Arrangements, matroids and codes

second lecture

Ruud Pellikaan
joint work with
Relinde Jurrius

ACAGM summer school
Leuven, Belgium 19 July 2011

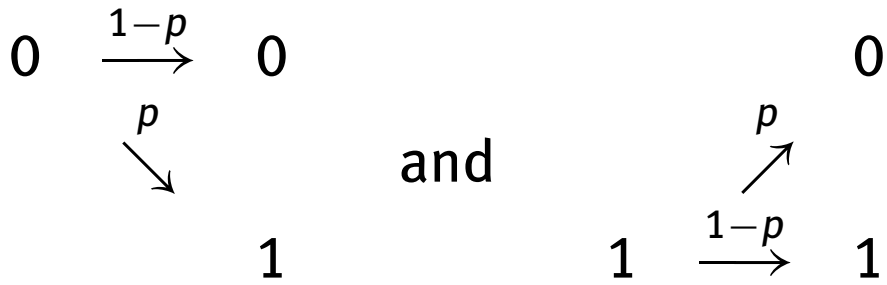
Content second lecture

1. q-ary symmetric channel
   Probability of undetected error
2. Projective systems, arrangements and codes
3. Arrangements and the weight enumerator
4. Exercises

q-ary symmetric channel

The binary symmetric channel (BSC)

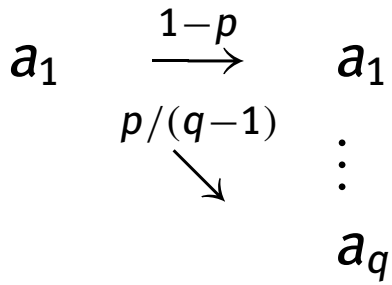
The BSC is a channel where binary words
are sent with independent errors
with the same cross-over probability p
at each coordinate with $0 \leq p \leq \frac{1}{2}$



So a symbol is transmitted correctly with probability $1 - p$

The q-ary symmetric channel (qSC)

The qSC is a channel where q-ary words
are sent with independent errors
with the same cross-over probability p
at each coordinate with $0 \leq p \leq \frac{q-1}{q}$
such that all the $q-1$ wrong symbols
occur with the same probability $p/(q-1)$



So a symbol is transmitted correctly with probability $1-p$

Probability

$P(\mathbf{x})$ is the probability that the codeword $\mathbf{x}$ is sent

Assume that this probability is the same for all codewords

Hence

$$P(\mathbf{x}) = \frac{1}{|C|} \text{ for all } \mathbf{x} \in C$$

$P(\mathbf{y}|\mathbf{x})$ is the probability that $\mathbf{y}$ is received for given $\mathbf{x}$

Then for a q-ary symmetric channel:

$$P(\mathbf{y}|\mathbf{x}) = \left(\frac{p}{q-1}\right)^{d(\mathbf{x},\mathbf{y})} (1-p)^{n-d(\mathbf{x},\mathbf{y})}$$

Probability

$P(\mathbf{x})$ is the probability that the codeword $\mathbf{x}$ is sent

Assume that this probability is the same for all codewords

Hence

$$P(\mathbf{x}) = \frac{1}{|C|} \text{ for all } \mathbf{x} \in C$$

$P(\mathbf{y}|\mathbf{x})$ is the probability that $\mathbf{y}$ is received for given $\mathbf{x}$

Then for a q-ary symmetric channel:

$$P(\mathbf{y}|\mathbf{x}) = \left(\frac{p}{q-1}\right)^{d(\mathbf{x},\mathbf{y})} (1-p)^{n-d(\mathbf{x},\mathbf{y})}$$

Error detection

The parity check matrix can be used for error detection
Useful in a communication channel where one asks for retransmission

Let C be a linear code of minimum distance d and
H is a parity check matrix of C.

Let $\mathbf{c}$ be the codeword $\mathbf{c}$ is transmitted and $\mathbf{r} = \mathbf{c} + \mathbf{e}$ received
Then $\mathbf{e}$ is the error vector and $\mathrm{wt}(\mathbf{e})$ the number of errors

Now $H\mathbf{r}^T = 0$ if there is no error and
$H\mathbf{r}^T \neq 0$ for all $\mathbf{e}$ such that $0 < \mathrm{wt}(\mathbf{e}) < d$
Therefore we can detect any pattern of t errors with $t < d$

The vector $H\mathbf{r}^T$ is called the syndrome of the received word

Error detection

The parity check matrix can be used for error detection
Useful in a communication channel where one asks for retransmission

Let C be a linear code of minimum distance d and
H is a parity check matrix of C.

