Classifying polynomials of linear codes and hyperplane arrangements

Relinde Jurrius

Eindhoven University of Technology, The Netherlands

NATO-ASI on Information Security and Related Combinatorics, May 31 – June 11 2010, Opatija, Croatia
Outline

Extended weight enumerator

Hyperplane arrangements

Determination of extended weight enumerator

Geometric lattices and the coboundary polynomial

Summary
Extended weight enumerator

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

Generator matrix All the extension codes of \(C\) have the same generator matrix \(G\).
Extended weight enumerator

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

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

Extended weight enumerator

The homogeneous polynomial counting the number of words of a given weight “for all extension codes”, notation:

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

Note that with \(T = q^m\) we have \(W_C(X, Y, q^m) = W_{C \otimes \mathbb{F}_{q^m}}(X, Y)\).
Hyperplane arrangements

Arrangement of hyperplanes \( n \)-tuple of hyperplanes in \( \mathbb{F}_q^k \).

Essential arrangement Intersection of all hyperplanes is \( \{0\} \), hyperplanes are in \( \mathbb{P}^{k-1}(\mathbb{F}_q) \).
Hyperplane arrangements

Arrangement of hyperplanes \( n \)-tuple of hyperplanes in \( \mathbb{F}_q^k \).

Essential arrangement Intersection of all hyperplanes is \( \{0\} \), hyperplanes are in \( \mathbb{P}^{k-1}(\mathbb{F}_q) \).

Columns of a generator matrix \( G \) of a linear \([n,k]\) code form a hyperplane arrangement. Notation: \((H_1, \ldots, H_n)\).

- One-to-one correspondence between equivalence classes.
- Independent of choice of \( G \), so notation: \( A_G \).
- Also valid over an extension field \( \mathbb{F}_{q^m} \).
Hyperplane arrangements

**Theorem**

Let $C$ be a linear $[n, k]$ code with generator matrix $G$ and $x \in \mathbb{F}_q^k$. Then for every word $c = xG$ we have that $n - wt(c)$ is equal to the number of hyperplanes in $A_C$ through $x$.
Hyperplane arrangements

Theorem

Let $C$ be a linear $[n, k]$ code with generator matrix $G$ and $x \in \mathbb{F}_q^k$. Then for every word $c = xG$ we have that $n - \text{wt}(c)$ is equal to the number of hyperplanes in $\mathcal{A}_C$ through $x$.

To find the extended weight enumerator of $C$, we have to look at the intersections of the hyperplanes in the arrangement $\mathcal{A}_C$. 
Example

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

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

Use that $A_w(T)$ is the number of points on $n - w$ hyperplanes.

The extended weights are given by

$$A_0(T) = 1$$

The zero word is on all hyperplanes.
Example

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

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

Use that $A_w(T)$ is the number of points on $n - w$ hyperplanes.

The extended weights are given by

$$A_1(T) = A_2(T) = 0$$

No points are on 6 or 5 hyperplanes.
Let $q > 2$ and $C$ generated by

\[ G = \begin{pmatrix}
1 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 1 & 1 \\
0 & 0 & 1 & -1 & 0 & 1 & 1
\end{pmatrix}. \]

Use that $A_w(T)$ is the number of points on $n - w$ hyperplanes.

The extended weights are given by

\[ A_3(T) = 2(T - 1) \]

Two projective points are on 4 hyperplanes.
Determination of extended weight enumerator

Example

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

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

Use that $A_w(T)$ is the number of points on $n - w$ hyperplanes.

The extended weights are given by

$$A_4(T) = 3(T - 1)$$

Three projective points are on 3 hyperplanes.
Determination of extended weight enumerator

Example

Let \( q > 2 \) and \( C \) generated by

\[
G = \begin{pmatrix}
1 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 1 & 1 \\
0 & 0 & 1 & -1 & 0 & 1 & 1
\end{pmatrix}.
\]

Use that \( A_w(T) \) is the number of points on \( n - w \) hyperplanes.

The extended weights are given by

\[
A_5(T) = T(T - 1)
\]

\((T + 1) - 3\) points on double line; two points on 2 hyperplanes.
Example

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

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

Use that $A_w(T)$ is the number of points on $n - w$ hyperplanes.

