Arrangements, matroids and codes

first lecture

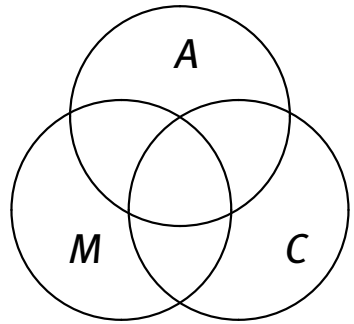
Ruud Pellikaan
joint work with
Relinde Jurrius

ACAGM summer school
Leuven Belgium, 18 July 2011

References

1. Codes, arrangements and matroids
   by Relinde Jurrius and Ruud Pellikaan,
   in Series on Coding Theory and Cryptology vol. 8
   Algebraic geometry modelling in information theory
   E. Martinez-Moro Ed., World Scientific 2011
   http://www.win.tue.nl/∼ruudp/paper/57.pdf
2. Error-correcting codes and cryptology
   by R. Pellikaan, X.-W. Wu and S. Bulygin
   Book in preparation, February 2011
   To be published by Cambridge University Press
   http://www.win.tue.nl/∼ruudp/courses/2WC11/2WC11-book.pdf

Introduction



- C = error-correcting codes
  (extended) weight enumerator polynomial $W_C(X, Y)$, $W_C(X, Y, T)$
- M = matroids
  generalization of linear algebra and graph theory
  (di)chromatic polynomial and Tutte polynomial $t_M(X, Y)$
- A = arrangements of hyperplanes
  topology, combinatorics
  characteristic polynomial $\chi(T)$, coboundary polynomial $\chi(S, T)$

Content 5 lectures

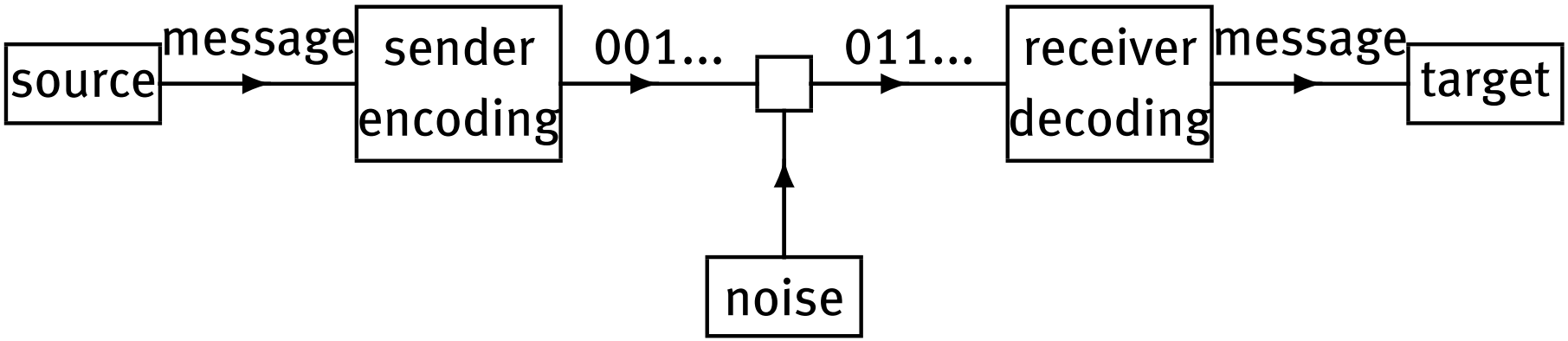
1. Error-correcting codes
   Weight enumerator
2. q-ary symmetric channel and the probability of undetected error
   Arrangements and projective systems
3. Extended weight enumerator
   Graph theory and colorings
4. Matroids
   Tutte-Whitney polynomial
5. Geometric lattices
   Characteristic polynomial

Content first lecture

1. Error-correcting codes:
   Shannon, Hamming distance
2. Linear codes:
   Generator and parity check matrix, inner product and dual code
   Hamming and simplex codes
3. Singleton bound and MDS codes:
   Vandermonde matrices and generalized Reed-Solomon codes
4. Weight enumerator:
   MacWilliams identity and examples
5. Exercises

Error-correcting codes

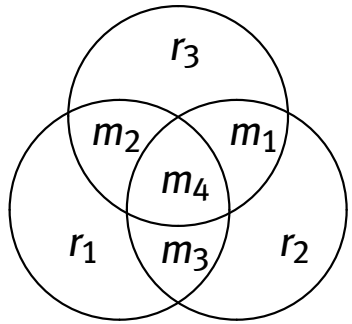
Shannon's block diagram



Shannon's block diagram of a communication system

Hamming code

4 message bits: (m_1, m_2, m_3, m_4)
3 redundant bits: (r_1, r_2, r_3)
Rule: number of ones in every circle is even