Let $\mathbf{c}$ be the codeword $\mathbf{c}$ is transmitted and $\mathbf{r} = \mathbf{c} + \mathbf{e}$ received
Then $\mathbf{e}$ is the error vector and $\mathrm{wt}(\mathbf{e})$ the number of errors

Now $H\mathbf{r}^T = 0$ if there is no error and
$H\mathbf{r}^T \neq 0$ for all $\mathbf{e}$ such that $0 < \mathrm{wt}(\mathbf{e}) < d$
Therefore we can detect any pattern of t errors with $t < d$

The vector $H\mathbf{r}^T$ is called the syndrome of the received word

Probability of undetected error

Proposition

Let $W_C(X, Y)$ be the weight enumerator of C
Then the probability of undetected error on a qSC with cross-over probability p is given by

$$P_{ue}(p) = W_C\left(1-p, \frac{p}{q-1}\right) - (1-p)^n.$$

Proof of formula for undetected error

Without loss of generality we may assume that the zero word is sent

$$P_{ue}(p) = \frac{1}{|C|} \sum_{\mathbf{x} \in C} \sum_{\mathbf{x} \neq \mathbf{y} \in C} P(\mathbf{y}|\mathbf{x}) = \sum_{0 \neq \mathbf{y} \in C} P(\mathbf{y}|0).$$

If the received codeword y has weight w
then w symbols are changed and $n - w$ symbols remained the same:

$$P(\mathbf{y}|0) = (1-p)^{n-w} \left(\frac{p}{q-1} \right)^{w}$$

Hence

$$P_{ue}(p) = \sum_{w=1}^{n} A_w (1-p)^{n-w} \left(\frac{p}{q-1} \right)^{w}$$

Substitute $X = 1 - p$ and $Y = p/(q-1)$ in $W_C(X, Y)$

Proof of formula for undetected error

Without loss of generality we may assume that the zero word is sent

$$P_{ue}(p) = \frac{1}{|C|} \sum_{\mathbf{x} \in C} \sum_{\mathbf{x} \neq \mathbf{y} \in C} P(\mathbf{y}|\mathbf{x}) = \sum_{0 \neq \mathbf{y} \in C} P(\mathbf{y}|0).$$

If the received codeword y has weight w
then w symbols are changed and $n - w$ symbols remained the same:

$$P(\mathbf{y}|0) = (1-p)^{n-w} \left(\frac{p}{q-1} \right)^{w}$$

Hence

$$P_{ue}(p) = \sum_{w=1}^{n} A_w (1-p)^{n-w} \left(\frac{p}{q-1} \right)^{w}$$

Substitute $X = 1 - p$ and $Y = p/(q-1)$ in $W_C(X, Y)$

Projective systems arrangements and codes

Projective systems and codes

Let $\mathbb{F}$ be a field
A projective system $\mathcal{P} = (P_1, \ldots, P_n)$ in $\mathbb{P}^r(\mathbb{F})$
is an n-tuple of points P_j in this projective space
such that not all these points lie in a hyperplane

Let $P_j = (p_{0j} : p_{1j} : \ldots : p_{rj})$
Let $G_{\mathcal{P}}$ be the $(r+1) \times n$ matrix with $(p_{0j}, p_{1j}, \ldots, p_{rj})^T$ as j-th column

Then $G_{\mathcal{P}}$ has rank $r+1$, since not all points lie in a hyperplane

If $\mathbb{F}$ is a finite field, then $G_{\mathcal{P}}$ is the generator matrix
of a nondegenerate $[n, r+1, d]$ code over $\mathbb{F}$ where
$n - d$ is the maximal number of points of $\mathcal{P}_G$
that lie in a hyperplane of $\mathbb{P}^{k-1}(\mathbb{F})$

Projective systems and codes

Let $\mathbb{F}$ be a field
A projective system $\mathcal{P} = (P_1, \ldots, P_n)$ in $\mathbb{P}^r(\mathbb{F})$
is an n-tuple of points P_j in this projective space
such that not all these points lie in a hyperplane

Let $P_j = (p_{0j} : p_{1j} : \ldots : p_{rj})$
Let $G_{\mathcal{P}}$ be the $(r+1) \times n$ matrix with $(p_{0j}, p_{1j}, \ldots, p_{rj})^T$ as j-th column

Then $G_{\mathcal{P}}$ has rank $r+1$, since not all points lie in a hyperplane

If $\mathbb{F}$ is a finite field, then $G_{\mathcal{P}}$ is the generator matrix
of a nondegenerate $[n, r+1, d]$ code over $\mathbb{F}$ where
$n - d$ is the maximal number of points of $\mathcal{P}_G$
that lie in a hyperplane of $\mathbb{P}^{k-1}(\mathbb{F})$

Equivalent codes

Let C and D be linear codes in $\mathbb{F}_q^n$

Then C is called permutation equivalent to D
if there exists a permutation matrix Π such that $\Pi(C) = D$
If moreover $C = D$, then Π is called an permutation automorphism of C

