The (extended) coset leader and list weight enumerator

Relinde Jurrius
(joint work with Ruud Pellikaan)

Vrije Universiteit Brussel

Fq11
July 24, 2013

Extension codes

Weight	The number of nonzero coordinates of a vector.
Linear $[n, k]$ code	Linear subspace $C \subseteq \mathrm{GF}(q)^n$ of dimension k. Elements are called *(code)words*, n is called the *length*.
Generator matrix	The rows of this $k \times n$ matrix form a basis for C.

Extension codes

Weight	The number of nonzero coordinates of a vector.
Linear $[n, k]$ code	Linear subspace $C \subseteq \mathrm{GF}(q)^n$ of dimension k. Elements are called *(code)words*, n is called the *length*.
Generator matrix	The rows of this $k \times n$ matrix form a basis for C.

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

Coset leader weight enumerator

Coset Translation of the code by a vector $\mathbf{y} \in \mathrm{GF}(q)^n$.

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 $\mathbf{y} \in \mathrm{GF}(q)^n$.

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 $\alpha_C(X, Y, q^m) = \alpha_{C \otimes \mathrm{GF}(q^m)}(X, Y)$.

List weight enumerator

Extended list weight enumerator

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

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

Note that we have $\lambda_C(X, Y, q^m) = \lambda_{C \otimes \mathrm{GF}(q^m)}(X, Y)$.

List weight enumerator

Extended list weight enumerator

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

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

Note that we have $\lambda_C(X, Y, q^m) = \lambda_{C \otimes \mathrm{GF}(q^m)}(X, Y)$.

In general, we have

$$\alpha_i(T) \leq \lambda_i(T),$$

with equality iff all cosets of weight i have a unique coset leader.

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.

The extended list weight enumerator is interesting because:

- Determines the size of lists in list decoding.
- Determines the probability of correct decoding in list decoding.

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

Hyperplane arrangements and projective systems

Arrangement of hyperplanes	n-tuple of hyperplanes in $\mathrm{GF}(q)^k$.
Essential arrangement	Intersection of all hyperplanes is $\{\mathbf{0}\}$, hyperplanes are in $\mathrm{PG}(k-1,q)$.
Projective system	n-tuple of points in $\mathrm{PG}(k-1,q)$.

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

Hyperplane arrangements and projective systems

Arrangement of hyperplanes	n-tuple of hyperplanes in $\mathrm{GF}(q)^k$.
Essential arrangement	Intersection of all hyperplanes is $\{\mathbf{0}\}$, hyperplanes are in $\mathrm{PG}(k-1,q)$.
Projective system	n-tuple of points in $\mathrm{PG}(k-1,q)$.

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

Columns of a generator matrix G of a linear $[n,k]$ code form a hyperplane arrangement / projective system.

- One-to-one correspondence between equivalence classes.
- Independent of choice of G, so notation: $\mathcal{A}_C$ or $\mathcal{P}_C$.
- Also valid over an extension field $\mathrm{GF}(q^m)$.

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 $GH^T = 0$.

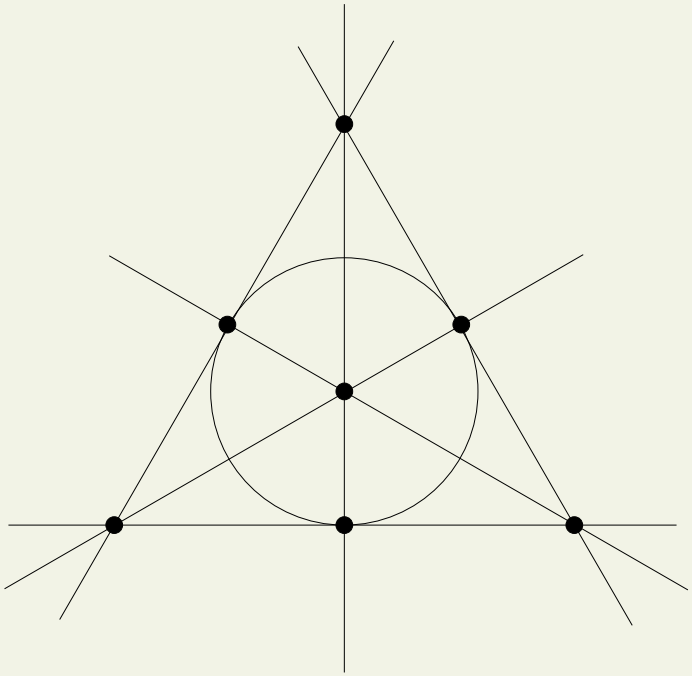
Syndrome of $\mathbf{y}$ The vector $\mathbf{s} = H\mathbf{y}^T$, zero for codewords.