Venn diagram of the Hamming code

Block codes

The message words have a fixed length of k symbols
the encoded words have a fixed length of n symbols
both from the same alphabet Q

Add redundant symbols to the message in a clever way

An error-correcting code C of length n over Q
is a non-empty subset of Q^n

The elements of C are called codewords
If C contains M codewords, then M is called the size

$n - \log_q(M)$ is called the redundancy
$R = \log_q(M)/n$ is the information rate

Block codes

The message words have a fixed length of k symbols
the encoded words have a fixed length of n symbols
both from the same alphabet Q

Add redundant symbols to the message in a clever way

An error-correcting code C of length n over Q
is a non-empty subset of Q^n

The elements of C are called codewords
If C contains M codewords, then M is called the size

$n - \log_q(M)$ is called the redundancy
$R = \log_q(M)/n$ is the information rate

Block codes

The message words have a fixed length of k symbols
the encoded words have a fixed length of n symbols
both from the same alphabet Q

Add redundant symbols to the message in a clever way

An error-correcting code C of length n over Q
is a non-empty subset of Q^n

The elements of C are called codewords
If C contains M codewords, then M is called the size

$n - \log_q(M)$ is called the redundancy
$R = \log_q(M)/n$ is the information rate

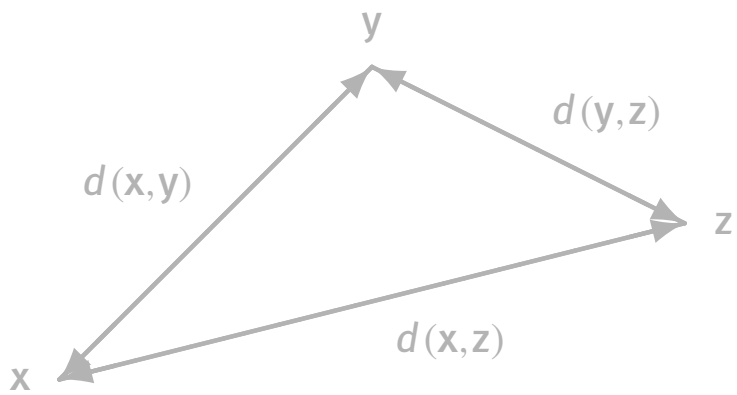
Hamming distance

The Hamming distance $d(\mathbf{x}, \mathbf{y})$ on Q^n is defined by

$$d(\mathbf{x}, \mathbf{y}) = |\{i : x_i \neq y_i\}|$$

It is a metric:

1. $d(\mathbf{x}, \mathbf{y}) \geq 0$ and equality hods if and only if $\mathbf{x} = \mathbf{y}$
2. $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{y}, \mathbf{x})$ (symmetry)
3. $d(\mathbf{x}, \mathbf{z}) \leq d(\mathbf{x}, \mathbf{y}) + d(\mathbf{y}, \mathbf{z})$ (triangle inequality)



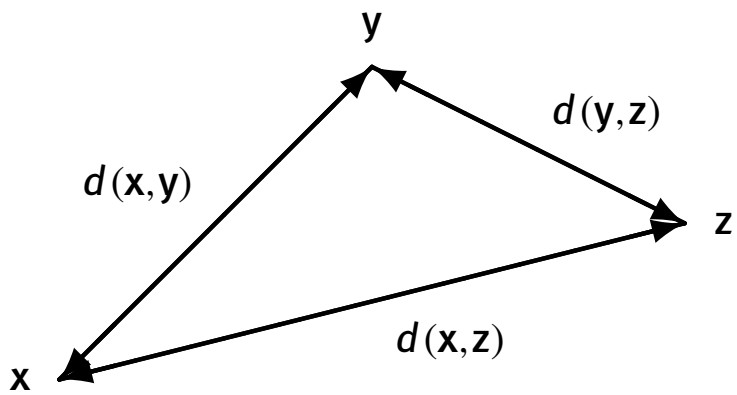
Hamming distance

The Hamming distance $d(\mathbf{x}, \mathbf{y})$ on Q^n is defined by

$$d(\mathbf{x}, \mathbf{y}) = |\{i : x_i \neq y_i\}|$$

It is a metric:

1. $d(\mathbf{x}, \mathbf{y}) \geq 0$ and equality hods if and only if $\mathbf{x} = \mathbf{y}$
2. $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{y}, \mathbf{x})$ (symmetry)
3. $d(\mathbf{x}, \mathbf{z}) \leq d(\mathbf{x}, \mathbf{y}) + d(\mathbf{y}, \mathbf{z})$ (triangle inequality)