The code C is called generalized or monomial equivalent to D
if there exists a monomial matrix M such that $M(C) = D$
If moreover $C = D$, then M is called a monomial automorphismof C

Equivalent codes

Let C and D be linear codes in $\mathbb{F}_q^n$

Then C is called permutation equivalent to D
if there exists a permutation matrix Π such that $\Pi(C) = D$
If moreover $C = D$, then Π is called an permutation automorphism of C

The code C is called generalized or monomial equivalent to D
if there exists a monomial matrix M such that $M(C) = D$
If moreover $C = D$, then M is called a monomial automorphismof C

Codes and projective systems

Conversely:

Let G be a generator matrix of a nondegenerate $[n, k, d]$ code over $\mathbb{F}_q$
Then G has no zero columns
Take the columns of G as homogeneous coordinates
of points in $\mathbb{P}^{k-1}(\mathbb{F}_q)$

This gives the projective system $\mathcal{P}_G$ over $\mathbb{F}_q$ of G

One-to-one correspondence between:
generalized equivalence classes of nondegenerate $[n, k]$ codes over $\mathbb{F}_q$
and
equivalence classes of projective systems of n points in $\mathbb{P}^{k-1}(\mathbb{F}_q)$

Codes and projective systems

Conversely:

Let G be a generator matrix of a nondegenerate $[n, k, d]$ code over $\mathbb{F}_q$
Then G has no zero columns
Take the columns of G as homogeneous coordinates
of points in $\mathbb{P}^{k-1}(\mathbb{F}_q)$

This gives the projective system $\mathcal{P}_G$ over $\mathbb{F}_q$ of G

One-to-one correspondence between:
generalized equivalence classes of nondegenerate $[n, k]$ codes over $\mathbb{F}_q$
and
equivalence classes of projective systems of n points in $\mathbb{P}^{k-1}(\mathbb{F}_q)$

Arrangements

An arrangement in $\mathbb{F}^k$ is an
n-tuple $(H_1, \ldots, H_n)$ of hyperplanes in $\mathbb{F}^k$

The arrangement is called simple
if all the n hyperplanes are mutually distinct

The arrangement is called central if $\mathbf{0} \in H_j$ for all j
If the arrangement is central one considers the hyperplanes in $\mathbb{P}^{k-1}(\mathbb{F})$

A central arrangement is called essential if $\cap_j H_j = \{\mathbf{0}\}$
Projective systems and essential arrangements are dual notions

Arrangements and codes

Let $G = (g_{ij})$ be a generator matrix of a nondegenerate code C of dimension k
So G has no zero columns

Let H_j be the linear hyperplane in $\mathbb{F}_q^k$ with equation

$$g_{1j}X_1 + \cdots + g_{kj}X_k = 0.$$

$\mathcal{A}_G$ is the arrangement $(H_1, \ldots, H_n)$ associated with G

Arrangements, projective systems and codes

There is a one-to-one correspondence between:

1. generalized equivalence classes of nondegenerate $[n, k]$ codes over $\mathbb{F}_q$
2. equivalence classes of projective systems of n points in $\mathbb{P}^{k-1}(\mathbb{F}_q)$
3. equivalence classes of essential arrangements of n hyperplanes in $\mathbb{P}^{k-1}(\mathbb{F}_q)$

Arrangements, codes and minimal weight

Proposition

Let C be a nondegenerate code over $\mathbb{F}_q$ with generator matrix G
Let $\mathbf{c}$ be a codeword $\mathbf{c} = \mathbf{x}G$ for the unique $\mathbf{x} \in \mathbb{F}_q^k$

Then $n - \mathrm{wt}(\mathbf{c})$ is equal to the number of hyperplanes of $\mathcal{A}_G$ through $\mathbf{x}$

Proof

Now $c_j = \sum_i g_{ij} x_i$
So $c_j = 0$ if and only if $\mathbf{x} \in H_j$
Hence

$$n - \mathrm{wt}(\mathbf{c}) = |\{j : c_j = 0\}| = |\{j : \mathbf{x} \in H_j\}|$$

Arrangements, codes and minimal weight

Proposition

Let C be a nondegenerate code over $\mathbb{F}_q$ with generator matrix G
Let $\mathbf{c}$ be a codeword $\mathbf{c} = \mathbf{x}G$ for the unique $\mathbf{x} \in \mathbb{F}_q^k$

Then $n - \mathrm{wt}(\mathbf{c})$ is equal to the number of hyperplanes of $\mathcal{A}_G$ through $\mathbf{x}$

Proof

Now $c_j = \sum_i g_{ij} x_i$
So $c_j = 0$ if and only if $\mathbf{x} \in H_j$
Hence

$$n - \mathrm{wt}(\mathbf{c}) = |\{j : c_j = 0\}| = |\{j : \mathbf{x} \in H_j\}|$$