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.

Determination of coset weights

Example



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

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

This is a projective system of seven points in the projective plane.

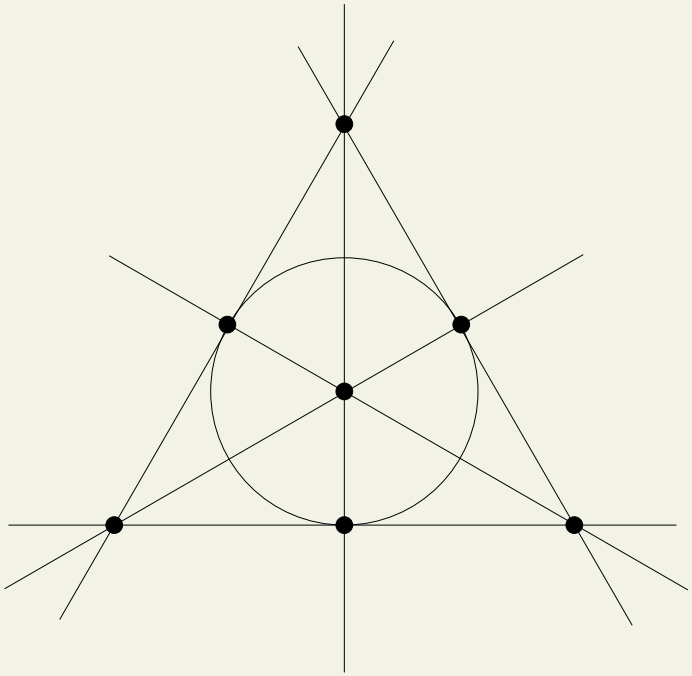
The extended coset leader weights are given by

$$\alpha_0(T) = 1$$

The code itself.

Determination of coset weights

Example



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

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

This is a projective system of seven points in the projective plane.

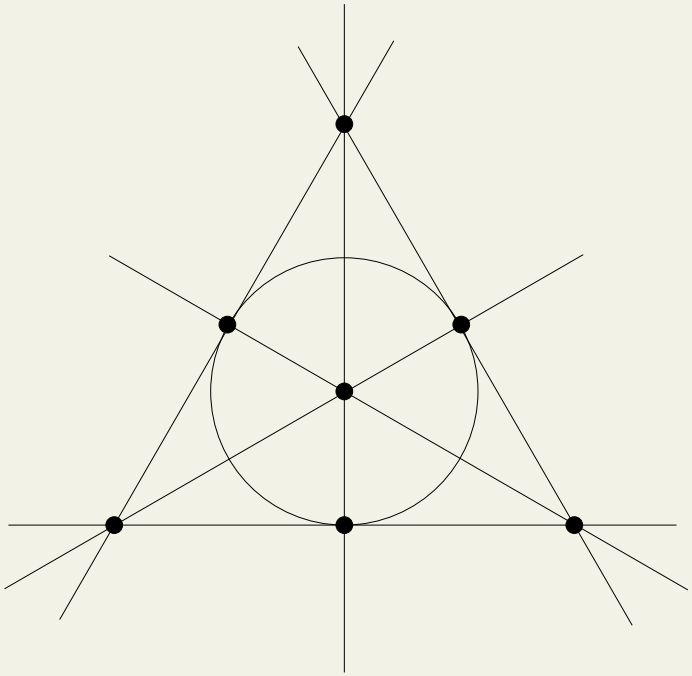
The extended coset leader weights are given by

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

Seven projective points.

Determination of coset weights

Example



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

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

This is a projective system of seven points in the projective plane.

