The coset leader weight enumerator of the code of the twisted cubic

Ruud Pellikaan
g.r.pellikaan@tue.nl

Arithmetic, Geometry, Cryptography and Coding Theory
$AGC^2T - 17$, Luminy, 11 June 2019

Technische Universiteit Eindhoven University of Technology

Gilles Lachaud †21 February 2018 at the age 71

Image taken from his homepage:
http://iml.univ-mrs.fr/fiche/Gilles_Lachaud.html

Introduction and content

- (Extended) weight enumerator
- Projective systems and arrangements of hyperplanes
- (Extended) coset leader weight enumerator
- for codes on conic
- for codes on twisted cubic

Error-correcting codes and weight enumerators

Weight and distance

$\mathbb{F}_q$ is the finite field with q elements

The weight of $\mathbf{x}$ in $\mathbb{F}_q^n$ is defined by

$$\mathrm{wt}(\mathbf{x}) = |\{\, j \;:\; x_j \neq 0 \,\}|$$

that is the number of nonzero entries of $\mathbf{x}$

The Hamming distance between $\mathbf{x}$ and $\mathbf{y}$ is defined by

$$d(\mathbf{x}, \mathbf{y}) = |\{\, j \;:\; x_j \neq y_j \,\}|$$

So

$$d(\mathbf{x}, \mathbf{y}) = \mathrm{wt}(\mathbf{x} - \mathbf{y})$$

Weight and distance

$\mathbb{F}_q$ is the finite field with q elements

The weight of $\mathbf{x}$ in $\mathbb{F}_q^n$ is defined by

$$\mathrm{wt}(\mathbf{x}) = |\{ j : x_j \neq 0 \}|$$

that is the number of nonzero entries of $\mathbf{x}$

The Hamming distance between $\mathbf{x}$ and $\mathbf{y}$ is defined by

$$d(\mathbf{x}, \mathbf{y}) = |\{ j : x_j \neq y_j \}|$$

So

$$d(\mathbf{x}, \mathbf{y}) = \mathrm{wt}(\mathbf{x} - \mathbf{y})$$

Weight and distance

$\mathbb{F}_q$ is the finite field with q elements

The weight of $\mathbf{x}$ in $\mathbb{F}_q^n$ is defined by

$$\mathrm{wt}(\mathbf{x}) = |\{\, j \ : \ x_j \neq 0 \,\}|$$

that is the number of nonzero entries of $\mathbf{x}$

The Hamming distance between $\mathbf{x}$ and $\mathbf{y}$ is defined by

$$d(\mathbf{x}, \mathbf{y}) = |\{\, j \ : \ x_j \neq y_j \,\}|$$

So

$$d(\mathbf{x}, \mathbf{y}) = \mathrm{wt}(\mathbf{x} - \mathbf{y})$$

C is called an $[n, k, d]_q$ code if it is a
k dimensional $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$
of minimum distance $d = d(C)$ where

$$d(C) = \min\{\, d(\mathbf{x}, \mathbf{y}) \;:\; \mathbf{x}, \mathbf{y} \in C,\; \mathbf{x} \neq \mathbf{y} \,\}$$

So

$$d(C) = \min\{\, \mathrm{wt}(\mathbf{c}) \;:\; \mathbf{0} \neq \mathbf{c} \in C \,\}$$

C is called degenerate
if for there is a position j such that $c_j = 0$ for all $\mathbf{c} \in C$

Error-correcting codes

C is called an $[n, k, d]_q$ code if it is a
k dimensional $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$
of minimum distance $d = d(C)$ where

$$d(C) = \min\{\, d(\mathbf{x}, \mathbf{y}) \;:\; \mathbf{x}, \mathbf{y} \in C,\ \mathbf{x} \neq \mathbf{y} \,\}$$

So

$$d(C) = \min\{\, \mathrm{wt}(\mathbf{c}) \;:\; \mathbf{0} \neq \mathbf{c} \in C \,\}$$

C is called degenerate
if for there is a position j such that $c_j = 0$ for all $\mathbf{c} \in C$

Error-correcting codes

C is called an $[n, k, d]_q$ code if it is a
k dimensional $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$
of minimum distance $d = d(C)$ where

$$d(C) = \min\{\, d(\mathbf{x}, \mathbf{y}) \,:\, \mathbf{x}, \mathbf{y} \in C,\ \mathbf{x} \neq \mathbf{y} \,\}$$

So

$$d(C) = \min\{\, \mathrm{wt}(\mathbf{c}) \,:\, \mathbf{0} \neq \mathbf{c} \in C \,\}$$

C is called degenerate
if for there is a position j such that $c_j = 0$ for all $\mathbf{c} \in C$

Generator and parity check matrix

C an $\mathbb{F}_q$-linear code of length n and dimension k

A $k \times n$ matrix G with entries in $\mathbb{F}_q$
is called generator matrix of C if

$$C = \{ \mathbf{m}G \ : \ \mathbf{m} \in \mathbb{F}_q^k \}$$

A $(n-k) \times n$ matrix H with entries in $\mathbb{F}_q$
is called a parity check matrix of C if

$$C = \{ \mathbf{c} \in \mathbb{F}_q^n \ : \ \mathbf{c}H^T = 0 \}$$

Generator and parity check matrix

C an $\mathbb{F}_q$-linear code of length n and dimension k

A $k \times n$ matrix G with entries in $\mathbb{F}_q$
is called generator matrix of C if

$$C = \{ \mathbf{m}G \ : \ \mathbf{m} \in \mathbb{F}_q^k \}$$

A $(n-k) \times n$ matrix H with entries in $\mathbb{F}_q$
is called a parity check matrix of C if

$$C = \{ \mathbf{c} \in \mathbb{F}_q^n \ : \ \mathbf{c}H^T = 0 \}$$

Inner product and dual code

The inner product on $\mathbb{F}_q^n$ is defined by

$$\mathbf{x} \cdot \mathbf{y} = x_1 y_1 + \cdots + x_n y_n$$

For an $[n, k]$ code C we define the dual or orthogonal code $C^\perp$ as

$$C^\perp = \{\, \mathbf{x} \in \mathbb{F}_q^n \;:\; \mathbf{c} \cdot \mathbf{x} = 0 \text{ for all } \mathbf{c} \in C \,\}$$

G is generator matrix of C if and only if G is a parity check matrix of $C^\perp$

Inner product and dual code

The inner product on $\mathbb{F}_q^n$ is defined by

$$\mathbf{x} \cdot \mathbf{y} = x_1 y_1 + \cdots + x_n y_n$$

For an $[n, k]$ code C we define the dual or orthogonal code $C^\perp$ as

$$C^\perp = \{ \mathbf{x} \in \mathbb{F}_q^n \ : \ \mathbf{c} \cdot \mathbf{x} = 0 \text{ for all } \mathbf{c} \in C \}$$

