greater than 2, then for some self-dual code D of length n, we have that C is the parent of D.

Child

The existence of a $[72, 36, 16]$ Type I code is equivalent to the existence of a Type I $[70, 35, 14]$ code.

Child

Table: The Weight Distribution of a [70,35,14] Code

Weight	Frequency
0, 70	1
14, 56	11730
16, 54	150535
18, 52	1345960
20, 50	9393384
22, 48	49991305
24, 46	204312290
26, 44	650311200
28, 42	1627498400
30, 40	3221810284
32, 38	5066556495
34, 36	6348487600

Child

Table: The Weight Distribution of the Shadow of a [70,35,14] Code

Weight	Frequency
15, 55	87584
19, 51	7367360
23, 47	208659360
27, 43	2119532800
31, 39	8314349120
35	13059745920

Child

Lemma

A doubly-even self-dual $[24k, 12k, 4k + 4]$ *code is an extremal code and has a unique weight enumerator. Every singly-even* $[24k - 2, 12k - 1]$ *code is a child of a doubly-even* $[24k, 12k]$ *code.*

Child

Lemma

A doubly-even self-dual $[24k, 12k, 4k+4]$ *code is an extremal code and has a unique weight enumerator. Every singly-even* $[24k-2, 12k-1]$ *code is a child of a doubly-even* $[24k, 12k]$ *code.*

Lemma

The weight enumerator of a $[24k-2, 12k-1, 4k+2]$ *child of a doubly-even* $[24k, 12k, 4k+4]$ *is uniquely determined. The shadow of the child has minimum weight* $4k+3$*.*

Child

Theorem

For fixed k, the existence of a singly-even $[24k-2, 12k-1, 4k+2]$ *code whose shadow has minimum weight* $4k+3$ *is equivalent to the existence of an extremal doubly-even code of length* $24k$.

Equivalence

Theorem

The existence of an extremal doubly-even self-dual code of length $24k$ is equivalent to the existence of a singly-even self-dual $[24k-2, 12k-1, 4k+2]$ code.

Neighbors

Let $\mathbf{v}$ be any weight 4 vector of length $24k$. Consider the neighbor $C' = N(C, \mathbf{v})$. That is, if C_0 is the subcode of C with vectors orthogonal to $\mathbf{v}$ then $C' = \langle C_0, \mathbf{v} \rangle$.

Neighbors

Let $\mathbf{v}$ be any weight 4 vector of length $24k$. Consider the neighbor $C' = N(C, \mathbf{v})$. That is, if C_0 is the subcode of C with vectors orthogonal to $\mathbf{v}$ then $C' = \langle C_0, \mathbf{v} \rangle$.

Theorem

If C is a doubly-even $[24k, 12k, 4k+4]$ code, then the neighbor $C' = N(C, \mathbf{v})$ where $\mathbf{v}$ is any weight 4 vector, has a uniquely determined weight enumerator.

Neighbor

Let E be a $[24k-4, 12k-2, 4k]$ child of the code C'. That is, if

$$C^* = (0,0,0,0,C_0) \cup (1,1,0,0,C_2) \cup (1,0,1,0,C_1) \cup (0,1,1,0,C_3)$$

then $C' = \langle v, C^* \rangle$.

Neighbor

Let E be a $[24k-4, 12k-2, 4k]$ child of the code C'. That is, if

$$C^* = (0,0,0,0,C_0) \cup (1,1,0,0,C_2) \cup (1,0,1,0,C_1) \cup (0,1,1,0,C_3)$$

then $C' = \langle v, C^* \rangle$.

Theorem

If C' is the weight 4 neighbor of a doubly-even $[24k, 12k, 4k+4]$ code then the child E of C' is a $[24k-4, 12k-2, 4k]$ code and has a uniquely determined weight enumerator.

To show for a particular k that there is no doubly-even $[24k, 12k, 4k+4]$ code it is enough to show that the code C' or E as described above does not exist.

Neighbor

Table: The Weight Distribution of the Weight 4 Neighbor and its Subcode

	C_0	C'
Weight	Frequency	Frequency
0, 72	1	1
4, 68	0	1
12, 60	0	442
16, 56	134521	264673
20, 52	9284176	18589296
24, 48	232444043	464824659
28, 44	2196187840	4392509606
32, 40	8298695163	16597183691
36	12886246880	25772731998

Neighbor

Table: The Weight Distribution of the Child of the Weight 4 Neighbor

Weight	Frequency
0, 68	1
12, 56	442
14, 54	14960
16, 52	174471
18, 50	1478048
20, 48	9546537
22, 46	46699952
24, 44	175078410
26, 42	509477760
28, 40	1160564636
30, 38	2081169376
32, 36	2949602799
34	3312254400

Designs

An incidence structure $D = (P, B, I)$ is a $t - (v, k, \lambda)$ design, where t, v, k, λ are non-negative integers, if

- $|P| = v$;
- every block $b \in B$ is incident with precisely k points;
- every t distinct points are together incident with precisely λ blocks.