Minimum distance

The minimum (Hamming) distance of a code C is defined as

$$d = d(C) = \min\{d(\mathbf{x}, \mathbf{y}) : \mathbf{x}, \mathbf{y} \in C, \mathbf{x} \neq \mathbf{y}\}$$

The main problem of error-correcting codes
from Hamming's point of view is:

to construct for a given length and number of codewords
a code with the largest possible minimum distance
and
to find efficient encoding and decoding algorithms

Minimum distance

The minimum (Hamming) distance of a code C is defined as

$$d = d(C) = \min\{d(\mathbf{x}, \mathbf{y}) : \mathbf{x}, \mathbf{y} \in C, \mathbf{x} \neq \mathbf{y}\}$$

The main problem of error-correcting codes
from Hamming's point of view is:

to construct for a given length and number of codewords
a code with the largest possible minimum distance
and
to find efficient encoding and decoding algorithms

Examples

The triple repetition binary code has length 3 and 2 codewords
its information rate is $1/3$
its minimum distance is 3.

The binary Hamming code has length 7 and 2^4 codewords
therefore its rate is $4/7$
its minimum distance is 3

Linear codes

Linear codes

If the alphabet Q is the finite field $\mathbb{F}_q$ with q elements
then Q^n is a vector space
Therefore it is natural to look at codes in Q^n
that are linear subspaces

A linear code C is a linear subspace of $\mathbb{F}_q^n$
Its dimension is denoted by $k = k(C)$
and its minimum distance by $d = d(C)$

Then $[n, k, d]_q$ or $[n, k, d]$ denote the parameters of the code

Size: $M = q^k$
Information rate: $R = k/n$
Redundancy: $n - k$

Support and minimal weight

The support of $\mathbf{x}$ in $\mathbb{F}_q^n$ is defined by

$$\operatorname{supp}(\mathbf{x}) = \{j : x_j \neq 0\}$$

The weight of $\mathbf{x}$ is defined by

$$\operatorname{wt}(\mathbf{x}) = |\operatorname{supp}(\mathbf{x})|$$

that is the number of nonzero entries of $\mathbf{x}$

Let C be an $\mathbb{F}_q$-linear code, then

$$d(C) = \min\{\operatorname{wt}(\mathbf{c}) : \mathbf{0} \neq \mathbf{c} \in C\}$$

Support and minimal weight

The support of $\mathbf{x}$ in $\mathbb{F}_q^n$ is defined by

$$\operatorname{supp}(\mathbf{x}) = \{j : x_j \neq 0\}$$

The weight of $\mathbf{x}$ is defined by

$$\operatorname{wt}(\mathbf{x}) = |\operatorname{supp}(\mathbf{x})|$$

that is the number of nonzero entries of $\mathbf{x}$

Let C be an $\mathbb{F}_q$-linear code, then

$$d(C) = \min\{\operatorname{wt}(\mathbf{c}) : \mathbf{0} \neq \mathbf{c} \in C\}$$

Generator and parity check matrix

C an $\mathbb{F}_q$-linear code of dimension k

A $k \times n$ matrix G with entries in $\mathbb{F}_q$
is called generator matrix of C if

$$C = \{ \mathbf{x}G \mid \mathbf{x} \in \mathbb{F}_q^k \}$$

A $(n-k) \times n$ matrix H with entries in $\mathbb{F}_q$
is called a parity check matrix of C if

$$C = \{ \mathbf{c} \in \mathbb{F}_q^n \mid \mathbf{c}H^T = 0 \}$$

Generator and parity check matrix

C an $\mathbb{F}_q$-linear code of dimension k

A $k \times n$ matrix G with entries in $\mathbb{F}_q$
is called generator matrix of C if

$$C = \{ \mathbf{x}G \mid \mathbf{x} \in \mathbb{F}_q^k \}$$

A $(n-k) \times n$ matrix H with entries in $\mathbb{F}_q$
is called a parity check matrix of C if

$$C = \{ \mathbf{c} \in \mathbb{F}_q^n \mid \mathbf{c}H^T = 0 \}$$

Example

The binary Hamming code with parameters $[7, 4, 3]$ has generator matrix G:

$$G = \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right)$$

and parity check matrix H:

$$H = \left(\begin{array}{cccc|ccc} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right)$$

Example

The binary Hamming code with parameters $[7, 4, 3]$ has generator matrix G:

$$G = \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right)$$

and parity check matrix H:

$$H = \left(\begin{array}{cccc|ccc} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right)$$

Proposition

Suppose C is a $[n, k]$ code
Let I_k be the $k \times k$ identity matrix
Let P be a $k \times (n - k)$ matrix