G is generator matrix of C if and only if G is a parity check matrix of $C^\perp$

Inner product and dual code

The inner product on $\mathbb{F}_q^n$ is defined by

$$\mathbf{x} \cdot \mathbf{y} = x_1 y_1 + \cdots + x_n y_n$$

For an $[n, k]$ code C we define the dual or orthogonal code $C^\perp$ as

$$C^\perp = \{ \mathbf{x} \in \mathbb{F}_q^n \ : \ \mathbf{c} \cdot \mathbf{x} = 0 \text{ for all } \mathbf{c} \in C \}$$

G is generator matrix of C if and only if G is a parity check matrix of $C^\perp$

Weight enumerator

Let C be a code of length n
Define

$$A_w = |\{ \mathbf{c} \in C \ : \ \mathrm{wt}(\mathbf{c}) = w \}|$$

So A_w denotes the number of codewords in C of weight w

The weight enumerator of C is:

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

A_w is divisible by $q-1$ if $w > 0$
Define

$$\bar{A}_w = A_w/(q-1)$$

Weight enumerator

Let C be a code of length n
Define

$$A_w = |\{ \mathbf{c} \in C \ : \ \mathrm{wt}(\mathbf{c}) = w \}|$$

So A_w denotes the number of codewords in C of weight w

The weight enumerator of C is:

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

A_w is divisible by $q-1$ if $w > 0$
Define

$$\bar{A}_w = A_w/(q-1)$$

Technische Universiteit Eindhoven University of Technology

Weight enumerator

Let C be a code of length n
Define

$$A_w = |\{ \mathbf{c} \in C \ : \ \mathrm{wt}(\mathbf{c}) = w \}|$$

So A_w denotes the number of codewords in C of weight w

The weight enumerator of C is:

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

A_w is divisible by $q - 1$ if $w > 0$
Define

$$\bar{A}_w = A_w/(q-1)$$

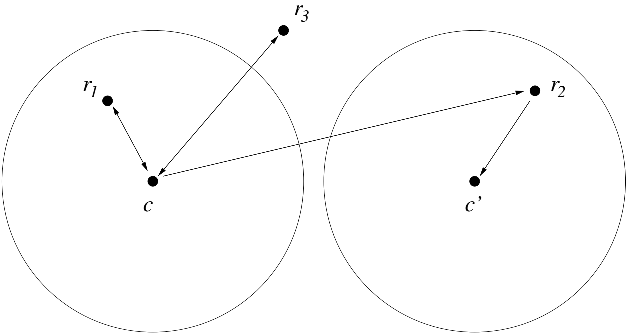
PROPOSITION

Let $W_C(X, Y)$ be the weigh enumerator of the code C

Then the probability of undetected error on a q-ary symmetric channel with cross-over probability p is given by

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

Decoding correctly, error and failure



Figuur: r_1: decoded correctly, r_2: decoding error, r_3: failure

PROPOSITION

Consider the q-ary symmetric channel with cross-over probability p
Let C be a code of minimum distance d
Let $2t + 1 \leq d$

The probability of decoding error of a strict t-bounded distance decoder is given by

$$P_{de}(p) = \sum_{w=0}^{n} \left(\frac{p}{q-1}\right)^{w} (1-p)^{n-w} \sum_{s=0}^{t} \sum_{v=1}^{n} A_v N_q(n, v, w, s)$$

where $N_q(n, v, w, s)$ be the number of vectors in $\mathbb{F}_q^n$
of weight w that are at distance s from a given vector of weight v
(It does not depend on the chosen vector)

Extended code by scalars

Let C be a linear $[n, k]$ code over $\mathbb{F}_q$

Then $C \otimes \mathbb{F}_{q^m}$ is the extended code by scalars
that is the $\mathbb{F}_{q^m}$-linear code in $\mathbb{F}_{q^m}^n$ that is generated by C

If G is a $k \times n$ generator matrix of C with entries in $\mathbb{F}_q$
then G is also a generator matrix of $C \otimes \mathbb{F}_{q^m}$

Extended code by scalars

Let C be a linear $[n, k]$ code over $\mathbb{F}_q$

Then $C \otimes \mathbb{F}_{q^m}$ is the extended code by scalars
that is the $\mathbb{F}_{q^m}$-linear code in $\mathbb{F}_{q^m}^n$ that is generated by C

If G is a $k \times n$ generator matrix of C with entries in $\mathbb{F}_q$
then G is also a generator matrix of $C \otimes \mathbb{F}_{q^m}$

Weight enumerator via projective systems and arrangements

Segre, finite geometers, Katsman-Tsfasman, Jurrius-P

Projective systems and codes

A projective system $(P_1, \dots, P_n)$
is an n-tuple of points in projective space $\mathbb{P}^r(\mathbb{F}_q)$
such that not all of them lie in a hyperplane

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

Let P_j be the point in $\mathbb{P}^{k-1}(\mathbb{F}_q)$ with homogeneous coordinates

$$P_j = (g_{1j} : \cdots : g_{kj})$$

Let $\mathcal{P}_G$ be the projective system $(P_1, \dots, P_n)$ associated with G

Projective systems and codes

A projective system $(P_1, \ldots, P_n)$
is an n-tuple of points in projective space $\mathbb{P}^r(\mathbb{F}_q)$
such that not all of them lie in a hyperplane

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

Let P_j be the point in $\mathbb{P}^{k-1}(\mathbb{F}_q)$ with homogeneous coordinates

$$P_j = (g_{1j} : \cdots : g_{kj})$$

Let $\mathcal{P}_G$ be the projective system $(P_1, \ldots, P_n)$ associated with G

Projective systems and codes

A projective system $(P_1, \ldots, P_n)$
is an n-tuple of points in projective space $\mathbb{P}^r(\mathbb{F}_q)$
such that not all of them lie in a hyperplane

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

Let P_j be the point in $\mathbb{P}^{k-1}(\mathbb{F}_q)$ with homogeneous coordinates

$$P_j = (g_{1j} : \cdots : g_{kj})$$

Let $\mathcal{P}_G$ be the projective system $(P_1, \ldots, P_n)$ associated with G

Projective systems, codes and minimal weight

PROPOSITION

Let C be a nondegenerate $[n,k]$ code over $\mathbb{F}_q$ with generator matrix G
Let $\mathbf{c}$ be a nonzero codeword $\mathbf{c} = \mathbf{m}G$ for the unique $\mathbf{m} \in \mathbb{F}_q^k$
Let H be the hyperplane in $\mathbb{P}^{k-1}(\mathbb{F}_q)$ with equation

$$H : \ m_1X_1 + \cdots + m_kX_k = 0$$

Then $n - \mathrm{wt}(\mathbf{c})$ is equal to the number of points of of $\mathcal{P}_G$ in H