Projective codes

Let G be a generator matrix of C
Remember:
a code C is nondegenerate if and only if
G has no zero column if and only if
$d(C^{\perp}) \geq 2$

A code C is called projective if $d(C^{\perp}) \geq 3$

The following statements are equivalent:

1. C is projective
2. $d(C^{\perp}) \geq 3$
3. C is nondegenerate and the points of $\mathcal{P}_G$ are mutually distinct
4. C is nondegenerate and the hyperplanes of $\mathcal{A}_G$ are mutually distinct

Projective codes

Let G be a generator matrix of C
Remember:
a code C is nondegenerate if and only if
G has no zero column if and only if
$d(C^{\perp}) \geq 2$

A code C is called projective if $d(C^{\perp}) \geq 3$

The following statements are equivalent:

1. C is projective
2. $d(C^{\perp}) \geq 3$
3. C is nondegenerate and the points of $\mathcal{P}_G$ are mutually distinct
4. C is nondegenerate and the hyperplanes of $\mathcal{A}_G$ are mutually distinct

Arrangements and weight enumerator

Arrangements and weight enumerator

A_w the number of codewords of weight w equals
the number of points that are on exactly $n - w$ of the hyperplanes of $\mathcal{A}_G$

In particular A_n is equal to the number of points that is in
the complement of the union of these hyperplanes in $\mathbb{F}_q^k$

This number can be computed by the principle of inclusion/exclusion:

$$\begin{aligned} A_n &= q^k - |H_1 \cup \cdots \cup H_n| \\ &= q^k + \sum_{w=1}^{n} (-1)^w \sum_{i_1 < \cdots < i_w} |H_{i_1} \cap \cdots \cap H_{i_w}|. \end{aligned}$$

Arrangements and weight enumerator

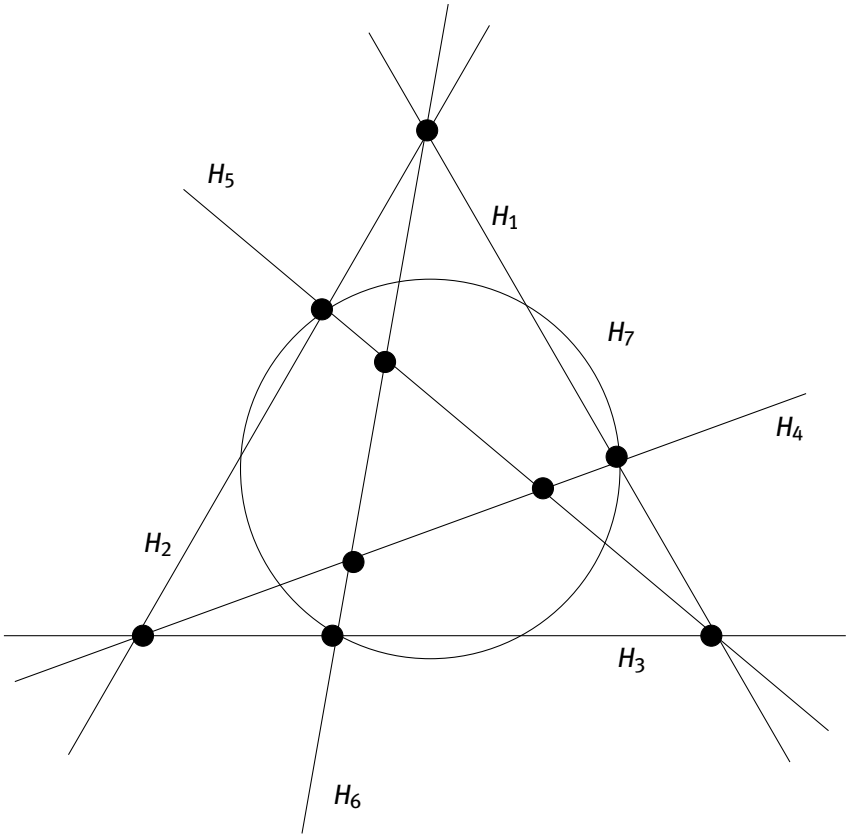
A_w the number of codewords of weight w equals
the number of points that are on exactly $n - w$ of the hyperplanes of $\mathcal{A}_G$