Then $(I_k|P)$ is a generator matrix of C

if and only if

$(-P^T|I_{n-k})$ is a parity check matrix of C

Proposition

Suppose C is a $[n, k]$ code
Let I_k be the $k \times k$ identity matrix
Let P be a $k \times (n - k)$ matrix

Then $(I_k|P)$ is a generator matrix of C

if and only if

$(-P^T|I_{n-k})$ is a parity check matrix of C

Inner product and dual code

The inner product on $\mathbb{F}_q^n$ is defined by

$$\mathbf{x} \cdot \mathbf{y} = x_1 y_1 + \cdots + x_n y_n$$

This inner product is bilinear, symmetric and nondegenerate
but the notion of positive definite makes no sense over a finite field

For an $[n, k]$ code C we define the dual or orthogonal code $C^\perp$ as

$$C^\perp = \{\mathbf{x} \in \mathbb{F}_q^n : \mathbf{c} \cdot \mathbf{x} = 0 \text{ for all } \mathbf{c} \in C\}.$$

Inner product and dual code

The inner product on $\mathbb{F}_q^n$ is defined by

$$\mathbf{x} \cdot \mathbf{y} = x_1 y_1 + \cdots + x_n y_n$$

This inner product is bilinear, symmetric and nondegenerate
but the notion of positive definite makes no sense over a finite field

For an $[n, k]$ code C we define the dual or orthogonal code $C^\perp$ as

$$C^\perp = \{\mathbf{x} \in \mathbb{F}_q^n : \mathbf{c} \cdot \mathbf{x} = 0 \text{ for all } \mathbf{c} \in C\}.$$

Generator and parity check matrix of dual code

Proposition

If C has length n, then

$$\dim(C) + \dim(C^{\perp}) = n$$

Furthermore

G is a generator matrix of C if and only if
G is a parity check matrix of $C^{\perp}$

H is a parity check matrix of C if and only if
H is a generator matrix of $C^{\perp}$

Generator and parity check matrix of dual code

Proposition

If C has length n, then

$$\dim(C) + \dim(C^{\perp}) = n$$

Furthermore

G is a generator matrix of C if and only if
G is a parity check matrix of $C^{\perp}$

H is a parity check matrix of C if and only if
H is a generator matrix of $C^{\perp}$

Parity check matrix and minimum distance

Proposition Let H be a parity check matrix of a code C
Then the minimum distance d of C is the smallest integer d such that d columns of H are linearly dependent

Proof

H parity check matrix with entries $h_{i,j}$

c a codeword of weight d with nonzero entries c_{j_i}

$Hc^T = 0$

$\cdots$	c_{j_1}	$\cdots$	c_{j_d}	$\cdots$
$\cdots$	h_{1,j_1}	$\cdots$	h_{1,j_d}	$\cdots$
$\cdots$	$\vdots$	$\cdots$	$\vdots$	$\cdots$
$\cdots$	$h_{(n-k),j_1}$	$\cdots$	$h_{(n-k),j_d}$	$\cdots$

Parity check matrix and minimum distance

Proposition Let H be a parity check matrix of a code C
Then the minimum distance d of C is the smallest integer d such that d columns of H are linearly dependent

Proof

H parity check matrix with entries $h_{i,j}$
$\mathbf{c}$ a codeword of weight d with nonzero entries c_{j_i}
$H\mathbf{c}^T = \mathbf{0}$

$\cdots$	c_{j_1}	$\cdots$	c_{j_d}	$\cdots$
$\cdots$	h_{1,j_1}	$\cdots$	h_{1,j_d}	$\cdots$
$\cdots$	$\vdots$	$\cdots$	$\vdots$	$\cdots$
$\cdots$	$h_{(n-k),j_1}$	$\cdots$	$h_{(n-k),j_d}$	$\cdots$

Nondegenerate codes

Let G be a generator matrix of C

C is called nondegenerate
if for every position j there is codeword $\mathbf{c}$ such that $c_j \neq 0$

The following statements are equivalent:

1. C is nondegenerate
2. G has no zero column
3. $d(C^{\perp}) \geq 2$

Nondegenerate codes

Let G be a generator matrix of C

C is called nondegenerate
if for every position j there is codeword $\mathbf{c}$ such that $c_j \neq 0$

The following statements are equivalent:

1. C is nondegenerate
2. G has no zero column
3. $d(C^{\perp}) \geq 2$

q-ary Hamming and simplex codes

Let $n = (q^r - 1)/(q - 1)$
Let $H_r(q)$ be a $r \times n$ matrix over $\mathbb{F}_q$
such that no two columns are dependent

The code $\mathcal{H}_r(q)$ with $H_r(q)$ as parity check matrix
is called a q-ary Hamming code

The code with $H_r(q)$ as generator matrix
is called a q-ary simplex code and is denoted by $\mathcal{S}_r(q)$

