Application of hyperplane arrangements to error-correcting codes

Dr. Relinde Jurrius
(joint work with Dr. Ruud Pellikaan)

University of Neuchâtel, Switzerland

December 21, 2016

Coding theory

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.

Example

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

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

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 $\mathbb{F}_q^*$.

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 = number of words of weight w.

Weight enumeration

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: $[n, k]$ 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.

Weight enumeration

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.

Weight enumeration

Example

The [7, 4] Hamming code has extended weight enumerator

$$
\begin{aligned}
W_C(X, Y, T) \;=\; & X^7 + \\
& 7(T-1)X^4Y^3 + \\
& 7(T-1)X^3Y^4 + \\
& 21(T-1)(T-2)X^2Y^5 + \\
& 7(T-1)(T-2)(T-3)XY^6 + \\
& (T-1)(T^3-6T^2+15T-13)Y^7
\end{aligned}
$$

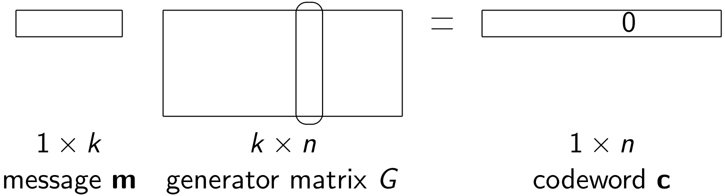
Why do we study this?

The extended weight enumerator is interesting because:

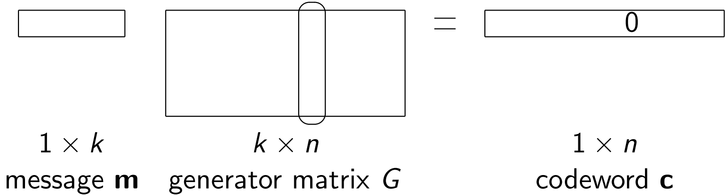
- Determines the probability of undetected error in error-detection.
- Determines the probability of decoding error in bounded distance decoding.
- Connection to Tutte polynomial in matroid theory.
- Connection to zeta function of (algebraic geometric) codes.

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

Weight enumeration



Weight enumeration



Theorem

$$c_j = 0 \iff \mathbf{m} \textit{ lies in hyperplane } H_j$$

Weight enumeration = counting points in (intersections of) hyperplanes.

Codes and hyperplane arrangements

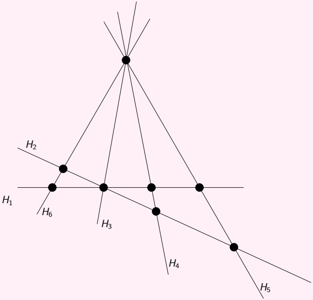
Columns of a generator matrix G of a linear $[n, k]$ code form a linear hyperplane arrangement in $\mathbb{F}_q^k$. Notation: $(H_1, \ldots, H_n)$.

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

Theorem

$A_w(T) =$ number of points from vectorspace over field of T elements that are on $n - w$ hyperplanes.

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 $a \neq 0, 1$.

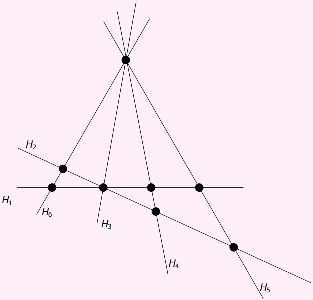
The extended weights are given by

$$A_0(T) = 1$$

The zero word is on all hyperplanes.

Codes and hyperplane arrangements

Example



Let $q > 2$ and C generated by

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

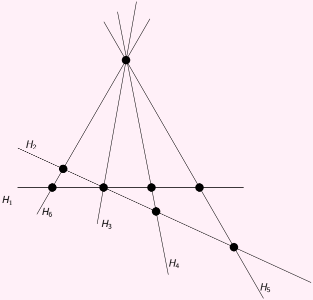
where $a \neq 0, 1$.

The extended weights are given by

$$A_1(T) = 0$$

No points are on 5 hyperplanes.

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 $a \neq 0, 1$.