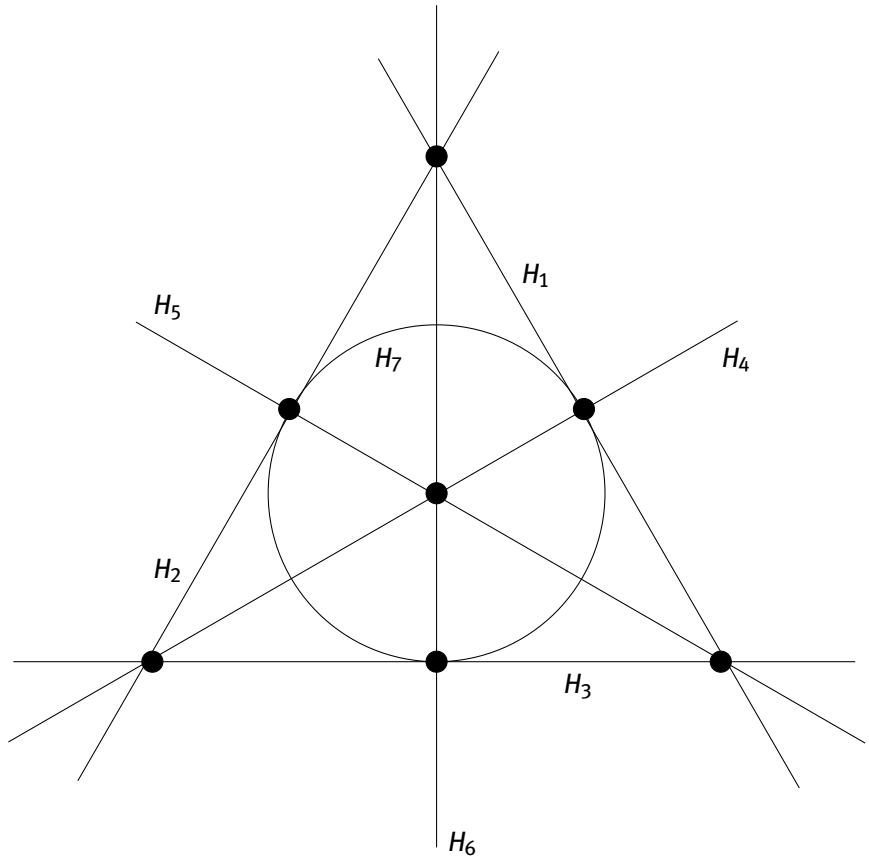
In particular A_n is equal to the number of points that is in
the complement of the union of these hyperplanes in $\mathbb{F}_q^k$

This number can be computed by the principle of inclusion/exclusion:

$$\begin{aligned} A_n &= q^k - |H_1 \cup \cdots \cup H_n| \\ &= q^k + \sum_{w=1}^{n} (-1)^w \sum_{i_1 < \cdots < i_w} |H_{i_1} \cap \cdots \cap H_{i_w}|. \end{aligned}$$

Example





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

Example, q even

Let C be the code over $\mathbb{F}_q$ with generator matrix G
For $q = 2$, this is the simplex code $\mathcal{S}_2(2)$
The columns of G represent also the coefficients of the lines of $\mathcal{A}_G$

Assume q is even
$A_0 = 1$
$A_4 = 7(q-1)$ there are 7 points on exactly 3 lines
$A_6 = 7(q-1)[(q+1)-3] = 7(q-1)(q-2)$ there are 7 lines
and $(q+1)-3$ points of such a line is exactly on one of these
$A_7 = q^3 - A_0 - A_4 - A_6 = (q-1)(q-2)(q-4)$
So

$$W_C(X,Y) = X^7 + 7(q-1)X^3Y^4 + 7(q-1)(q-2)XY^6 + (q-1)(q-2)(q-4)Y^7$$

Example, q even

Let C be the code over $\mathbb{F}_q$ with generator matrix G
For $q = 2$, this is the simplex code $\mathcal{S}_2(2)$
The columns of G represent also the coefficients of the lines of $\mathcal{A}_G$

Assume q is even
$A_0 = 1$
$A_4 = 7(q-1)$ there are 7 points on exactly 3 lines
$A_6 = 7(q-1)[(q+1)-3] = 7(q-1)(q-2)$ there are 7 lines
and $(q+1)-3$ points of such a line is exactly on one of these
$A_7 = q^3 - A_0 - A_4 - A_6 = (q-1)(q-2)(q-4)$
So