$\mathcal{S}_r(q)$ and $\mathcal{H}_r(q)$ are dual codes

q-ary Hamming and simplex codes

Let $n = (q^r - 1)/(q - 1)$
Let $H_r(q)$ be a $r \times n$ matrix over $\mathbb{F}_q$
such that no two columns are dependent

The code $\mathcal{H}_r(q)$ with $H_r(q)$ as parity check matrix
is called a q-ary Hamming code

The code with $H_r(q)$ as generator matrix
is called a q-ary simplex code and is denoted by $\mathcal{S}_r(q)$

$\mathcal{S}_r(q)$ and $\mathcal{H}_r(q)$ are dual codes

Parameters of Hamming and Simplex codes

Let $r \geq 2$

The q-ary Hamming code $\mathcal{H}_r(q)$
has parameters $[(q^r - 1)/(q - 1), (q^r - 1)/(q - 1) - r, 3]$

The q-ary simplex code $\mathcal{S}_r(q)$ is a constant weight code
with parameters $[(q^r - 1)/(q - 1), r, q^{r-1}]$

Parameters of Hamming and Simplex codes

Let $r \geq 2$

The q-ary Hamming code $\mathcal{H}_r(q)$
has parameters $[(q^r - 1)/(q - 1), (q^r - 1)/(q - 1) - r, 3]$

The q-ary simplex code $\mathcal{S}_r(q)$ is a constant weight code
with parameters $[(q^r - 1)/(q - 1), r, q^{r-1}]$

Example $\mathcal{S}_3(3)$

Consider the ternary Hamming code $\mathcal{S}_3(3)$
of redundancy 3 of length 13 with parity check matrix

$$H_3(3) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 2 & 2 & 2 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 2 & 1 & 0 & 2 & 1 & 0 & 2 & 1 & 0 & 2 & 1 & 0 & 1 \end{pmatrix}.$$

The code $\mathcal{H}_3(3)$ has parameters $[13, 10, 3]$

The code $\mathcal{S}_3(3)$ has parameters $[13, 3, 9]$

All rows of $H_3(3)$ have weight 9
In fact all nonzero codewords have weight 9

Example $\mathcal{S}_3(3)$

Consider the ternary Hamming code $\mathcal{S}_3(3)$
of redundancy 3 of length 13 with parity check matrix

$$H_3(3) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 2 & 2 & 2 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 2 & 1 & 0 & 2 & 1 & 0 & 2 & 1 & 0 & 2 & 1 & 0 & 1 \end{pmatrix}.$$

The code $\mathcal{H}_3(3)$ has parameters $[13, 10, 3]$

The code $\mathcal{S}_3(3)$ has parameters $[13, 3, 9]$

All rows of $H_3(3)$ have weight 9
In fact all nonzero codewords have weight 9

Singleton bound

and

MDS codes

Singleton bound

Theorem If C is an $[n, k, d]$ code, then

$$d \leq n - k + 1$$

Proof

Let H be a parity check matrix of C

This is an $(n - k) \times n$ matrix

There exist $n - k + 1$ dependent columns

in fact every $(n - k + 1)$-tuple of columns is dependent

Now $d(C)$ is the smallest integer d such that

H has d linearly dependent columns

So $d \leq n - k + 1$

Singleton bound

Theorem If C is an $[n, k, d]$ code, then

$$d \leq n - k + 1$$

Proof

Let H be a parity check matrix of C
This is an $(n - k) \times n$ matrix
There exist $n - k + 1$ dependent columns
in fact every $(n - k + 1)$-tuple of columns is dependent
Now $d(C)$ is the smallest integer d such that
H has d linearly dependent columns
So $d \leq n - k + 1$

MDS codes

Definition Let C be a $[n, k, n-k+1]$ code
Then C is called a **maximum distance separable (MDS) code**

From the Singleton bound, an MDS code achieves the maximum possible value for the minimum distance given its length and dimension

Examples

The minimum distance of the zero code of length n is $n+1$, by definition
Hence the zero code has parameters $[n, 0, n+1]$ and is MDS
Its dual is the whole space $\mathbb{F}_q^n$ with parameters $[n, n, 1]$ and is also MDS

The n-fold repetition code has parameters $[n, 1, n]$ and its dual is an $[n, n-1, 2]$ code and both are MDS

MDS codes

Definition Let C be a $[n, k, n-k+1]$ code
Then C is called a **maximum distance separable (MDS) code**

From the Singleton bound, an MDS code achieves the maximum possible value for the minimum distance given its length and dimension

Examples
The minimum distance of the zero code of length n is $n+1$, by definition
Hence the zero code has parameters $[n, 0, n+1]$ and is MDS
Its dual is the whole space $\mathbb{F}_q^n$ with parameters $[n, n, 1]$ and is also MDS