Designs

The Assmus-Mattson theorem gives 5-designs in the length 72 code.

Designs

Let D be a $[70, 35, 14]$ Type I code, and let D_0 be the subcode of doubly-even vectors. The weight enumerators for D_0 and $D_0^{\perp}$ can be easily calculated using Tables 2 and 3. It follows from the Assmus-Mattson Theorem that the vectors of any weight in D_0 and $D_0^{\perp}$ hold 3-designs. This gives divisibility conditions on the coefficients of the shadow if a code exists, namely the λ_j for $j = 1, 2, 3$ for each weight must be integers.

Designs

Table: Design Parameters

i	λ_1	λ_2	λ_3
15	18768	3808	728
19	1999712	521664	130416
23	68559504	21859552	6750744
27	817534080	308056320	113256000
31	3682068896	1600899520	682736560
35	6529872960	3217618560	1561491360
39	4632280224	2551110848	1388104432
43	1301998720	792520960	477843520
47	140099856	93399904	61808760
51	5367648	3889600	2802800
55	68816	53856	41976

Higher Weights

Let $D \subseteq \mathbb{F}_2^n$ be a linear subspace, then

$$||D|| = |Supp(D)|, \tag{9}$$

where

$$Supp(D) = \{i \mid \exists v \in D,\ v_i \neq 0\}. \tag{10}$$

Higher Weights

Let $D \subseteq \mathbb{F}_2^n$ be a linear subspace, then

$$||D|| = |Supp(D)|, \tag{9}$$

where

$$Supp(D) = \{i \mid \exists v \in D,\ v_i \neq 0\}. \tag{10}$$

For a linear code C define

$$d_r(C) = min\{||D|| \mid D \subseteq C,\ \dim(D) = r\}. \tag{11}$$

Higher Weights

Let $D \subseteq \mathbb{F}_2^n$ be a linear subspace, then

$$||D|| = |Supp(D)|, \tag{9}$$

where

$$Supp(D) = \{i \mid \exists v \in D,\ v_i \neq 0\}. \tag{10}$$

For a linear code C define

$$d_r(C) = min\{||D|| \mid D \subseteq C,\ \dim(D) = r\}. \tag{11}$$

The higher weight spectrum is defined as

$$A_i^r = |\{D \subseteq C \mid \dim(D) = r,\ ||D|| = i\}|. \tag{12}$$

and then we define the higher weight enumerator by

$$W^r(C; y) = W^r(C) = \sum A_i^r y^i. \tag{13}$$

Higher Weight Enumerator

Table: The Second Higher Weight Enumerator

coefficient of y^i	weight i
96191865	24
4309395552	26
119312891460	28
2379079500864	30
37327599503964	32
466987648992480	34
4687779244903412	36
37810235197002240	38
244777798274765679	40
1269000323938260672	42
5251816390965277320	44
17262594429823645056	46
44763003632389491540	48

Higher Weight Enumerator

Table: The Second Higher Weight Enumerator

coefficient of y^i	weight i
90768836016453484224	50
142313871132195291144	52
170060449665123790080	54
152060783100409784007	56
99349931253373567200	58
45970401654169517364	60
14440224673488398400	62
2900924791551272475	64
340809968304405600	66
20197782231604740	68
451381581930240	70
1617151596337	72

Automorphism Group

The automorphism group of the putative $[72, 36, 16]$ has order less than or equal to 5.

Automorphism Group

The automorphism group of the putative $[72, 36, 16]$ has order less than or equal to 5.
Is there a contradiction that can be found in terms of the automorphism group?

Open Problems

- Prove that the $[70, 35, 14]$ Type I code with weight enumerator given above does not exist or construct it and then the length 72 code from it.

Open Problems

- Prove that the $[70, 35, 14]$ Type I code with weight enumerator given above does not exist or construct it and then the length 72 code from it.
- Prove that the $[68, 34, 12]$ Type I code with weight enumerator given above does not exist or construct it and then the length 72 code from it.

Open Problems

- Prove that the $[70, 35, 14]$ Type I code with weight enumerator given above does not exist or construct it and then the length 72 code from it.
- Prove that the $[68, 34, 12]$ Type I code with weight enumerator given above does not exist or construct it and then the length 72 code from it.
- Show that one of the designs given in the paper does not exist showing that the code does not exist.