$$W_C(X,Y) = X^7 + 7(q-1)X^3Y^4 + 7(q-1)(q-2)XY^6 + (q-1)(q-2)(q-4)Y^7$$

Example, q odd

Assume q is odd

$A_0 = 1$

$A_4 = 6(q-1)$ there are 6 points on exactly 3 lines

$A_5 = 3(q-1)$ there are 3 points on exactly 2 lines

$A_6 = (q-1)[4((q+1)-3)+3((q+1)-4)] = (q-1)(7q-17)$ there are 7 lines

4 of them have $(q+1)-3$ points that are exactly on one of these 7

3 of them have $(q+1)-4$ points that are exactly on one of these 7

$A_7 = q^3 - A_0 - A_4 - A_5 - A_6 = (q-1)(q-3)^2$

Hence

$$W_C(X,Y) =$$

$$X^7+6(q-1)X^3Y^4+3(q-1)X^2Y^5+(q-1)(7q-17)XY^6+(q-1)(q-3)^2Y^7$$

Example, q odd

Assume q is odd

$A_0 = 1$

$A_4 = 6(q-1)$ there are 6 points on exactly 3 lines

$A_5 = 3(q-1)$ there are 3 points on exactly 2 lines

$A_6 = (q-1)[4((q+1)-3)+3((q+1)-4)] = (q-1)(7q-17)$
there are 7 lines

4 of them have $(q+1)-3$ points that are exactly on one of these 7

3 of them have $(q+1)-4$ points that are exactly on one of these 7

$A_7 = q^3 - A_0 - A_4 - A_5 - A_6 = (q-1)(q-3)^2$

Hence

$$W_C(X,Y) =$$

$$X^7+6(q-1)X^3Y^4+3(q-1)X^2Y^5+(q-1)(7q-17)XY^6+(q-1)(q-3)^2Y^7$$

A formalism for the weight enumerator

The following method is based on Katsman-Tsfasman
Later we will encounter another method:
matroids and the Tutte polynomial

Definition

For a subset J of $[n] := \{1, 2, \ldots, n\}$ define

$$\begin{aligned} C(J) &= \{\mathbf{c} \in C : c_j = 0 \text{ for all } j \in J\} \\ l(J) &= \dim C(J) \\ B_J &= q^{l(J)} - 1 \\ B_t &= \sum_{|J|=t} B_J . \end{aligned}$$

A formalism for the weight enumerator

The following method is based on Katsman-Tsfasman
Later we will encounter another method:
matroids and the Tutte polynomial

Definition
For a subset J of $[n] := \{1, 2, \ldots, n\}$ define

$$\begin{aligned} C(J) &= \{\mathbf{c} \in C : c_j = 0 \text{ for all } j \in J\} \\ l(J) &= \dim C(J) \\ B_J &= q^{l(J)} - 1 \\ B_t &= \sum_{|J|=t} B_J. \end{aligned}$$

Remark on $C(J)$

The encoding map $\mathbf{x} \mapsto \mathbf{x}G = \mathbf{c}$
from vectors $\mathbf{x} \in \mathbb{F}_q^k$ to codewords
gives the following isomorphism of vector spaces

$$\bigcap_{j \in J} H_j \cong C(J)$$

Furthermore B_J is equal to the number of nonzero codewords $\mathbf{c}$
that are zero at all j in J
and this is equal to the number of nonzero
elements of the intersection $\bigcap_{j \in J} H_j$.

Remark on $C(J)$

The encoding map $\mathbf{x} \mapsto \mathbf{x}G = \mathbf{c}$
from vectors $\mathbf{x} \in \mathbb{F}_q^k$ to codewords
gives the following isomorphism of vector spaces

$$\bigcap_{j \in J} H_j \cong C(J)$$

Furthermore B_J is equal to the number of nonzero codewords $\mathbf{c}$
that are zero at all j in J
and this is equal to the number of nonzero
elements of the intersection $\bigcap_{j \in J} H_j$.

l(J) and r(J)

Lemma

Let C be a linear code with generator matrix G
Let $J \subseteq [n]$ and $|J| = t$
G_J is the $k \times t$ submatrix of G existing of the columns of G indexed by J
Let $r(J)$ be the rank of G_J
Then $l(J) = k - r(J)$

Proof

Let C_J be the code generated by G_J
Consider the projection map $\pi : C \to \mathbb{F}_q^t$
given by deleting the coordinates that are not indexed by J
Then π is a linear map, the image of C under π is C_J
and the kernel is $C(J)$ by definition
Hence $\dim C_J + \dim C(J) = \dim C$
So $l(J) = k - r(J)$

l(J) and r(J)

Lemma

Let C be a linear code with generator matrix G
Let $J \subseteq [n]$ and $|J| = t$
G_J is the $k \times t$ submatrix of G existing of the columns of G indexed by J
Let $r(J)$ be the rank of G_J
Then $l(J) = k - r(J)$

Proof

Let C_J be the code generated by G_J
Consider the projection map $\pi : C \to \mathbb{F}_q^t$
given by deleting the coordinates that are not indexed by J
Then π is a linear map, the image of C under π is C_J
and the kernel is $C(J)$ by definition
Hence $\dim C_J + \dim C(J) = \dim C$
So $l(J) = k - r(J)$