The n-fold repetition code has parameters $[n, 1, n]$ and its dual is an $[n, n-1, 2]$ code and both are MDS

MDS codes

Definition Let C be a $[n, k, n-k+1]$ code
Then C is called a **maximum distance separable (MDS) code**

From the Singleton bound, an MDS code achieves the maximum possible value for the minimum distance given its length and dimension

Examples
The minimum distance of the zero code of length n is $n+1$,
by definition
Hence the zero code has parameters $[n, 0, n+1]$ and is MDS
Its dual is the whole space $\mathbb{F}_q^n$ with parameters $[n, n, 1]$ and is also MDS

The n-fold repetition code has parameters $[n, 1, n]$ and
its dual is an $[n, n-1, 2]$ code and both are MDS

Dual of an MDS code

Proposition

Let C be an $[n, k, d]$ code over $\mathbb{F}_q$

Then the following statements are equivalent:

1. C is an MDS code,
2. every $n - k$ columns of a parity check matrix H of C are linearly independent,
3. every k columns of a generator matrix G of C are linearly independent.

Corollary

The dual of an MDS code is again MDS

Dual of an MDS code

Proposition

Let C be an $[n, k, d]$ code over $\mathbb{F}_q$
Then the following statements are equivalent:

1. C is an MDS code,
2. every $n - k$ columns of a parity check matrix H of C are linearly independent,
3. every k columns of a generator matrix G of C are linearly independent.

Corollary

The dual of an MDS code is again MDS

Vandermonde matrices and MDS codes

Proposition Let $n \leq q$
Let $\mathbf{a} = (a_1, \ldots, a_n)$ be an n-tuple of mutually distinct elements of $\mathbb{F}_q$
Let k be an integer such that $0 \leq k \leq n$
Define the matrix $G_k(\mathbf{a})$ by

$$G_k(\mathbf{a}) = \begin{pmatrix} 1 & \cdots & 1 \\ a_1 & \cdots & a_n \\ \vdots & \ddots & \vdots \\ a_1^{k-1} & \cdots & a_n^{k-1} \end{pmatrix}$$

The code with generator matrix $G_k(\mathbf{a})$ is MDS

Proof
All $k \times k$ submatrices are Vandermonde matrices
and their determinants are not zero

Vandermonde matrices and MDS codes

Proposition Let $n \leq q$
Let $\mathbf{a} = (a_1, \ldots, a_n)$ be an n-tuple of mutually distinct elements of $\mathbb{F}_q$
Let k be an integer such that $0 \leq k \leq n$
Define the matrix $G_k(\mathbf{a})$ by

$$G_k(\mathbf{a}) = \begin{pmatrix} 1 & \cdots & 1 \\ a_1 & \cdots & a_n \\ \vdots & \ddots & \vdots \\ a_1^{k-1} & \cdots & a_n^{k-1} \end{pmatrix}$$

The code with generator matrix $G_k(\mathbf{a})$ is MDS

Proof
All $k \times k$ submatrices are Vandermonde matrices
and their determinants are not zero

Reed-Solomon codes

$$f(X) = f_0 + f_1 X + \cdots + f_i X^i + \cdots + f_{k-1} X^{k-1} \in \mathbb{F}_q[X]$$

	a_1	$\cdots$	a_n	
f_0	1	$\cdots$	1	1
f_1	a_1	$\cdots$	a_n	X
$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
f_i	a_1^i	$\cdots$	a_n^i	X^i
$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
f_{k-1}	a_1^{k-1}	$\cdots$	a_n^{k-1}	X^{k-1}
	$f(a_1)$	$\cdots$	$f(a_n)$	$f(X)$

The linear combination of the rows of $G_k(\mathbf{a})$ is equal to the evaluation of $f(X)$ at $a_1, \ldots, a_n$

Reed-Solomon codes

$$f(X) = f_0 + f_1 X + \cdots + f_i X^i + \cdots + f_{k-1} X^{k-1} \in \mathbb{F}_q[X]$$

	a_1	$\cdots$	a_n	
f_0	1	$\cdots$	1	1
f_1	a_1	$\cdots$	a_n	X
$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
f_i	a_1^i	$\cdots$	a_n^i	X^i
$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
f_{k-1}	a_1^{k-1}	$\cdots$	a_n^{k-1}	X^{k-1}
	$f(a_1)$	$\cdots$	$f(a_n)$	$f(X)$

The linear combination of the rows of $G_k(\mathbf{a})$ is equal to the evaluation of $f(X)$ at $a_1, \ldots, a_n$