And $\bar{A}_w$ is the number of hyperplanes in the
projective space $\mathbb{P}^{k-1}(\mathbb{F}_q)$
with exactly $n-w$ points of $\mathcal{P}_P$ on it

Projective systems, codes and minimal weight

PROPOSITION

Let C be a nondegenerate $[n, k]$ code over $\mathbb{F}_q$ with generator matrix G
Let $\mathbf{c}$ be a nonzero codeword $\mathbf{c} = \mathbf{m}G$ for the unique $\mathbf{m} \in \mathbb{F}_q^k$
Let H be the hyperplane in $\mathbb{P}^{k-1}(\mathbb{F}_q)$ with equation

$$H : \quad m_1X_1 + \cdots + m_kX_k = 0$$

Then $n - \mathrm{wt}(\mathbf{c})$ is equal to the number of points of of $\mathcal{P}_G$ in H

And $\bar{A}_w$ is the number of hyperplanes in the
projective space $\mathbb{P}^{k-1}(\mathbb{F}_q)$
with exactly $n - w$ points of $\mathcal{P}_P$ on it

PROPOSITION

Let C be a nondegenerate $[n, k]$ code over $\mathbb{F}_q$ with generator matrix G
Let $\mathbf{c}$ be a nonzero codeword $\mathbf{c} = \mathbf{m}G$ for the unique $\mathbf{m} \in \mathbb{F}_q^k$
Let H be the hyperplane in $\mathbb{P}^{k-1}(\mathbb{F}_q)$ with equation

$$H : \quad m_1 X_1 + \cdots + m_k X_k = 0$$

Then $n - \mathrm{wt}(\mathbf{c})$ is equal to the number of points of of $\mathcal{P}_G$ in H

And $\bar{A}_w$ is the number of hyperplanes in the
projective space $\mathbb{P}^{k-1}(\mathbb{F}_q)$
with exactly $n - w$ points of $\mathcal{P}_P$ on it

Points in general position - MDS codes

Let C be a nondegenerate $[n, k]_q$ code

Then C is an MDS code, that is an $[n, k, n-k+1]_q$ code attaining the Singleton bound

if and only if

the points of the projective system $\mathcal{P}_G$ in $\mathbb{P}^{k-1}(\mathbb{F}_q)$ are in general position that is to say that
there are at most $k-1$ points of $\mathcal{P}_G$ in a hyperplane

Points in general position - MDS codes

Let C be a nondegenerate $[n, k]_q$ code

Then C is an MDS code, that is an $[n, k, n-k+1]_q$ code attaining the Singleton bound

if and only if

the points of the projective system $\mathcal{P}_G$ in $\mathbb{P}^{k-1}(\mathbb{F}_q)$ are in general position that is to say that
there are at most $k-1$ points of $\mathcal{P}_G$ in a hyperplane

Points in general position - MDS codes

Let C be a nondegenerate $[n, k]_q$ code

Then C is an MDS code, that is an $[n, k, n-k+1]_q$ code attaining the Singleton bound

if and only if

the points of the projective system $\mathcal{P}_G$ in $\mathbb{P}^{k-1}(\mathbb{F}_q)$ are in general position that is to say that
there are at most $k-1$ points of $\mathcal{P}_G$ in a hyperplane

Dually: arrangements and codes

An arrangement $(H_1, \ldots, H_n)$
is an n-tuple of hyperplanes in $\mathbb{F}_q^k$ or $\mathbb{P}^r(\mathbb{F}_q)$
such that their intersection is $\{0\}$ or empty, resp.

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

Let H_j be the linear hyperplane in $\mathbb{F}_q^k$ or $\mathbb{P}^{k-1}(\mathbb{F}_q)$ with equation

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

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

Dually: arrangements and codes

An arrangement $(H_1, \ldots, H_n)$
is an n-tuple of hyperplanes in $\mathbb{F}_q^k$ or $\mathbb{P}^r(\mathbb{F}_q)$
such that their intersection is $\{0\}$ or empty, resp.

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

Let H_j be the linear hyperplane in $\mathbb{F}_q^k$ or $\mathbb{P}^{k-1}(\mathbb{F}_q)$ with equation

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

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

Dually: arrangements and codes

An arrangement $(H_1, \ldots, H_n)$
is an n-tuple of hyperplanes in $\mathbb{F}_q^k$ or $\mathbb{P}^r(\mathbb{F}_q)$
such that their intersection is $\{0\}$ or empty, resp.

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

Let H_j be the linear hyperplane in $\mathbb{F}_q^k$ or $\mathbb{P}^{k-1}(\mathbb{F}_q)$ with equation

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

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

PROPOSITION

Let C be a nondegenerate $[n, k]$ 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 $\mathcal{A}_G$ going through $(x_1 : \cdots : x_k)$

And $\bar{A}_w$ is the number of points in $\mathbb{P}^{k-1}(\mathbb{F}_q)$ on exactly $n - w$ hyperplanes of $\mathcal{A}_G$

PROPOSITION

Let C be a nondegenerate $[n, k]$ 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 $\mathcal{A}_G$ going through $(x_1 : \cdots : x_k)$

And $\bar{A}_w$ is the number of points in $\mathbb{P}^{k-1}(\mathbb{F}_q)$ on exactly $n - w$ hyperplanes of $\mathcal{A}_G$

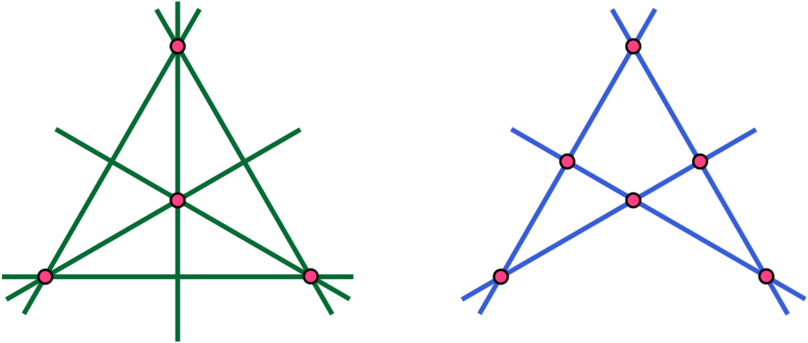
PROPOSITION

Let C be a nondegenerate $[n, k]$ 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 $\mathcal{A}_G$ going through $(x_1 : \cdots : x_k)$