Open Problems

- Prove that the $[70, 35, 14]$ Type I code with weight enumerator given above does not exist or construct it and then the length 72 code from it.
- Prove that the $[68, 34, 12]$ Type I code with weight enumerator given above does not exist or construct it and then the length 72 code from it.
- Show that one of the designs given in the paper does not exist showing that the code does not exist.
- Find one of the designs given in the paper and examine the code generated by the incidence vectors of the blocks and determine if they construct one of the codes.

Codes and Lattices

The Euclidean weight $wt_E(x)$ of a vector $(x_1, x_2, \ldots, x_n)$ is $\sum_{i=1}^{n} \min\{x_i^2, (2k - x_i)^2\}$.

Codes and Lattices

The Euclidean weight $wt_E(x)$ of a vector $(x_1, x_2, \ldots, x_n)$ is $\sum_{i=1}^{n} \min\{x_i^2, (2k - x_i)^2\}$.

Theorem

Suppose that C is a self-dual code over $\mathbb{Z}_{2k}$ which has the property that every Euclidean weight is a multiple of a positive integer. Then the largest positive integer c is either $2k$ or $4k$.

Codes and Lattices

The Euclidean weight $wt_E(x)$ of a vector $(x_1, x_2, \ldots, x_n)$ is $\sum_{i=1}^{n} \min\{x_i^2, (2k - x_i)^2\}$.

Theorem

Suppose that C is a self-dual code over $\mathbb{Z}_{2k}$ which has the property that every Euclidean weight is a multiple of a positive integer. Then the largest positive integer c is either $2k$ or $4k$.

A self-dual code over $\mathbb{Z}_{2k}$ where every vector has weight a multiple of $4k$ is said to be Type II, otherwise it is said to be Type I.

Lattices

Let $\mathbb{R}^n$ be an n-dimensional Euclidean space with the standard inner product. An n-dimensional lattice Λ in $\mathbb{R}^n$ is a free $\mathbb{Z}$-module spanned by n linearly independent vectors $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$.

Lattices

Let $\mathbb{R}^n$ be an n-dimensional Euclidean space with the standard inner product. An n-dimensional lattice Λ in $\mathbb{R}^n$ is a free $\mathbb{Z}$-module spanned by n linearly independent vectors $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$.

A matrix whose rows are the vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n$ is called a generator matrix G of the lattice Λ. The fundamental volume $V(\Lambda)$ of Λ is $|\det G|$.

Lattices

Let $\mathbb{R}^n$ be an n-dimensional Euclidean space with the standard inner product. An n-dimensional lattice Λ in $\mathbb{R}^n$ is a free $\mathbb{Z}$-module spanned by n linearly independent vectors $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$.

A matrix whose rows are the vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n$ is called a generator matrix G of the lattice Λ. The fundamental volume $V(\Lambda)$ of Λ is $|\det G|$.

The dual lattice Λ^* is given by
$\Lambda^* = \{\mathbf{v} \in \mathbb{R}^n \mid \mathbf{v} \cdot \mathbf{w} \in \mathbb{Z} \text{ for all } \mathbf{w} \in \Lambda\}$.

Lattices

We say that a lattice Λ is *integral* if $\Lambda \subseteq \Lambda^*$ and that an integral lattice with $\det \Lambda = 1$ (or $\Lambda = \Lambda^*$) is unimodular.

Lattices

We say that a lattice Λ is *integral* if $\Lambda \subseteq \Lambda^*$ and that an integral lattice with $\det \Lambda = 1$ (or $\Lambda = \Lambda^*$) is unimodular.

If the norm $\mathbf{v} \cdot \mathbf{v}$ is an even integer for all $\mathbf{v} \in \Lambda$, then Λ is said to even. Unimodular lattices which are not even are called odd. The minimum norm of Λ is the smallest norm among all nonzero vectors of Λ.

Lattices

We say that a lattice Λ is *integral* if $\Lambda \subseteq \Lambda^*$ and that an integral lattice with $\det \Lambda = 1$ (or $\Lambda = \Lambda^*$) is unimodular.

If the norm $\mathbf{v} \cdot \mathbf{v}$ is an even integer for all $\mathbf{v} \in \Lambda$, then Λ is said to even. Unimodular lattices which are not even are called odd. The minimum norm of Λ is the smallest norm among all nonzero vectors of Λ.

It is well known that except for $n = 23$, the minimum norm of a unimodular lattice of length n is bounded above by $2\lfloor \frac{n}{24} \rfloor + 2$.