The extended weights are given by

$$A_6(T) = 5(T - 1)(T - 2)(T + 1) - 3$$

extra points on 5 projective lines.
Example

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

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

Use that $A_w(T)$ is the number of points on $n - w$ hyperplanes.

The extended weights are given by

$$A_7(T) = (T - 1)(T^2 - 5T + 6)$$

The total number of projective points is $T^2 + T + 1$. 
Determination of extended weight enumerator

For all subsets $J \subseteq [n]$ define

$$C(J) = \{ c \in C : c_j = 0 \text{ for all } j \in J \}$$
$$l(J) = \dim C(J)$$
$$B_J(T) = T^{l(J)} - 1$$
$$B_t(T) = \sum_{|J|=t} B_J(T)$$

Note:

- $\dim C(J) = \dim (C \otimes \mathbb{F}_{q^m})(J)$.
- $B_J(q^m)$ is the number of nonzero words in $(C \otimes \mathbb{F}_{q^m})(J)$.
- $C(J) \cong \bigcup_{j \in J} H_j$, where $H_j$ are in $\mathcal{A}_C$. 
To determine the number of points on $n - w$ hyperplanes, we use an inclusion-exclusion argument.

Proposition

$$A_w(T) = \sum_{t=n-w}^{n} (-1)^{n+w+t} \binom{t}{n-w} B_t(T)$$
To determine the number of points on \( n - w \) hyperplanes, we use an inclusion-exclusion argument.

**Proposition**

\[
A_w(T) = \sum_{t=n-w}^{n} (-1)^{n+w+t} \binom{t}{n-w} B_t(T)
\]

**Theorem**

*The extended weight enumerator can be written as*

\[
W_C(X, Y, T) = X^n + \sum_{t=0}^{n} B_t(T)(X - Y)^t Y^{n-t}.
\]
A *geometric lattice* $L$ is a set with partial ordering $\leq$ and some additional specifying properties.

An arrangement $\mathcal{A}_C$ gives rise to a geometric lattice $L(C)$:

- **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**: Corank of $x$ in $\mathbb{F}_q^k$
- **Atoms**: The hyperplanes of the arrangements, without multiplicity
Geometric lattices

Example
The Möbius function of a geometric lattice is defined for all $x \leq y$ by $\mu_L(x, x) = 0$ and

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

Note the function is alternating in the rank of the geometric lattice.
Coboundary polynomial

The Möbius function of a geometric lattice is defined for all \( x \leq y \) by \( \mu_L(x, x) = 0 \) and

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

Note the function is alternating in the rank of the geometric lattice.

Coboundary polynomial

The coboundary of a geometric lattice is defined by

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

where \( \mid x \mid \) is the number of atoms smaller then \( x \).
If all the hyperplanes in \( \mathcal{A}_C \) are distinct, we say the code is \textit{projective}. (Equivalent: \( d(C^\perp) \geq 3 \).)

**Theorem**

\textit{The extended weight enumerator of a projective code is determined the coboundary polynomial of the associated geometric lattice, and vise versa, via}

\[
\chi_{L(C)}(S, T) = W_C(S, 1, T)
\]

\[
W_C(X, Y, T) = Y^n \cdot \chi_{L(C)}(XY^{-1}, T)
\]
• Extending the underlying field gives extension codes $C \otimes \mathbb{F}_{q^m}$, and we define the extended weight enumerator $W_C(X, Y, T)$. 
Summary

- 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 $\mathcal{A}_C$ to a code.
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 $A_C$ to a code.

Finding the extended weight enumerator means counting points in intersections of hyperplanes.
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 $\mathcal{A}_C$ to a code.

Finding the extended weight enumerator means counting points in intersections of hyperplanes.

This counting can also be done using the geometric lattice associated with the arrangement.
Summary

• 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 $A_C$ to a code.

• Finding the extended weight enumerator means counting points in intersections of hyperplanes.

• This counting can also be done using the geometric lattice associated with the arrangement.

• For projective codes, the coboundary polynomial of $L(C)$ is equivalent to the extended weight enumerator.