And $\bar{A}_w$ is the number of points in $\mathbb{P}^{k-1}(\mathbb{F}_q)$ on exactly $n - w$ hyperplanes of $\mathcal{A}_G$

Projective system versus arrangement of lines



Figuur: Projective system (L), Arrangement of lines (R) in $\mathbb{P}^2(\mathbb{F}_q)$ of $[4, 3, 2]$ code

$\bar{A}_n$ and complement of hyperplanes

In particular $\bar{A}_n$ is equal to the number of points that is in the complement of the union of these hyperplanes in $\mathbb{P}^{k-1}(\mathbb{F}_q)$

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

$$\bar{A}_n = \frac{q^k - 1}{q - 1} - |H_1 \cup \cdots \cup H_n| =$$

$$\sum_{w=0}^{n} (-1)^w \sum_{i_1 < \cdots < i_w} |H_{i_1} \cap \cdots \cap H_{i_w}|$$

In particular $\bar{A}_n$ is equal to the number of points that is in the complement of the union of these hyperplanes in $\mathbb{P}^{k-1}(\mathbb{F}_q)$

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

$$\bar{A}_n = \frac{q^k - 1}{q - 1} - |H_1 \cup \cdots \cup H_n| =$$

$$\sum_{w=0}^{n} (-1)^w \sum_{i_1 < \cdots < i_w} |H_{i_1} \cap \cdots \cap H_{i_w}|$$

REMARK

Define for a subset J of $\{1, 2, \ldots, n\}$

$$C(J) = \{\mathbf{c} \in C \mid c_j = 0 \text{ for all } j \in J\}$$

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

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

REMARK

Define for a subset J of $\{1, 2, \ldots, n\}$

$$C(J) = \{\mathbf{c} \in C \mid c_j = 0 \text{ for all } j \in J\}$$

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

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

DEFINITION

Define following Katsman and Tsfasman

$$l(J) = \dim C(J)$$

$$B_J = q^{l(J)} - 1$$

$$B_t = \sum_{|J|=t} B_J$$

Then 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

$$\bigcap_{j \in J} H_j$$

DEFINITION

Define following Katsman and Tsfasman

$$l(J) = \dim C(J)$$

$$B_J = q^{l(J)} - 1$$

$$B_t = \sum_{|J|=t} B_J$$

Then 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

$$\bigcap_{j \in J} H_j$$

DEFINITION

Define following Katsman and Tsfasman

$$l(J) = \dim C(J)$$

$$B_J = q^{l(J)} - 1$$

$$B_t = \sum_{|J|=t} B_J$$

Then 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

$$\bigcap_{j \in J} H_j$$

DEFINITION extended version

$$B_J(T) = T^{l(J)} - 1$$

$$B_t(T) = \sum_{|J|=t} B_J(T)$$

PROPOSITION

The following relation between the B_t and A_w holds

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

and for the extended version

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

PROPOSITION

The following relation between the B_t and A_w holds

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

and for the extended version

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

THEOREM (Katsman-Tsfasman and Jurrius-P)

The homogeneous weight enumerator of C can be expressed in terms of the B_t as follows

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

and for the extended version

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

This motivic version works over any field of coefficients
The number of codewords in $C \otimes \mathbb{F}_{q^m}$ of weight w is $A_w(q^m)$ and

$$W_C(X,Y,q^m) = W_{C\otimes\mathbb{F}_{q^m}}(X,Y)$$

THEOREM (Katsman-Tsfasman and Jurrius-P)

The homogeneous weight enumerator of C can be expressed in terms of the B_t as follows

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

and for the extended version

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

This motivic version works over any field of coefficients

The number of codewords in $C \otimes \mathbb{F}_{q^m}$ of weight w is $A_w(q^m)$ and

$$W_C(X, Y, q^m) = W_{C \otimes \mathbb{F}_{q^m}}(X, Y)$$

THEOREM (Katsman-Tsfasman and Jurrius-P)

The homogeneous weight enumerator of C can be expressed in terms of the B_t as follows

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

and for the extended version

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

This motivic version works over any field of coefficients
The number of codewords in $C \otimes \mathbb{F}_{q^m}$ of weight w is $A_w(q^m)$ and

$$W_C(X,Y,q^m) = W_{C\otimes\mathbb{F}_{q^m}}(X,Y)$$

The weight distribution of an MDS code of length n and dimension k is given for $w \geq d = n - k + 1$ by

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

and for the extend version

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

PROPOSITION

The weight distribution of an MDS code of length n and dimension k is given for $w \geq d = n - k + 1$ by

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

and for the extend version

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

Arrangement of 4 lines of [4, 3, 2] code

$\bar{A}_1(T) = 0$

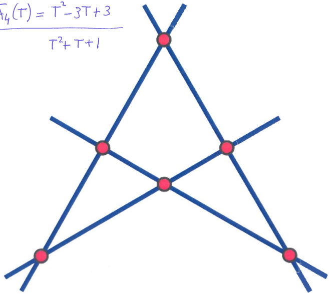
$\bar{A}_2(T) = 6$

$\bar{A}_3(T) = 4(T-2)$

$\bar{A}_4(T) = T^2 - 3T + 3$ +

$T^2 + T + 1$

$$\bar{A}_i(T) = \frac{A_i(T)}{T-1}$$



Connections

The following polynomials determine each other:

$W_C(X, Y, T)$ extended weight enumerator of C

$\{W_C^{(r)}(X, Y) : r = 1, \ldots, k\}$ generalized weight enumerators of C

$t_C(X, Y)$ dichromatic Tutte polynomial of matroid M_C by Greene

$\chi_C(S, T)$ coboundary or two variable char.pol. of geometric lattice L_C

$\zeta_C(S, T)$ two variable zeta function of C by Duursma

But $W_C(X, Y)$ is weaker than $W_C(X, Y, T)$

Connections

The following polynomials determine each other:

$W_C(X, Y, T)$ extended weight enumerator of C

$\{W_C^{(r)}(X, Y) : r = 1, \ldots, k\}$ generalized weight enumerators of C

$t_C(X, Y)$ dichromatic Tutte polynomial of matroid M_C by Greene

$\chi_C(S, T)$ coboundary or two variable char.pol. of geometric lattice L_C

$\zeta_C(S, T)$ two variable zeta function of C by Duursma

But $W_C(X, Y)$ is weaker than $W_C(X, Y, T)$

Connections

The following polynomials determine each other:

$W_C(X, Y, T)$ extended weight enumerator of C

$\{W_C^{(r)}(X, Y) : r = 1, \ldots, k\}$ generalized weight enumerators of C

$t_C(X, Y)$ dichromatic Tutte polynomial of matroid M_C by Greene

$\chi_C(S, T)$ coboundary or two variable char.pol. of geometric lattice L_C

$\zeta_C(S, T)$ two variable zeta function of C by Duursma

But $W_C(X, Y)$ is weaker than $W_C(X, Y, T)$

Connections

The following polynomials determine each other:

$W_C(X, Y, T)$ extended weight enumerator of C

$\{W_C^{(r)}(X, Y) : r = 1, \ldots, k\}$ generalized weight enumerators of C

$t_C(X, Y)$ dichromatic Tutte polynomial of matroid M_C by Greene

$\chi_C(S, T)$ coboundary or two variable char.pol. of geometric lattice L_C

$\zeta_C(S, T)$ two variable zeta function of C by Duursma

But $W_C(X, Y)$ is weaker than $W_C(X, Y, T)$

Connections

The following polynomials determine each other:

$W_C(X, Y, T)$ extended weight enumerator of C

$\{W_C^{(r)}(X, Y) : r = 1, \ldots, k\}$ generalized weight enumerators of C

$t_C(X, Y)$ dichromatic Tutte polynomial of matroid M_C by Greene

$\chi_C(S, T)$ coboundary or two variable char.pol. of geometric lattice L_C

$\zeta_C(S, T)$ two variable zeta function of C by Duursma

But $W_C(X, Y)$ is weaker than $W_C(X, Y, T)$

Connections

The following polynomials determine each other:

$W_C(X, Y, T)$ extended weight enumerator of C

$\{W_C^{(r)}(X, Y) : r = 1, \dots, k\}$ generalized weight enumerators of C

$t_C(X, Y)$ dichromatic Tutte polynomial of matroid M_C by Greene

$\chi_C(S, T)$ coboundary or two variable char.pol. of geometric lattice L_C

$\zeta_C(S, T)$ two variable zeta function of C by Duursma

But $W_C(X, Y)$ is weaker than $W_C(X, Y, T)$

Coset leader weight enumerator

Helleseth, Jurrius-P, Utomo-P

Coset leader weight enumerator

Let C be a linear $[n, k, d]_q$ code
The weight of the coset $\mathbf{y} + C$ is defined by

$$\mathrm{wt}(\mathbf{y} + C) = \min\{\, \mathrm{wt}(\mathbf{y} + \mathbf{c}) \;:\; \mathbf{c} \in C \,\}$$

A coset leader of $\mathbf{r} + C$ is a choice of an element of minimal weight in the coset $\mathbf{r} + C$
Let

$$\alpha_i = \text{ the number of cosets of } C \text{ that are of weight } i$$

The coset leader weight enumerator of C is the polynomial defined by

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

Coset leader weight enumerator

Let C be a linear $[n,k,d]_q$ code
The weight of the coset $\mathbf{y}+C$ is defined by

$$\mathrm{wt}(\mathbf{y}+C)=\min\{\,\mathrm{wt}(\mathbf{y}+\mathbf{c})\ :\ \mathbf{c}\in C\,\}$$

A coset leader of $\mathrm{r}+C$ is a choice of an element of minimal weight in the coset $\mathrm{r}+C$
Let

$$\alpha_i = \text{ the number of cosets of } C \text{ that are of weight } i$$

The coset leader weight enumerator of C is the polynomial defined by

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

Coset leader weight enumerator

Let C be a linear $[n, k, d]_q$ code

The weight of the coset $\mathbf{y} + C$ is defined by

$$\mathrm{wt}(\mathbf{y} + C) = \min\{\, \mathrm{wt}(\mathbf{y} + \mathbf{c}) \ : \ \mathbf{c} \in C \,\}$$

A coset leader of $\mathrm{r} + C$ is a choice of an element of minimal weight in the coset $\mathrm{r} + C$

Let

$$\alpha_i = \text{ the number of cosets of } C \text{ that are of weight } i$$

The coset leader weight enumerator of C is the polynomial defined by

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

Coset leader weight enumerator

Let C be a linear $[n, k, d]_q$ code
The weight of the coset $\mathbf{y} + C$ is defined by

$$\mathrm{wt}(\mathbf{y} + C) = \min\{\, \mathrm{wt}(\mathbf{y} + \mathbf{c}) \;:\; \mathbf{c} \in C \,\}$$

A coset leader of $\mathbf{r} + C$ is a choice of an element of minimal weight in the coset $\mathbf{r} + C$
Let

$$\alpha_i = \text{ the number of cosets of } C \text{ that are of weight } i$$

The coset leader weight enumerator of C is the polynomial defined by

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

Coset leader decoding

The coset leader decoder $\mathcal{D}$ is defined by

- Preprocessing: make a list of all coset leaders
- Input: $\mathbf{r}$ a received word
- Let $\mathbf{e}$ be the chosen coset leader of $\mathbf{r} + C$ in the list
- Output: $\mathcal{D}(\mathbf{r}) = \mathbf{c} = \mathbf{r} - \mathbf{e}$

Then

$$\mathbf{c} \in C \text{ and } d(\mathbf{r}, \mathbf{c}) = \mathrm{wt}(\mathbf{e}) = d(\mathbf{r}, C)$$

Hence $\mathcal{D}$ is a nearest codeword decoder

Note that $\mathbf{c}$ is not necessarily the codeword sent

Coset leader decoding

The coset leader decoder $\mathcal{D}$ is defined by

- Preprocessing: make a list of all coset leaders
- Input: $\mathbf{r}$ a received word
- Let $\mathbf{e}$ be the chosen coset leader of $\mathbf{r} + C$ in the list
- Output: $\mathcal{D}(\mathbf{r}) = \mathbf{c} = \mathbf{r} - \mathbf{e}$

Then

$$\mathbf{c} \in C \text{ and } d(\mathbf{r}, \mathbf{c}) = \mathrm{wt}(\mathbf{e}) = d(\mathbf{r}, C)$$

Hence $\mathcal{D}$ is a nearest codeword decoder

Note that $\mathbf{c}$ is not necessarily the codeword sent

Coset leader decoding

The coset leader decoder $\mathcal{D}$ is defined by
- Preprocessing: make a list of all coset leaders
- Input: $\mathbf{r}$ a received word
- Let $\mathbf{e}$ be the chosen coset leader of $\mathbf{r} + C$ in the list
- Output: $\mathcal{D}(\mathbf{r}) = \mathbf{c} = \mathbf{r} - \mathbf{e}$

Then

$$\mathbf{c} \in C \text{ and } d(\mathbf{r}, \mathbf{c}) = \mathrm{wt}(\mathbf{e}) = d(\mathbf{r}, C)$$