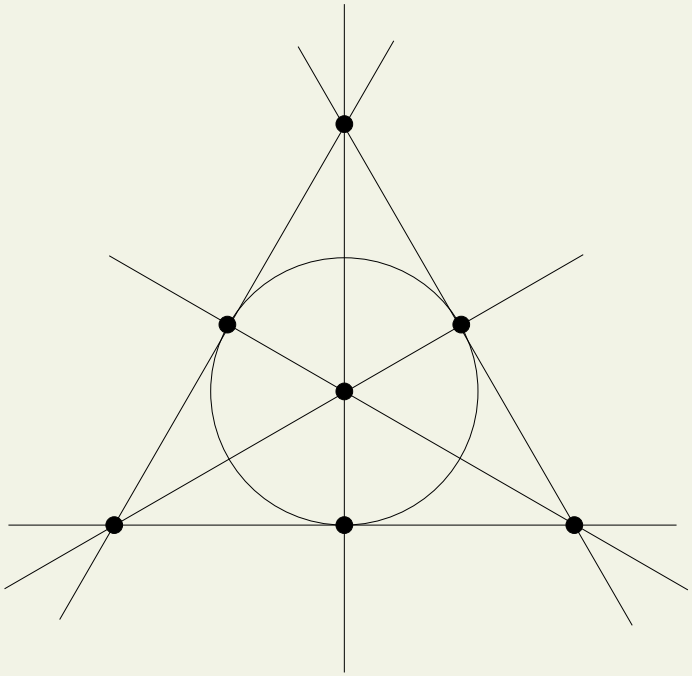
The extended coset leader weights are given by

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

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

Determination of coset weights

Example



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

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

This is a projective system of seven points in the projective plane.

The extended coset leader weights are given by

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

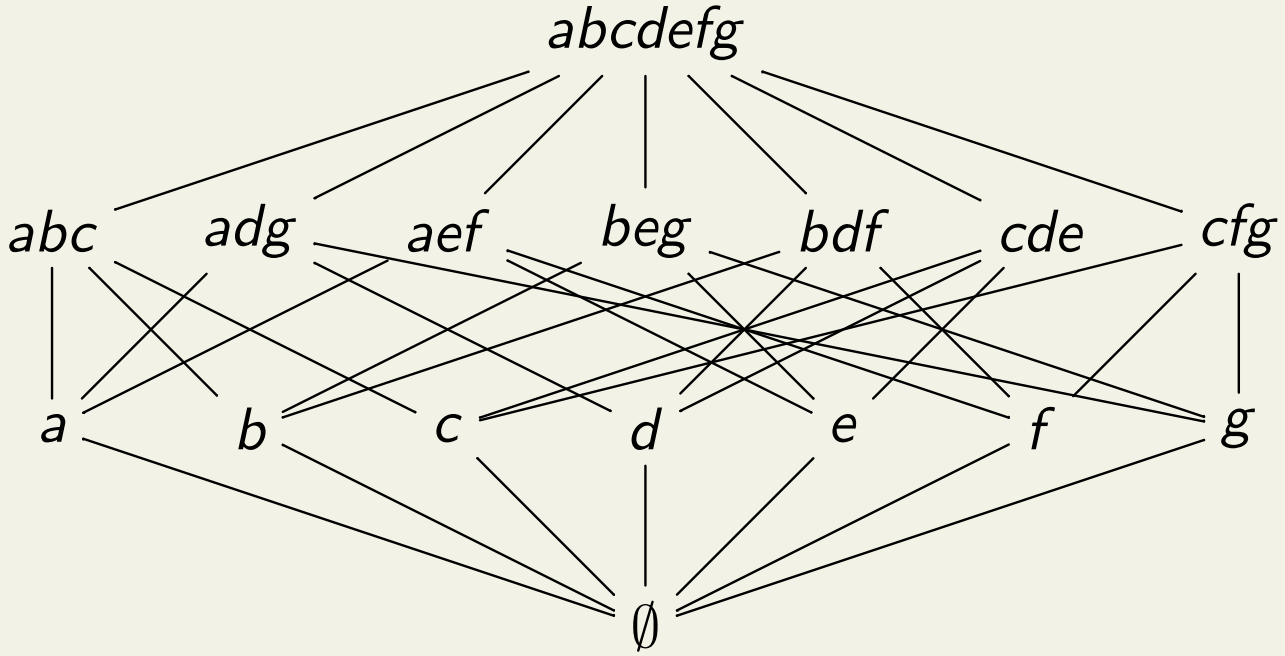
$\alpha_0(T) + \alpha_1(T) + \alpha_2(T) + \alpha_3(T) = T^3$ total number of cosets.