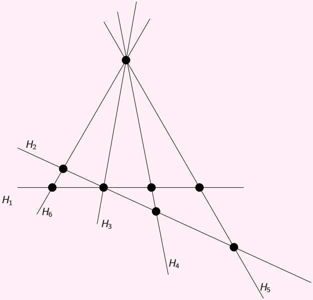
The extended weights are given by

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

One projective point is on 4 hyperplanes.

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 $a \neq 0, 1$.

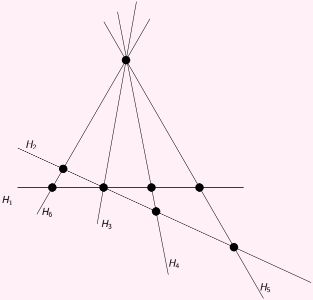
The extended weights are given by

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

One projective point is on 3 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 $a \neq 0, 1$.

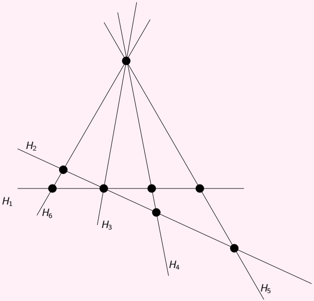
The extended weights are given by

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

Six projective points are on 2 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 $a \neq 0, 1$.

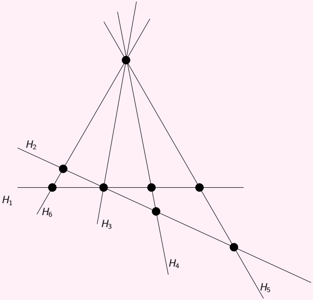
The extended weights are given by

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

Six lines with $T+1$ points; minus the points counted before.

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

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

The total number of projective points is $T^2 + T + 1$.

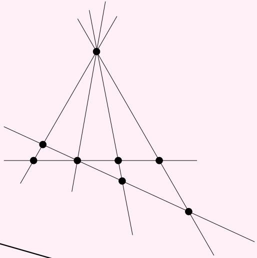
Geometric lattice

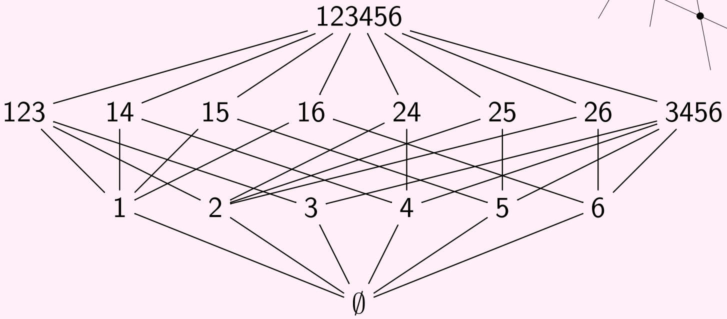
To formalize this counting, we use the *geometric lattice* associated to the arrangement. Notation: L.

Elements	All intersections of hyperplanes
Ordering	$x \leq y$ if $y \subseteq x$
Minimum	Whole space $\mathbb{F}_q^k$
Maximum	Zero vector $\mathbf{0} \in \mathbb{F}_q^k$
Rank	Codimension of x in $\mathbb{F}_q^k$
Atoms	The hyperplanes of the arrangement

Geometric lattice

Example





Möbius function

For all $x \leq y$, we have $\mu_L(x,x) = 1$ and

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

Characteristic polynomial

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

Coboundary polynomial

Coboundary polynomial

The coboundary of a geometric lattice is defined by

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

where $a(x)$ is the number of atoms smaller then x.