Hence $\mathcal{D}$ is a nearest codeword decoder
Note that $\mathbf{c}$ is not necessarily the codeword sent

$P_{C,dc}$ for coset leader decoder

PROPOSITION

The probability of decoding correctly of the coset leader decoder on a q-ary symmetric channel with cross-over probability p is given by

$$P_{C,dc}(p) = \alpha_C \left(1 - p, \frac{p}{q-1}\right)$$

Properties coset leader weight enumerator

Let C be a linear $[n, k, d]_q$ code with covering radius $\rho(C)$
Then

$$\alpha_i = \binom{n}{i}(q-1)^i \text{ if } i \leq (d-1)/2$$

Since every vector $\mathbf{e}$ of weight at most $(d-1)/2$ is
the unique word of minimal weight in the coset $\mathbf{e} + C$

$$\alpha_i = 0 \text{ if } i > \rho(C)$$

Since by definition there is no word r such that $d(\mathrm{r}, C) > \rho(C)$

$$\alpha_C(1,1) = \sum_{i=0}^{n} \alpha_i = q^{n-k}$$

Since the total number of cosets is q^{n-k}

Properties coset leader weight enumerator

Let C be a linear $[n, k, d]_q$ code with covering radius $\rho(C)$
Then

$$\alpha_i = \binom{n}{i}(q-1)^i \text{ if } i \leq (d-1)/2$$

Since every vector **e** of weight at most $(d-1)/2$ is
the unique word of minimal weight in the coset $\mathbf{e} + C$

$$\alpha_i = 0 \text{ if } i > \rho(C)$$

Since by definition there is no word r such that $d(\mathrm{r}, C) > \rho(C)$

$$\alpha_C(1,1) = \sum_{i=0}^{n} \alpha_i = q^{n-k}$$

Since the total number of cosets is q^{n-k}

Properties coset leader weight enumerator

Let C be a linear $[n, k, d]_q$ code with covering radius $\rho(C)$
Then

$$\alpha_i = \binom{n}{i}(q-1)^i \text{ if } i \leq (d-1)/2$$

Since every vector **e** of weight at most $(d-1)/2$ is
the unique word of minimal weight in the coset $\mathbf{e} + C$

$$\alpha_i = 0 \text{ if } i > \rho(C)$$

Since by definition there is no word r such that $d(\mathrm{r}, C) > \rho(C)$

$$\alpha_C(1,1) = \sum_{i=0}^{n} \alpha_i = q^{n-k}$$

Since the total number of cosets is q^{n-k}

C_n the dual repetition code

Let C_n be the dual code of the n-fold repetition code

So

$$(1, 1, \ldots, 1)$$

is a parity check matrix of C_n

And C_n is an $[n, n-1, 2]_q$ code and we can choose the $(\lambda, 0, \ldots, 0)$ for $\lambda \in \mathbb{F}_q$ as a complete collection of coset leaders

Hence the coset leader weight enumerator of C_n is given by

$$\alpha_{C_n}(X, Y) = X^n + (q-1)X^{n-1}Y^1$$

C_n the dual repetition code

Let C_n be the dual code of the n-fold repetition code

So

$$(1, 1, \ldots, 1)$$

is a parity check matrix of C_n

And C_n is an $[n, n-1, 2]_q$ code and we can choose the $(\lambda, 0, \ldots, 0)$ for $\lambda \in \mathbb{F}_q$ as a complete collection of coset leaders

Hence the coset leader weight enumerator of C_n is given by

$$\alpha_{C_n}(X, Y) = X^n + (q-1)X^{n-1}Y^1$$

C_n the dual repetition code

Let C_n be the dual code of the n-fold repetition code

So

$$(1, 1, \ldots, 1)$$

is a parity check matrix of C_n

And C_n is an $[n, n-1, 2]_q$ code and we can choose the $(\lambda, 0, \ldots, 0)$ for $\lambda \in \mathbb{F}_q$ as a complete collection of coset leaders

Hence the coset leader weight enumerator of C_n is given by

$$\alpha_{C_n}(X, Y) = X^n + (q-1)X^{n-1}Y^1$$

C_n the dual repetition code

Let C_n be the dual code of the n-fold repetition code

So

$$(1, 1, \ldots, 1)$$

is a parity check matrix of C_n

And C_n is an $[n, n-1, 2]_q$ code and we can choose the $(\lambda, 0, \ldots, 0)$ for $\lambda \in \mathbb{F}_q$ as a complete collection of coset leaders

Hence the coset leader weight enumerator of C_n is given by

$$\alpha_{C_n}(X, Y) = X^n + (q-1)X^{n-1}Y^1$$

$C_m \otimes C_n$ product code

Let $C_m \otimes C_n$ be the product code of C_m and C_n
Its codewords are considered as $m \times n$ matrices with entries in $\mathbb{F}_q$
such that every row sum is zero and every column sum is zero

Then $C_m \otimes C_n$ is an $[mn, (m-1)(n-1), 4]_q$ code

Its coset leader weight enumerator is determined
for $q = 2$ and $q = 3$ by Utomo-P
But it is an open question for other q

$C_m \otimes C_n$ product code

Let $C_m \otimes C_n$ be the product code of C_m and C_n
Its codewords are considered as $m \times n$ matrices with entries in $\mathbb{F}_q$
such that every row sum is zero and every column sum is zero

Then $C_m \otimes C_n$ is an $[mn, (m-1)(n-1), 4]_q$ code

Its coset leader weight enumerator is determined
for $q = 2$ and $q = 3$ by Utomo-P
But it is an open question for other q

$C_m \otimes C_n$ product code

Let $C_m \otimes C_n$ be the product code of C_m and C_n
Its codewords are considered as $m \times n$ matrices with entries in $\mathbb{F}_q$
such that every row sum is zero and every column sum is zero

Then $C_m \otimes C_n$ is an $[mn, (m-1)(n-1), 4]_q$ code

Its coset leader weight enumerator is determined
for $q = 2$ and $q = 3$ by Utomo-P
But it is an open question for other q

Extended coset leader weight enumerator

PROPOSITION (Helleseth, Jurrius-P)
Let C be a linear $[n, k, d]_q$ code
Then there exist polynomials $\alpha_i(T)$ such that

$$\alpha_i(q^m) = \text{ the number of cosets of } C \otimes \mathbb{F}_{q^m} \text{ that are of weight } i$$

$\alpha_i(T)$ is divisible by $T - 1$ for $i > 0$
Define $\bar{\alpha}_i(T) = \alpha_i(T)/(T - 1)$