Determination of coset weights

This kind of inclusion/exclusion counting is formalized by the *geometric lattice* associated to a projective system and its *Möbius function*.

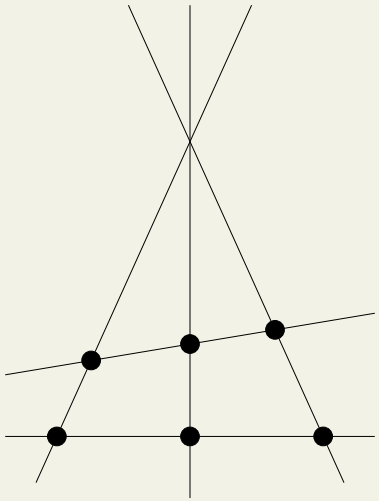
Example (continued)

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

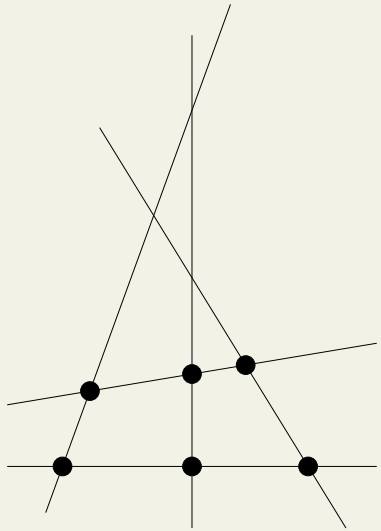


Determination of coset weights

Example



1 coset with
3 coset leaders



3 cosets with
2 leaders each

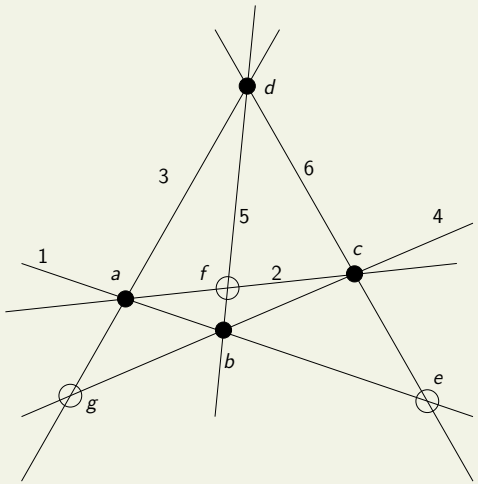
Projective systems with equal geometric lattices may have different coset leader weight enumerators!