Lemma on $l(J)$ and B_t

Lemma

Let C be an $\mathbb{F}_q$-linear code of dimension k
Let d and $d^\perp$ be the minimum distance of C and $C^\perp$, respectively
Let $J \subseteq [n]$ and $|J| = t$
Then

$$l(J) = \begin{cases} k - t & \text{for all } t < d^\perp \\ 0 & \text{for all } t > n - d \end{cases}$$

and

$$B_t = \begin{cases} \binom{n}{t}(q^{k-t} - 1) & \text{for all } t < d^\perp \\ 0 & \text{for all } t > n - d \end{cases}$$

Proof of Lemma on $l(J)$ and B_t

1. Let $t > n - d$ and let $\mathbf{c} \in C(J)$
Then J is contained in the complement of $\mathrm{supp}(\mathbf{c})$
So $t \leq n - \mathrm{wt}(\mathbf{c})$
Hence $\mathrm{wt}(\mathbf{c}) \leq n - t < d$ and $\mathbf{c} = \mathbf{0}$
Therefore $l(J) = 0$

2. Let G be a generator matrix for C
then G is a parity check matrix for $C^{\perp}$
Now $l(J) = k - r(J)$ where $r(J)$ is the rank of the matrix G_J
Let $t < d^{\perp}$, then every t-tuple of columns of G is linearly independent
So $r(J) = t$ and $l(J) = k - t$

Proof of Lemma on $l(J)$ and B_t

1. Let $t > n - d$ and let $\mathbf{c} \in C(J)$
Then J is contained in the complement of $\mathrm{supp}(\mathbf{c})$
So $t \leq n - \mathrm{wt}(\mathbf{c})$
Hence $\mathrm{wt}(\mathbf{c}) \leq n - t < d$ and $\mathbf{c} = \mathbf{0}$
Therefore $l(J) = 0$

2. Let G be a generator matrix for C
then G is a parity check matrix for $C^{\perp}$
Now $l(J) = k - r(J)$ where $r(J)$ is the rank of the matrix G_J
Let $t < d^{\perp}$, then every t-tuple of columns of G is linearly independent
So $r(J) = t$ and $l(J) = k - t$

Relating B_t to the A_w's

Proposition

B_t relates to the weight distribution as follows:

$$B_t = \sum_{w=d}^{n-t} \binom{n-w}{t} A_w$$

Proof

Count in two ways the number of elements of the set

$$\{(J, \mathbf{c}) : J \subseteq [n], |J| = t, \mathbf{c} \in C(J), \mathbf{c} \neq 0\}$$

Relating B_t to the A_w's

Proposition

B_t relates to the weight distribution as follows:

$$B_t = \sum_{w=d}^{n-t} \binom{n-w}{t} A_w$$

Proof

Count in two ways the number of elements of the set

$$\{(J, \mathbf{c}) : J \subseteq [n], |J| = t, \mathbf{c} \in C(J), \mathbf{c} \neq 0\}$$

Relating $W_C(X, Y)$ to the B_t's

Theorem

The generalize weight enumerator is given by the following formula:

$$W_C(X, Y) = X^n + \sum_{t=0}^{n} B_t (X - Y)^t Y^{n-t}$$

Proof

Use the previous proposition
the fact that $B_t = 0$ for $t > n - d$
change the order of summation and
use the binomial expansion:

$$X^{n-w} = ((X - Y) + Y)^{n-w}$$

Relating $W_C(X, Y)$ to the B_t's

Theorem

The generalize weight enumerator is given by the following formula:

$$W_C(X, Y) = X^n + \sum_{t=0}^{n} B_t (X - Y)^t Y^{n-t}$$

Proof

Use the previous proposition
the fact that $B_t = 0$ for $t > n - d$
change the order of summation and
use the binomial expansion:

$$X^{n-w} = ((X - Y) + Y)^{n-w}$$

Proof of relation $W_C(X, Y)$ and B_t's

$$X^n + \sum_{t=0}^{n-d} B_t (X-Y)^t Y^{n-t} = X^n + \sum_{t=0}^{n-d} \sum_{w=0}^{n} \binom{n-w}{t} A_w (X-Y)^t Y^{n-t}$$

$$= X^n + \sum_{w=d}^{n} A_w \left(\sum_{t=0}^{n-w} \binom{n-w}{t} (X-Y)^t Y^{n-w-t} \right) Y^w$$

$$= X^n + \sum_{w=d}^{n} A_w X^{n-w} Y^w$$

$$= W_C(X, Y)$$

In the second step, we let the summation over t run to $n-w$ instead of n because $\binom{n-w}{t} = 0$ for $t > n-w$