The extended coset leader weight enumerator of C
is the polynomial defined by

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

PROPOSITION (Helleseth, Jurrius-P)
Let C be a linear $[n, k, d]_q$ code
Then there exist polynomials $\alpha_i(T)$ such that

$$\alpha_i(q^m) = \text{ the number of cosets of } C \otimes \mathbb{F}_{q^m} \text{ that are of weight } i$$

$\alpha_i(T)$ is divisible by $T - 1$ for $i > 0$
Define $\bar{\alpha}_i(T) = \alpha_i(T)/(T - 1)$

The extended coset leader weight enumerator of C
is the polynomial defined by

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

PROPOSITION (Helleseth, Jurrius-P)
Let C be a linear $[n, k, d]_q$ code
Then there exist polynomials $\alpha_i(T)$ such that

$$\alpha_i(q^m) = \text{ the number of cosets of } C \otimes \mathbb{F}_{q^m} \text{ that are of weight } i$$

$\alpha_i(T)$ is divisible by $T - 1$ for $i > 0$
Define $\bar{\alpha}_i(T) = \alpha_i(T)/(T - 1)$

The extended coset leader weight enumerator of C
is the polynomial defined by

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

Coset versus syndrome

Let C be a linear $[n, k, d]_q$ code

let H be a parity check matrix of C and $\mathbf{r} \in \mathbb{F}_q^n$
Then

$$\mathbf{r}_1 + C = \mathbf{r}_2 + C \text{ if and only if } H\mathbf{r}_1^T = H\mathbf{r}_2^T$$

Then the column vector

$$\mathbf{s} = H\mathbf{r}^T \in \mathbb{F}_q^{n-k}$$

is called the syndrome of $\mathbf{r}$ with respect to H

Hence there is a one-one correspondence between
cosets of C and syndromes in $\mathbb{F}_q^{n-k}$

Let C be a linear $[n, k, d]_q$ code

let H be a parity check matrix of C and $\mathbf{r} \in \mathbb{F}_q^n$
Then

$$\mathbf{r}_1 + C = \mathbf{r}_2 + C \text{ if and only if } H\mathbf{r}_1^T = H\mathbf{r}_2^T$$

Then the column vector

$$\mathbf{s} = H\mathbf{r}^T \in \mathbb{F}_q^{n-k}$$

is called the syndrome of $\mathbf{r}$ with respect to H

Hence there is a one-one correspondence between cosets of C and syndromes in $\mathbb{F}_q^{n-k}$

Syndrome weight

Let H be a parity check matrix of a linear $[n, k]$ code C over $\mathbb{F}_q$

The weight of $\mathbf{s}$ with respect to H
also called the syndrome weight of $\mathbf{s}$ is defined by

$$\mathrm{wt}_H(\mathbf{s}) = \mathrm{wt}(\mathbf{r} + C)$$

A syndrome $\mathbf{s}$ is a linear combination of the columns of H

The syndrome weight of of $\mathbf{s}$ is the minimal way to write $\mathbf{s}$
as a linear combination of the columns of a parity check matrix

Hence 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

Syndrome weight

Let H be a parity check matrix of a linear $[n, k]$ code C over $\mathbb{F}_q$

The weight of s with respect to H
also called the syndrome weight of s is defined by

$$\mathrm{wt}_H(\mathbf{s}) = \mathrm{wt}(\mathbf{r} + C)$$

A syndrome s is a linear combination of the columns of H

The syndrome weight of of s is the minimal way to write s
as a linear combination of the columns of a parity check matrix

Hence 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

Syndrome weight

Let H be a parity check matrix of a linear $[n, k]$ code C over $\mathbb{F}_q$

The weight of **s** with respect to H
also called the syndrome weight of **s** is defined by

$$\mathrm{wt}_H(\mathbf{s}) = \mathrm{wt}(\mathbf{r} + C)$$

A syndrome **s** is a linear combination of the columns of H

The syndrome weight of of **s** is the minimal way to write **s**
as a linear combination of the columns of a parity check matrix

Hence 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

Syndrome weight

Let H be a parity check matrix of a linear $[n, k]$ code C over $\mathbb{F}_q$

The weight of $\mathbf{s}$ with respect to H
also called the syndrome weight of $\mathbf{s}$ is defined by

$$\mathrm{wt}_H(\mathbf{s}) = \mathrm{wt}(\mathbf{r} + C)$$

A syndrome $\mathbf{s}$ is a linear combination of the columns of H

The syndrome weight of of $\mathbf{s}$ is the minimal way to write $\mathbf{s}$
as a linear combination of the columns of a parity check matrix

Hence 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

Syndrome weight

Let H be a parity check matrix of a linear $[n, k]$ code C over $\mathbb{F}_q$

The weight of $\mathbf{s}$ with respect to H
also called the syndrome weight of $\mathbf{s}$ is defined by

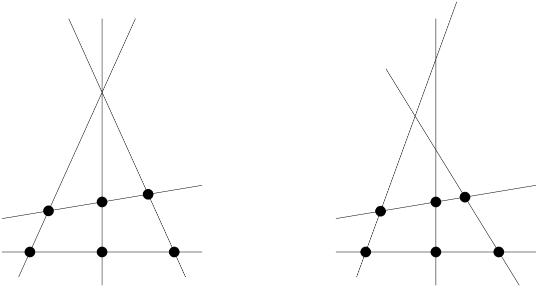
$$\mathrm{wt}_H(\mathbf{s}) = \mathrm{wt}(\mathbf{r} + C)$$

A syndrome $\mathbf{s}$ is a linear combination of the columns of H

The syndrome weight of of $\mathbf{s}$ is the minimal way to write $\mathbf{s}$
as a linear combination of the columns of a parity check matrix

Hence 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

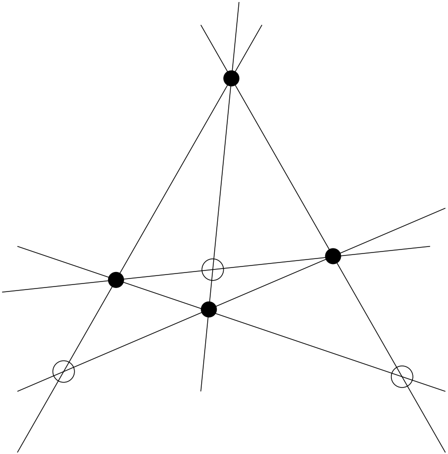
Projective systems of H of $[6, 3, 3]$ codes



Figuur: Two projective systems that induce the same geometric lattice, but induce codes with different coset leader weight enumerators

Derived arrangement of projective system

Derived arrangement of H of $[4, 1, 4]$ code



Normal Rational Curve

Segre, ... , Bruen-Hirschfeld, Blokhuis-P-Szőnyi

Normal rational curve $\mathcal{C}_r$

The normal rational curve of degree r is the curve $\mathcal{C}_r$ in $\mathbb{P}^r$ with parametric representation

$$(s^r : s^{r-1}t : \ldots : st^{r-1} : t^r) \text{ with } (s : t) \in \mathbb{P}^1$$