We write:

$$\chi_L(S,T) = \sum_{i=0}^{n} S^i \chi_i(T), \quad \text{with} \quad \chi_i(T) = \sum_{\substack{x \in L \\ a(x)=i}} \chi_{[x,\hat{1}]}(T).$$

Coboundary polynomial

Theorem

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

Proof:

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

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

Coboundary polynomial

Well-known fact:

$$\begin{aligned}\chi_L(q^m) &= \text{number of points in } \mathbb{F}_{q^m}^k \text{ not in the arrangement} \\ &= \text{number of points in } \mathbb{F}_{q^m}^k \text{ in } \hat{0} \text{ but not in any } y > \hat{0}\end{aligned}$$

This means that:

$$\begin{aligned}A_{n-i}(q^m) &= \sum_{\substack{x \in L \\ a(x)=i}} \text{number of points in } \mathbb{F}_{q^m}^k \text{ in } x \text{ but not in any } y > x \\ &= \sum_{\substack{x \in L \\ a(x)=i}} \chi_{[x,\hat{1}]}(q^m) \\ &= \chi_i(q^m)\end{aligned}$$

So by interpolation, $\chi_i(T) = A_{n-i}(T)$. □

Summary so far

- 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.

Coset leader weight enumerator

Coset Translation of the code by a vector $\mathbf{y} \in \mathbb{F}_q^n$.

Weight The minimum weight of all vectors in the coset.

Coset leader A vector of minimum weight in the coset.

Coset leader weight enumerator

Coset Translation of the code by a vector $\mathbf{y} \in \mathbb{F}_q^n$.

Weight The minimum weight of all vectors in the coset.

Coset leader A vector of minimum weight in the coset.

Extended coset leader weight enumerator

The homogeneous polynomial counting the number of cosets of a given weight "for all extension codes", notation:

$$\alpha_C(X, Y, T) = \sum_{i=0}^{n} \alpha_i(T) X^{n-i} Y^i.$$

Note that we have $\alpha_C(X, Y, q^m) = \alpha_{C \otimes \mathbb{F}_q^m}(X, Y)$.

Why do we study this?

The extended coset leader weight enumerator is interesting because:

- Determines the probability of correct decoding in coset leader decoding.
- Determines the average of changed symbols in *steganography* (information hiding).
- Not determined by the extended weight enumerator.

. . . and of course because they are invariants of linear codes.

Determination of coset weights

Parity check matrix: $(n-k) \times n$ matrix H such that $GH^T = 0$.

Syndrome of $\mathbf{y}$: The vector $\mathbf{s} = H\mathbf{y}^T$, zero for codewords.

Syndrome weight: Minimal number of columns whose span contains $\mathbf{s}$.

Determination of coset weights

Parity check matrix $(n-k) \times n$ matrix H such that $GH^T = 0$.

Syndrome of $\mathbf{y}$ The vector $\mathbf{s} = H\mathbf{y}^T$, zero for codewords.

Syndrome weight Minimal number of columns whose span contains $\mathbf{s}$.

- Isomorphism between cosets and syndromes, because $H(\mathbf{y}+\mathbf{c})^T = H\mathbf{y}^T + H\mathbf{c}^T = H\mathbf{y}^T$.
- Syndrome weight is equal to corresponding coset weight (weight of coset leader).
- α_i is the number of vectors that are in the span of i columns of H but not in the span of $i-1$ columns of H.

Projective systems

Projective system n-tuple of points in $\mathbb{P}^{k-1}(\mathbb{F}_q)$.

Columns of a generator matrix G of a linear $[n, k]$ code form a projective system. Notation: $(P_1, \ldots, P_n)$.

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

Projective systems

Projective system n-tuple of points in $\mathbb{P}^{k-1}(\mathbb{F}_q)$.

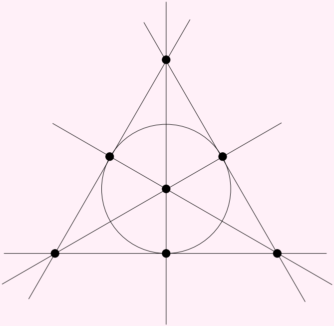
Columns of a generator matrix G of a linear $[n, k]$ code form a projective system. Notation: $(P_1, \ldots, P_n)$.

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

Projective systems are the geometric duals of hyperplane arrangements. Both induce the same geometric lattice.

