Application of hyperplane arrangements to weight enumeration

Relinde Jurrius
(joint work with Ruud Pellikaan)

Université de Neuchâtel

May 25, 2015
Coding theory

message → channel → message

noise
Coding theory

encoding

message → codeword → channel → received word

noise

decoding

message
Coding theory

**Code** Set of codewords (≈ vectors) of fixed length $n$.

$d(x, y)$ The number of places on which two vectors differ.

$d$ The minimal distance between codewords.
Coding theory

**Code**  Set of codewords (≈ vectors) of fixed length $n$.

$d(x, y)$  The number of places on which two vectors differ.

$d$  The minimal distance between codewords.

**Linear code**  Linear subspace $C \subseteq \mathbb{F}_q^n$ of dimension $k$.

**Generator matrix**  Some $k \times n$ matrix $G$ whose rows span $C$. 
Coding theory

Example

The [7, 4] Hamming code over $\mathbb{F}_2$ has generator matrix

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

The minimum distance is 3.
Codes are equivalent if generator matrices are the same up to

- left multiplication by nonsingular $k \times k$ matrix over $\mathbb{F}_q$ (i.e., same rowspace);
- permutation of columns;
- multiplication of column by element of $\mathbb{F}_q^*$. 

We restrict to projective codes: they have generator matrix where

- no column is zero;
- no column is a multiple of another column.

So, all columns coordinatize a different projective point.
Coding theory

Codes are equivalent if generator matrices are the same up to

- left multiplication by nonsingular $k \times k$ matrix over $\mathbb{F}_q$ (i.e., same rowspace);
- permutation of columns;
- multiplication of column by element of $\mathbb{F}_q^*$.

We restrict to projective codes: they have generator matrix where

- no column is zero;
- no column is a multiple of another column.

So, all columns coordinatize a different projective point.
Weight enumeration

**Weight**  The number of nonzero coordinates in a vector.

For linear codes: minimum distance $=$ minimum nonzero weight.
Weight enumeration

**Weight**  The number of nonzero coordinates in a vector.

For linear codes: minimum distance = minimum nonzero weight.

### Weight enumerator

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

where \(A_w = \text{number of words of weight } w\).
Example

The [7, 4] Hamming code over $\mathbb{F}_2$ has generator matrix

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

The weight enumerator is equal to

$$W_C(X, Y) = X^7 + 7X^4Y^3 + 7X^3Y^4 + Y^7.$$
Weight enumeration

**Extension code**  \([n, k] \text{ code } C \otimes \mathbb{F}_{q^m} \text{ over some extension field } \mathbb{F}_{q^m} \text{ generated by the words of } C.\)

**Generator matrix**  All extension codes of \(C\) have generator matrix \(G\).
Extension code \([n, k]\) code \(C \otimes \mathbb{F}_{q^m}\) over some extension field \(\mathbb{F}_{q^m}\) generated by the words of \(C\).

Generator matrix All extension codes of \(C\) have generator matrix \(G\).

Extended weight enumerator

\[
W_C(X, Y, T) = \sum_{w=0}^{n} A_w(T)X^{n-w}Y^w,
\]

where \(A_w(q^m) = \) number of words of weight \(w\) in \(C \otimes \mathbb{F}_{q^m}\).

Fact: the \(A_w(T)\) are polynomials of degree at most \(k\).
The $[7, 4]$ Hamming code has extended weight enumerator

$$W_C(X, Y, T) = X^7 + 7(T - 1)X^4Y^3 + 7(T - 1)X^3Y^4 + 21(T - 1)(T - 2)X^2Y^5 + 7(T - 1)(T - 2)(T - 3)XY^6 + (T - 1)(T^3 - 6T^2 + 15T - 13)Y^7$$
Why do we study this?

The extended weight enumerator is interesting because:

- Determines the probability of undetected error in error-detection.
- Determines the probability of decoding error in bounded distance decoding.
- Connection to Tutte polynomial in matroid theory.
- Connection to zeta function of (algebraic geometric) codes.

... and of course because it is an invariant of linear codes.
Weight enumeration

\[ m \times 1 \times k \times k \times n \times 1 \times n = 0 \]

- Message \( m \)
- Generator matrix \( G \)
- Codeword \( c \)
Weight enumeration

Theorem

\[ c_j = 0 \iff m \text{ lies in hyperplane } H_j \]

Weight enumeration = counting points in (intersections of) hyperplanes.
Columns of a generator matrix $G$ of a linear $[n, k]$ code form a linear hyperplane arrangement in $\mathbb{F}_q^k$. Notation: $(H_1, \ldots, H_n)$.

- One-to-one correspondence between equivalence classes.
- Independent of choice of $G$, so notation: $A_C$.
- Also valid over an extension field $\mathbb{F}_q^m$.

**Theorem**

$$A_w(T) = \text{number of points from vectorspace over field of } T \text{ elements that are on } n - w \text{ hyperplanes}.$$
Let $q > 2$ and $C$ generated by

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

where $a \neq 0, 1$. 