Relating A_w to the B_t's

Proposition

The following formula holds:

$$A_w = \sum_{t=n-w}^{n} (-1)^{n+w+t} \binom{t}{n-w} B_t.$$

Proof

There are several ways to prove this proposition

One is to reverse the argument of the previous Theorem

A second proof is by the following general lemma

Relating A_w to the B_t's

Proposition

The following formula holds:

$$A_w = \sum_{t=n-w}^{n} (-1)^{n+w+t} \binom{t}{n-w} B_t.$$

Proof

There are several ways to prove this proposition
One is to reverse the argument of the previous Theorem
A second proof is by the following general lemma

A Lemma

Lemma

Let V be a vector space of dimension $n+1$
Let $\mathbf{a} = (a_0, \ldots, a_n)$ and $\mathbf{b} = (b_0, \ldots, b_n)$ be vectors in V
Then the following formulas are equivalent:

$$a_j = \sum_{i=0}^{n} \binom{i}{j} b_i, \qquad b_j = \sum_{i=j}^{n} (-1)^{i+j} \binom{i}{j} a_i.$$

Proof

This is left as an exercise

A Lemma

Lemma

Let V be a vector space of dimension $n+1$
Let $\mathbf{a} = (a_0, \ldots, a_n)$ and $\mathbf{b} = (b_0, \ldots, b_n)$ be vectors in V
Then the following formulas are equivalent:

$$a_j = \sum_{i=0}^{n} \binom{i}{j} b_i, \qquad b_j = \sum_{i=j}^{n} (-1)^{i+j} \binom{i}{j} a_i.$$

Proof

This is left as an exercise

Weight enumerator of MDS codes

Proposition

The weight distribution of an MDS code of length n and dimension k is given by

$$A_w = \binom{n}{w} \sum_{j=0}^{w-d} (-1)^j \binom{w}{j} \left(q^{w-d+1-j} - 1\right)$$

for $w \geq d = n - k + 1$

Proof wt enum. of MDS codes

Let C be an $[n, k, n-k+1]$ MDS code
Then its dual is also an MDS code with parameters $[n, n-k, k+1]$
Then $B_t = \binom{n}{t}\left(q^{k-t}-1\right)$ for all $t < d^{\perp} = k+1$
and $B_t = 0$ for all $t > n-d = k-1$
Hence

$$A_w = \sum_{t=n-w}^{n-d} (-1)^{n+w+t} \binom{t}{n-w}\binom{n}{t}\left(q^{k-t}-1\right)$$

Make the substitution $j = t-n+w$
Then the summation is from $j = 0$ to $j = w-d$
Furthermore

$$\binom{t}{n-w}\binom{n}{t} = \binom{n}{w}\binom{w}{j}$$

This gives the formula for A_w

Proof wt enum. of MDS codes

Let C be an $[n, k, n-k+1]$ MDS code
Then its dual is also an MDS code with parameters $[n, n-k, k+1]$
Then $B_t = \binom{n}{t}\left(q^{k-t}-1\right)$ for all $t < d^{\perp} = k+1$
and $B_t = 0$ for all $t > n-d = k-1$
Hence

$$A_w = \sum_{t=n-w}^{n-d} (-1)^{n+w+t} \binom{t}{n-w}\binom{n}{t}\left(q^{k-t}-1\right)$$

Make the substitution $j = t-n+w$
Then the summation is from $j = 0$ to $j = w-d$
Furthermore

$$\binom{t}{n-w}\binom{n}{t} = \binom{n}{w}\binom{w}{j}$$

This gives the formula for A_w

Exercises

Exercises second lecture

1. Compute the error probability of undetected error of the binary triple repetition code.
2. Compute the error probability of undetected error of the binary $[7, 4, 3]$ Hamming code.
3. Compare the complexity of the methods exhaustive search and the formalism with the $l(J)$ to compute the weight enumerator as a function of q and the parameters $[n, k, d]$ and $d^{\perp}$.
4. Consider the square matrices A and B of size $n + 1$ with entries a_{ij} and b_{ij}, respectively given by

$$a_{ij} = (-1)^{i+j} \binom{i}{j}, \quad \text{and} \quad b_{ij} = \binom{i}{j} \quad \text{for } 0 \leq i, j \leq n.$$

Show that A and B are inverses of each other.

Exercises second lecture

5. Give a classification of the generalized equivalence classes of all codes of length at most 5
6. Let C be the code over $\mathbb{F}_q$ with generator matrix G given by

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 2 & 3 \\ 0 & 1 & 0 & 3 & 1 & 2 \\ 0 & 0 & 1 & 2 & 3 & 1 \end{pmatrix}$$

Give a picture of the projective arrangement $\mathcal{A}_G$ of lines in the projective plane
Compute the weight enumerator of this code in two ways:
by considering the picture of $\mathcal{A}_G$, and by computing all $l(J)$
Hint: make a distinction between the cases
i) characteristic $p = 2$ or $p = 3$
ii) $p \neq 2$ and $p \neq 3$