Generalized Reed-Solomon codes

$\mathbf{a} = (a_1, \ldots, a_n)$ an n-tuple of mutually distinct elements of $\mathbb{F}_q$
$\mathbf{b} = (b_1, \ldots, b_n)$ an n-tuple of nonzero elements of $\mathbb{F}_q$

$$GRS_k(\mathbf{a}, \mathbf{b}) = \{ (f(a_1)b_1, \ldots, f(a_n)b_n) \mid f(X) \in \mathbb{F}_q[X], \deg(f(X)) < k \}$$

Generator matrix:

$$G_k(\mathbf{a}, \mathbf{b}) = \begin{pmatrix} b_1 & \cdots & b_j & \cdots & b_n \\ a_1 b_1 & \cdots & a_j b_j & \cdots & a_n b_n \\ \vdots & \cdots & \vdots & \cdots & \vdots \\ a_1^{k-1} b_1 & \cdots & a_j^{k-1} b_j & \cdots & a_n^{k-1} b_n \end{pmatrix}$$

MDS code with parameters: $[n, k, n-k+1]$ if $k \leq n$

Generalized Reed-Solomon codes

$\mathbf{a} = (a_1, \ldots, a_n)$ an n-tuple of mutually distinct elements of $\mathbb{F}_q$
$\mathbf{b} = (b_1, \ldots, b_n)$ an n-tuple of nonzero elements of $\mathbb{F}_q$

$$GRS_k(\mathbf{a}, \mathbf{b}) = \{ (f(a_1)b_1, \ldots, f(a_n)b_n) \mid f(X) \in \mathbb{F}_q[X], \deg(f(X)) < k \}$$

Generator matrix:

$$G_k(\mathbf{a}, \mathbf{b}) = \begin{pmatrix} b_1 & \cdots & b_j & \cdots & b_n \\ a_1 b_1 & \cdots & a_j b_j & \cdots & a_n b_n \\ \vdots & \cdots & \vdots & \cdots & \vdots \\ a_1^{k-1} b_1 & \cdots & a_j^{k-1} b_j & \cdots & a_n^{k-1} b_n \end{pmatrix}$$

MDS code with parameters: $[n, k, n-k+1]$ if $k \leq n$

Weight enumerator

Weight enumerator

Let C be a code of length n
The weight spectrum or weight distribution is the set

$$\{(w, A_w) : w = 0, 1, \ldots, n\}$$

where A_w denotes the number of codewords in C of weight w

The weight enumerator is the polynomial:

$$W_C(Z) = \sum_{w=0}^{n} A_w Z^w.$$

The homogeneous weight enumerator is:

$$W_C(X, Y) = \sum_{w=0}^{n} A_w X^{n-w} Y^w.$$

Weight enumerator

Let C be a code of length n
The weight spectrum or weight distribution is the set

$$\{(w, A_w) : w = 0, 1, \ldots, n\}$$

where A_w denotes the number of codewords in C of weight w

The weight enumerator is the polynomial:

$$W_C(Z) = \sum_{w=0}^{n} A_w Z^w.$$

The homogeneous weight enumerator is:

$$W_C(X, Y) = \sum_{w=0}^{n} A_w X^{n-w} Y^w.$$

Example: trivial codes

The zero code has one codeword and its weight is zero
Hence

$$W_{\{0\}}(X, Y) = X^n$$

The number of words of weight w in the trivial code $\mathbb{F}_q^n$ is

$$A_w = \binom{n}{w}(q-1)^w$$

So

$$W_{\mathbb{F}_q^n}(X, Y) = \sum_{w=0}^{n} \binom{n}{w}(q-1)^w X^{n-w} Y^w = (X + (q-1)Y)^n$$

Example: trivial codes

The zero code has one codeword and its weight is zero
Hence

$$W_{\{0\}}(X, Y) = X^n$$

The number of words of weight w in the trivial code $\mathbb{F}_q^n$ is

$$A_w = \binom{n}{w}(q-1)^w$$

So

$$W_{\mathbb{F}_q^n}(X, Y) = \sum_{w=0}^{n} \binom{n}{w}(q-1)^w X^{n-w} Y^w = (X + (q-1)Y)^n$$

Example: repetition and even weight code

The n-fold repetition code C has homogeneous weight enumerator

$$W_C(X, Y) = X^n + (q-1)Y^n$$

In the binary case its dual is the even weight code

Hence it has homogeneous weight enumerator:

$$W_{C^\perp}(X, Y) = \sum_{t=0}^{\lfloor n/2 \rfloor} \binom{n}{2t} X^{n-2t} Y^{2t} = \frac{1}{2}\left((X+Y)^n + (X-Y)^n\right)$$