Codes and Lattices

Theorem

(**Bannai, Dougherty, Harada, Oura**) *Let* ρ *be a map from* $\mathbb{Z}_{2k}$ *to* $\mathbb{Z}$ *sending* $0, 1, \ldots, k$ *to* $0, 1, \ldots, k$ *and* $k+1, \ldots, 2k-1$ *to* $1-k, \ldots, -1$*, respectively. If* C *is a self-dual code of length* n *over* $\mathbb{Z}_{2k}$*, then the lattice*

$$\Lambda(C) = \frac{1}{\sqrt{2k}}\{\rho(C) + 2k\mathbb{Z}^n\},$$

is an n*-dimensional unimodular lattice, where* $\rho(C) = \{(\rho(c_1), \ldots, \rho(c_n)) \mid (c_1, \ldots, c_n) \in C\}$*. The minimum norm is* $\min\{2k, d_E/2k\}$ *where* d_E *is the minimum Euclidean weight of* C*. Moreover, if* C *is Type II then the lattice* $\Lambda(C)$ *is an even unimodular lattice.*

$\mathbb{Z}_8$ code

Eight is not four Patrick. – Vera Pless to Patrick Solé.

$\mathbb{Z}_8$ code

Eight is not four Patrick. – Vera Pless to Patrick Solé.

G. Nebe finds a Type II code over $\mathbb{Z}_8$ of length 72 with minimum Euclidean weight 64. The existence of this code implies the existence of an extremal Type II lattice of dimension 72.

Codes and Lattices

Open Question

Find a Type II self-dual code over $\mathbb{Z}_{2k}$, $2k \geq 2s+2$ *such that* $\frac{d_E}{2k} = 2s+2$. *Such an extremal code will give an extremal lattice using Theorem 5.*

Codes and Lattices

Open Question

Find a Type II self-dual code over $\mathbb{Z}_{2k}$, $2k \geq 2s+2$ such that $\frac{d_E}{2k} = 2s+2$. Such an extremal code will give an extremal lattice using Theorem 5.

The next case would be to find a $\mathbb{Z}_{16}$ code with $d_E = 160$. This would given an extremal lattice at length 96.

Decoding Algorithms

Decoding Algorithms

A decoding algorithm is an algorithm that takes received vectors and (efficiently) computes the error vector.

Decoding Algorithms

A decoding algorithm is an algorithm that takes received vectors and (efficiently) computes the error vector.

Cyclic codes have an efficient decoding algorithm.

Decoding algorithms

There exist efficient decoding algorithms for various classes of codes. However, for some well known families there do not exist such algorithms.

Decoding algorithms

There exist efficient decoding algorithms for various classes of codes. However, for some well known families there do not exist such algorithms.

The decoding algorithm for Reed Solomon codes was given as an example of an application of algebraic number theory in contradiction to Hardy's famous statement in the *Mathematician's Apology*.

N. Levison: Coding Theory – a Counterexample to G.H. Hardy's Conception of Applied Mathematics, Amer. Math. Monthly 77, 249-258.

Decoding Algorithms

Open Question

Find an efficient decoding algorithm for a family of self-dual codes or for all self-dual codes.

Decoding Algorithms

Open Question

Find an efficient decoding algorithm for a family of self-dual codes or for all self-dual codes.

It is rather mysterious that self-dual codes don't have a general decoding algorithm. Efficient decoding algorithms exist for the binary Golay $[24, 12, 8]$ code, four of the five Type II $[32, 16, 8]$ codes, and the Type II $[48, 24, 12]$ code q_{48}.

Decoding Algorithms

Open Question

Give a universal decoding algorithm for quasi-cyclic codes.

Decoding Algorithms

Open Question

Give a universal decoding algorithm for quasi-cyclic codes.

Given the fact cyclic codes have an efficient decoding algorithm, it seems that quasi-cyclic codes should as well. In this direction, find an algebraic description of these codes. Note that the image of quaternary cyclic codes are binary quasi-cyclic codes.

Gilbert-Varshamov bound

Let $A_q(n, d)$ be the maximum size of a q-ary code C of length n and minimum distance n. Then

$$A_q(n, d)(\sum_{j=0}^{d-1} \left(\begin{array}{c} n \\ j \end{array} \right))(q-1)^j) \geq q^n.$$

Gilbert-Varshamov bound

Let $A_q(n, d)$ be the maximum size of a q-ary code C of length n and minimum distance n. Then

$$A_q(n, d)(\sum_{j=0}^{d-1} \left(\begin{array}{c} n \\ j \end{array} \right))(q-1)^j) \geq q^n.$$

The linear programming bound puts restrictions on the maximum dimension of a code given the length and minimum distance using the MacWilliams relations.

Gilbert-Varshamov bound

Posed by P. Solé.

1. Bridge the gap between Gilbert-Varshamov and LP bound.

Gilbert-Varshamov bound

Posed by P. Solé.

1. Bridge the gap between Gilbert-Varshamov and LP bound.
2. Is the GV bound tight for $q = 2$? It is not for $q > 49$.