Determination of coset weights

Example



The $[7, 4]$ binary Hamming code has parity check matrix

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

$\alpha_i = \#$ vectors in span of i columns but not in span of $i-1$ columns

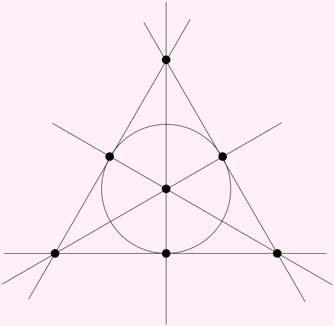
The extended coset leader weights are given by

$$\alpha_0(T) = 1$$

The code itself.

Determination of coset weights

Example



The $[7,4]$ binary Hamming code has parity check matrix

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

$\alpha_i = \#$ vectors in span of i columns but not in span of $i-1$ columns

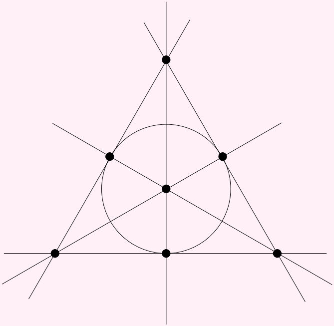
The extended coset leader weights are given by

$$\alpha_1(T) = 7(T-1)$$

Seven projective points.

Determination of coset weights

Example



The $[7,4]$ binary Hamming code has parity check matrix

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

$\alpha_i = \#$ vectors in span of i columns but not in span of $i-1$ columns

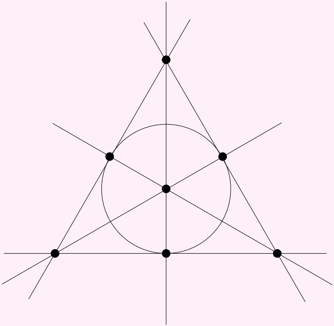
The extended coset leader weights are given by

$$\alpha_2(T) = 7(T-1)(T-2)$$

$(T+1) - 3$ extra points on 7 projective lines.

Determination of coset weights

Example



The $[7, 4]$ binary Hamming code has parity check matrix

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

$\alpha_i = \#$ vectors in span of i columns but not in span of $i-1$ columns

The extended coset leader weights are given by

$$\alpha_3(T) = (T-1)(T-2)(T-4)$$

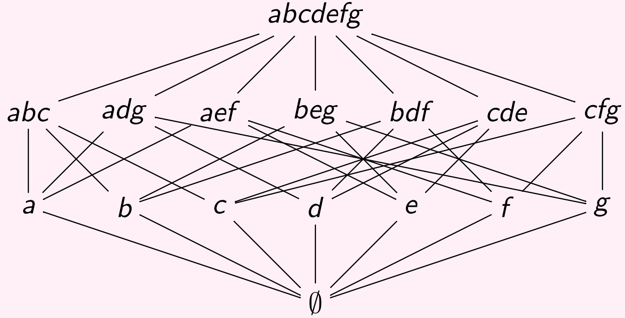
$\alpha_0(T) + \alpha_1(T) + \alpha_2(T) + \alpha_3(T) = T^3$ total number of cosets.

Determination of coset weights

How to formalize this counting?

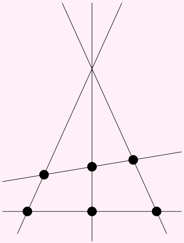
Example (continued)

The geometric lattice associated to the $[7, 4]$ binary Hamming code is visualized by

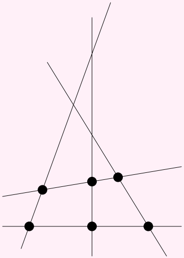


Determination of coset weights

Example



1 coset with
3 coset leaders



3 cosets with
2 leaders each

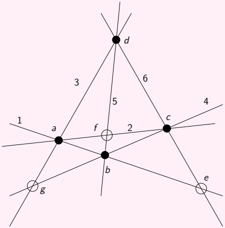
Projective systems with equal geometric lattices may have different coset leader weight enumerators!