Example: repetition and even weight code

The n-fold repetition code C has homogeneous weight enumerator

$$W_C(X, Y) = X^n + (q-1)Y^n$$

In the binary case its dual is the even weight code
Hence it has homogeneous weight enumerator:

$$W_{C^\perp}(X, Y) = \sum_{t=0}^{\lfloor n/2 \rfloor} \binom{n}{2t} X^{n-2t} Y^{2t} = \frac{1}{2}\left((X+Y)^n + (X-Y)^n\right)$$

Example: [7, 4, 3] binary Hamming code

The nonzero entries of the weight distribution are

$$A_0 = 1,\ A_3 = 7,\ A_4 = 7,\ A_7 = 1$$

by inspection of all the 16 codewords

Hence its homogeneous weight enumerator is

$$X^7 + 7X^4Y^3 + 7X^3Y^4 + Y^7$$

Example: $[7, 4, 3]$ binary Hamming code

The nonzero entries of the weight distribution are

$$A_0 = 1,\ A_3 = 7,\ A_4 = 7,\ A_7 = 1$$

by inspection of all the 16 codewords
Hence its homogeneous weight enumerator is

$$X^7 + 7X^4Y^3 + 7X^3Y^4 + Y^7$$

Example: simplex code $\mathcal{S}_r(q)$

This is a constant weight code with parameters

$$[(q^r - 1)/(q - 1), r, q^{r-1}]$$

Hence its homogeneous weight enumerator is

$$W_{\mathcal{S}_r(q)}(X, Y) = X^n + (q^r - 1)X^{n-q^{r-1}}Y^{q^{r-1}}$$

Example: simplex code $\mathcal{S}_r(q)$

This is a constant weight code with parameters

$$[(q^r - 1)/(q - 1), r, q^{r-1}]$$

Hence its homogeneous weight enumerator is

$$W_{\mathcal{S}_r(q)}(X, Y) = X^n + (q^r - 1)X^{n-q^{r-1}}Y^{q^{r-1}}$$

MacWilliams identity

Theorem

Let C be a $[n, k]$ code over $\mathbb{F}_q$
Then

$$W_{C^\perp}(X, Y) = q^{-k} W_C(X + (q-1)Y, X - Y)$$

Proof

Several proofs are known
One will be given at the end by means of the Tutte polynomial

MacWilliams identity

Theorem

Let C be a $[n, k]$ code over $\mathbb{F}_q$
Then

$$W_{C^\perp}(X, Y) = q^{-k} W_C(X + (q-1)Y, X - Y)$$

Proof

Several proofs are known
One will be given at the end by means of the Tutte polynomial

Example: dual repetition code

The n-fold repetition code C has homogeneous weight enumerator

$$W_C(X, Y) = X^n + (q-1)Y^n$$

Using MacWilliams identity gives the homogeneous weight enumerator of its dual:

$$\begin{aligned} W_{C^\perp}(X, Y) &= q^{-1} W_C(X + (q-1)Y, X - Y) \\ &= q^{-1}((X + (q-1)Y)^n + (q-1)(X - Y)^n) \end{aligned}$$

$$= \sum_{w=0}^{n} \binom{n}{w} \frac{(q-1)^w + (q-1)(-1)^w}{q} X^{n-w} Y^w$$

Example: dual repetition code

The n-fold repetition code C has homogeneous weight enumerator

$$W_C(X, Y) = X^n + (q-1)Y^n$$

Using MacWilliams identity gives the homogeneous weight enumerator of its dual:

$$\begin{aligned} W_{C^\perp}(X, Y) &= q^{-1} W_C(X + (q-1)Y, X - Y) \\ &= q^{-1}((X + (q-1)Y)^n + (q-1)(X - Y)^n) \end{aligned}$$

$$= \sum_{w=0}^{n} \binom{n}{w} \frac{(q-1)^w + (q-1)(-1)^w}{q} X^{n-w} Y^w$$

Exercises

Exercises first lecture

1. Check MacWilliams identity for the binary $[7, 4, 3]$ Hamming code and its dual the $[7, 3, 4]$ simplex code.
2. Compute the weight enumerators of the ternary Hamming $\mathcal{H}_3(3)$ code and its dual the Simplex $\mathcal{S}_3(3)$ code.
   Show that MacWilliams identity holds.
3. Compute the weight spectrum of the dual of the q-ary n-fold repetition code directly, without using MacWilliams identity.
   Compare this result as given in the lecture.
4. Consider the code with generator matrix $(I_k|I_k)$.
   Show that its weight enumerator is equal $(X^2 + (q-1)Y^2)^k$.
   Show that the code is self dual if and only if q is even.
   Verify that this code is formally self-dual, that is the code and its dual have the same weight enumerator.

Exercises first lecture

5. Let C be the code over $\mathbb{F}_q$ with generator matrix G given by

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

Determine the finite fields $\mathbb{F}_q$ such that the code C contains a word of weight 7?