The extended weights are given by

$$A_0(T) = 1$$

The zero word is on all hyperplanes.
Codes and hyperplane arrangements

Example

Let $q > 2$ and $C$ generated by

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

where $a \neq 0, 1$.

The extended weights are given by

$$A_1(T) = 0$$

No points are on 5 hyperplanes.
Codes and hyperplane arrangements

Example

Let $q > 2$ and $C$ generated by

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

where $a \neq 0, 1$.

The extended weights are given by

$$A_2(T) = T - 1$$

One projective point is on 4 hyperplanes.
Let $q > 2$ and $C$ generated by

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

where $a \neq 0, 1$.

The extended weights are given by

$$A_3(T) = T - 1$$

One projective point is on 3 hyperplanes.
Let $q > 2$ and $C$ generated by

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

where $a \neq 0, 1$.

The extended weights are given by

$$A_4(T) = 6(T - 1)$$

Six projective points are on 2 hyperplanes.
Let $q > 2$ and $C$ generated by

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

where $a \neq 0, 1$.

The extended weights are given by

$$A_5(T) = (6(T + 1) - 1 \cdot 4 - 1 \cdot 3 - 6 \cdot 2)(T - 1) = (6T - 13)(T - 1)$$

Six lines with $T + 1$ points; minus the points counted before.
Let $q > 2$ and $C$ generated by

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

where $a \neq 0, 1$.

The extended weights are given by

$$A_6(T) = (T - 1)(T - 2)(T - 3)$$

The total number of projective points is $T^2 + T + 1$. 
To formalize this counting, we use the geometric lattice associated to the arrangement. Notation: $L$.

**Elements**  All intersections of hyperplanes

**Ordering**  $x \leq y$ if $y \subseteq x$

**Minimum**  Whole space $\mathbb{F}_q^k$

**Maximum**  Zero vector $0 \in \mathbb{F}_q^k$

**Rank**  Codimension of $x$ in $\mathbb{F}_q^k$

**Atoms**  The hyperplanes of the arrangement
Geometric lattice

Möbius function

For all $x \leq y$, we have $\mu_L(x, x) = 0$ and

$$\sum_{x \leq z \leq y} \mu_L(x, z) = \sum_{x \leq z \leq y} \mu_L(z, y) = 0.$$ 

Characteristic polynomial

$$\chi_L(T) = \sum_{x \in L} \mu_L(\hat{0}, x) T^{r(L) - r(x)}$$
Geometric lattice

Example
The coboundary of a geometric lattice is defined by

\[ \chi_L(S, T) = \sum_{x \in L} \sum_{x \leq y \in L} \mu_L(x, y) S^{a(x)} T^{r(L) - r(y)} \]

where \( a(x) \) is the number of atoms smaller than \( x \).

We write:

\[ \chi_L(S, T) = \sum_{i=0}^{n} S^i \chi_i(T), \text{ with } \chi_i(T) = \sum_{x \in L \atop a(x) = i} \chi_{[x, \hat{x}]}(T). \]
Coboundary polynomial

\textbf{Theorem}

\[ \chi_i(T) = A_{n-i}(T) \]

\textbf{Proof:}

For every point in \( \mathbb{F}_{q^m}^k \) there is a unique biggest element of \( L \) that contains the point.

\[ A_{n-i}(q^m) = \text{number of points in } \mathbb{F}_{q^m}^k \text{ on exactly } i \text{ hyperplanes} \]

\[ = \sum_{x \in L} \text{number of points in } \mathbb{F}_{q^m}^k \text{ in } x \text{ but not in any } y > x \text{ with } a(x) = i \]
Coboundary polynomial

Well-known fact:

$$\chi_L(q^m) = \text{number of points in } \mathbb{F}_{q^m}^k \text{ not in the arrangement}$$

$$= \text{number of points in } \mathbb{F}_{q^m}^k \text{ in } \hat{0} \text{ but not in any } y > \hat{0}$$

This means that:

$$A_{n-i}(q^m) = \sum_{\substack{x \in L \\ a(x) = i}} \text{ number of points in } \mathbb{F}_{q^m}^k \text{ in } x \text{ but not in any } y > x$$

$$= \sum_{\substack{x \in L \\ a(x) = i}} \chi_{[x, \hat{1}]}(q^m)$$

$$= \chi_i(q^m)$$

So by interpolation, $$\chi_i(T) = A_{n-i}(T)$$. \[\square\]
Summary

- Codes are linear subspaces of $\mathbb{F}_q^n$.
- Extending the underlying field gives extension codes $C \otimes \mathbb{F}_{q^m}$, and we define the extended weight enumerator $W_C(X, Y, T)$.
- By viewing the columns of $G$ as hyperplanes, we associate an arrangement to a code.
- Finding the extended weight enumerator means counting points in intersections of hyperplanes.
- This counting can be done using the geometric lattice associated with the arrangement.
- The coboundary polynomial is equivalent to the extended weight enumerator.
Thank you for your attention.