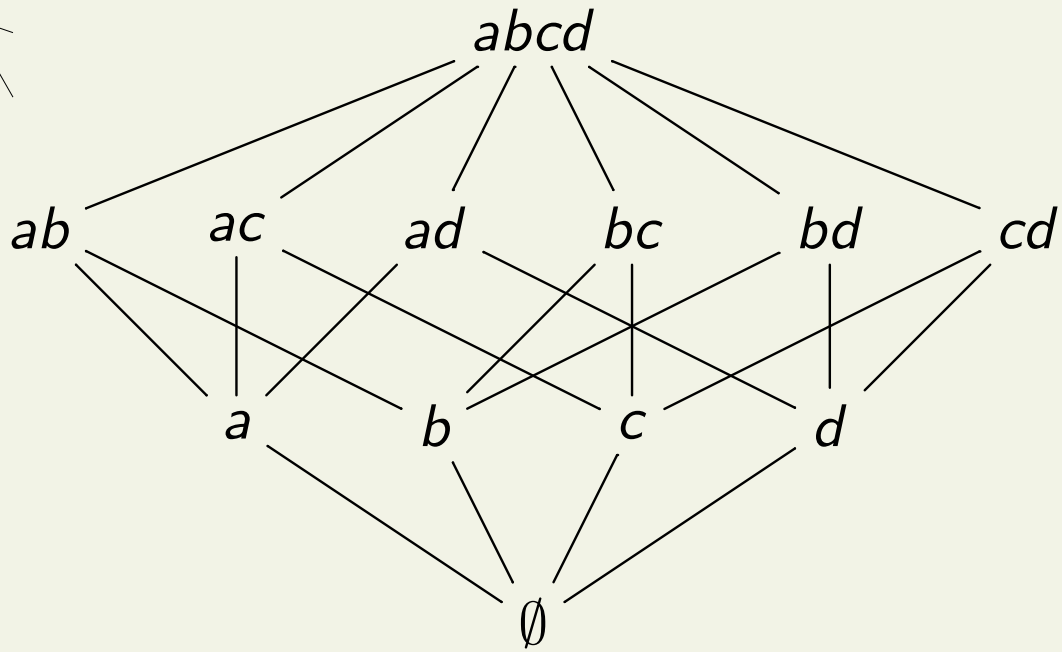
Derived code

- 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

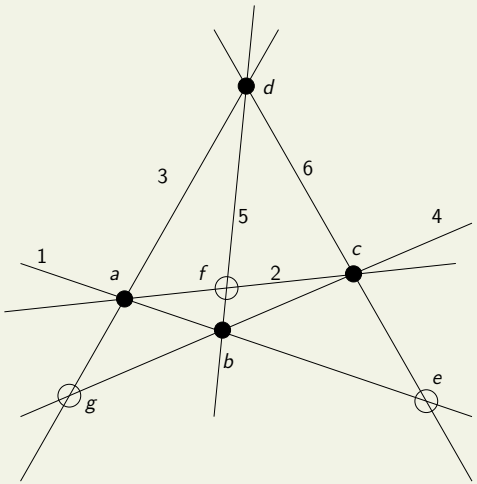
Example

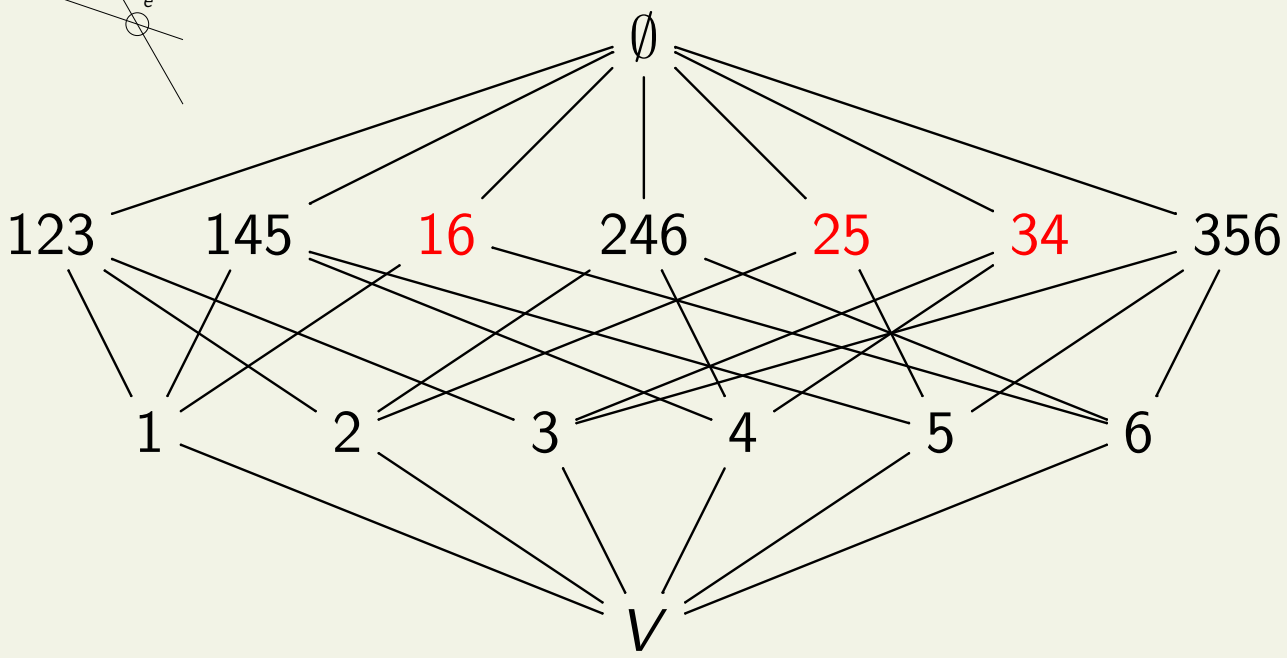




Derived code

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

- 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 $\mathrm{PG}(k-1,q)$. 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.