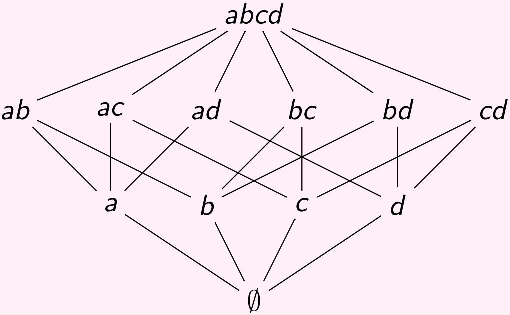
Derived code

- Start with $[n, k]$ code.
- Consider the projective system $\mathcal{P}_C$.
- Look at all hyperplanes spanned by $k-1$ points of $\mathcal{P}_C$. (Ignore $k-1$ points that span spaces of lower dimension.)
- Remove (multiple) copies of hyperplanes.
- These hyperplanes form an arrangement $\mathcal{A}$.
- The *derived code* $D(C)$ is the code such that $\mathcal{A} = \mathcal{A}_{D(C)}$.

Derived code

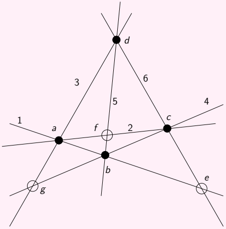
Example

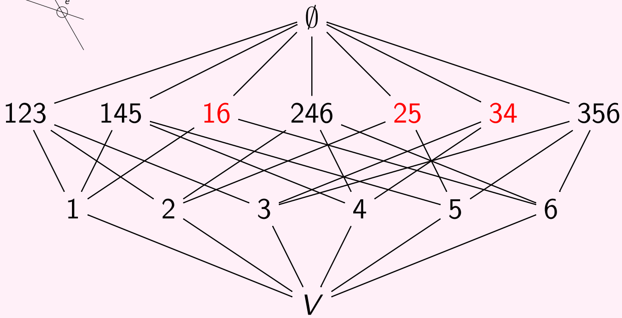




Derived code

Example





Extended coset leader weight enumerator

- The lattice of $\mathcal{P}_C$, upside-down, is contained in the lattice of $\mathcal{A}_{D(C)}$.
- This gives an injection $\psi : L(\mathcal{P}_C) \hookrightarrow L(\mathcal{A}_{D(C)})$.
- All elements that are not in the image $\psi(L(\mathcal{P}_C))$ should be counted similar to the largest element below it that is in $\psi(L(\mathcal{P}_C))$.
- Therefore, define $r^*(x) = \max\{r(y) : y \in \psi(L(\mathcal{P}_C)), y \leq x\}$.

Extended coset leader weight enumerator

- The lattice of $\mathcal{P}_C$, upside-down, is contained in the lattice of $\mathcal{A}_{D(C)}$.
- This gives an injection $\psi : L(\mathcal{P}_C) \hookrightarrow L(\mathcal{A}_{D(C)})$.
- All elements that are not in the image $\psi(L(\mathcal{P}_C))$ should be counted similar to the largest element below it that is in $\psi(L(\mathcal{P}_C))$.
- Therefore, define $r^*(x) = \max\{r(y) : y \in \psi(L(\mathcal{P}_C)), y \leq x\}$.

Theorem

The extended coset leader weight enumerator is equal to

$$\alpha_C(X, Y, T) = \sum_{x,y \in L(\mathcal{A}_{D(C)})} \mu(x, y) T^{n-k-r(y)} X^{k+r^*(x)} Y^{n-k-r^*(x)}.$$

Summary

- The extended coset leader weight enumerator is an important invariant of linear codes.
- Determining coset weights is equivalent to counting points in spans of points.
- Counting points can be formalized by using the geometric lattice of the derived code.

Further questions

- Are there other counting problems that use the derived arrangement?
- Does the extended coset leader weight enumerator determine the extended weight enumerator?
- Can we define a *derived lattice*?
- Taking $D(D(D(\cdots(C)\cdots)))$ eventually gives all hyperplanes in $\mathbb{P}^{k-1}(\mathbb{F}_q)$. How fast?
- Dependencies between dependencies are known as *second order syzygies* in computational geometry. Can this interpretation help?
- Can we determine $\alpha_C(X, Y, T)$ for concrete classes of codes? (For example: generalized Reed-Solomon codes)
- Can we classify codes using their coset leader weight enumerator?
- ...

Thank you for your attention.