Alternatively given by the vanishing ideal $I(\mathcal{C}_r)$ that is generated by the 2×2 minors of the $2 \times r$ matrix

$$\begin{pmatrix} X_0 & X_1 & \ldots & X_i & \ldots & X_{r-1} \\ X_1 & X_2 & \ldots & X_{i+1} & \ldots & X_r \end{pmatrix}.$$

$\mathcal{C}_2$ is the irreducible conic in $\mathbb{P}^2$
$\mathcal{C}_3$ is the twisted conic in $\mathbb{P}^3$

Normal rational curve $\mathcal{C}_r$

The normal rational curve of degree r is the curve $\mathcal{C}_r$ in $\mathbb{P}^r$ with parametric representation

$$(s^r : s^{r-1}t : \ldots : st^{r-1} : t^r) \text{ with } (s:t) \in \mathbb{P}^1$$

Alternatively given by the vanishing ideal $I(\mathcal{C}_r)$ that is generated by the 2×2 minors of the $2 \times r$ matrix

$$\left(\begin{array}{cccccc} X_0 & X_1 & \ldots & X_i & \ldots & X_{r-1} \\ X_1 & X_2 & \ldots & X_{i+1} & \ldots & X_r \end{array} \right).$$

$\mathcal{C}_2$ is the irreducible conic in $\mathbb{P}^2$
$\mathcal{C}_3$ is the twisted conic in $\mathbb{P}^3$

Normal rational curve $\mathcal{C}_r$

The normal rational curve of degree r is the curve $\mathcal{C}_r$ in $\mathbb{P}^r$ with parametric representation

$$(s^r : s^{r-1}t : \ldots : st^{r-1} : t^r) \text{ with } (s:t) \in \mathbb{P}^1$$

Alternatively given by the vanishing ideal $I(\mathcal{C}_r)$ that is generated by the 2×2 minors of the $2 \times r$ matrix

$$\begin{pmatrix} X_0 & X_1 & \ldots & X_i & \ldots & X_{r-1} \\ X_1 & X_2 & \ldots & X_{i+1} & \ldots & X_r \end{pmatrix}.$$

$\mathcal{C}_2$ is the irreducible conic in $\mathbb{P}^2$

$\mathcal{C}_3$ is the twisted conic in $\mathbb{P}^3$

Normal rational curve $\mathcal{C}_r$

The normal rational curve of degree r is the curve $\mathcal{C}_r$ in $\mathbb{P}^r$ with parametric representation

$$(s^r : s^{r-1}t : \ldots : st^{r-1} : t^r) \text{ with } (s:t) \in \mathbb{P}^1$$

Alternatively given by the vanishing ideal $I(\mathcal{C}_r)$ that is generated by the 2×2 minors of the $2 \times r$ matrix

$$\begin{pmatrix} X_0 & X_1 & \ldots & X_i & \ldots & X_{r-1} \\ X_1 & X_2 & \ldots & X_{i+1} & \ldots & X_r \end{pmatrix}.$$

$\mathcal{C}_2$ is the irreducible conic in $\mathbb{P}^2$
$\mathcal{C}_3$ is the twisted conic in $\mathbb{P}^3$

NRC and generalized Reed-Solomon codes

$\mathcal{C}_r(\mathbb{F}_q)$ has $q+1$ points lying in general position in $\mathbb{P}^r(\mathbb{F}_q)$

The projective system of these $q+1$ points in $\mathbb{P}^r(\mathbb{F}_q)$ comes from a generalized Reed-Solomon (GRS) code with parameters $[q+1, r+1, q+1-r]$

The dual code is again a generalized Reed-Solomon code with parameters $[q+1, q-r, r+2]$

NRC and generalized Reed-Solomon codes

$\mathcal{C}_r(\mathbb{F}_q)$ has $q+1$ points lying in general position in $\mathbb{P}^r(\mathbb{F}_q)$

The projective system of these $q+1$ points in $\mathbb{P}^r(\mathbb{F}_q)$ comes from a generalized Reed-Solomon (GRS) code with parameters $[q+1, r+1, q+1-r]$

The dual code is again a generalized Reed-Solomon code with parameters $[q+1, q-r, r+2]$

NRC and generalized Reed-Solomon codes

$\mathcal{C}_r(\mathbb{F}_q)$ has $q+1$ points lying in general position in $\mathbb{P}^r(\mathbb{F}_q)$

The projective system of these $q+1$ points in $\mathbb{P}^r(\mathbb{F}_q)$ comes from a generalized Reed-Solomon (GRS) code with parameters $[q+1, r+1, q+1-r]$

The dual code is again a generalized Reed-Solomon code with parameters $[q+1, q-r, r+2]$

Code on the conic $\mathcal{C}_2$

$\mathcal{C}_2(\mathbb{F}_q)$ has $q+1$ points lying in general position in $\mathbb{P}^2(\mathbb{F}_q)$

Lines intersect $\mathcal{C}_2(\mathbb{F}_q)$ in 0, 1 or 2 points and
are called exterior lines, tangents and secants, resp.

Consider the projective system $\mathcal{P}_H$ of these points in $\mathbb{P}^2(\mathbb{F}_q)$
coming from the $3 \times (q+1)$ parity check matrix H
of the (GRS) code with parameters $[q+1, q-2, 4]$

Code on the conic $\mathcal{C}_2$

$\mathcal{C}_2(\mathbb{F}_q)$ has $q+1$ points lying in general position in $\mathbb{P}^2(\mathbb{F}_q)$

Lines intersect $\mathcal{C}_2(\mathbb{F}_q)$ in 0, 1 or 2 points and
are called exterior lines, tangents and secants, resp.

Consider the projective system $\mathcal{P}_H$ of these points in $\mathbb{P}^2(\mathbb{F}_q)$
coming from the $3 \times (q+1)$ parity check matrix H
of the (GRS) code with parameters $[q+1, q-2, 4]$

Code on the conic $\mathcal{C}_2$

$\mathcal{C}_2(\mathbb{F}_q)$ has $q+1$ points lying in general position in $\mathbb{P}^2(\mathbb{F}_q)$

Lines intersect $\mathcal{C}_2(\mathbb{F}_q)$ in 0, 1 or 2 points and
are called exterior lines, tangents and secants, resp.

Consider the projective system $\mathcal{P}_H$ of these points in $\mathbb{P}^2(\mathbb{F}_q)$
coming from the $3 \times (q+1)$ parity check matrix H
of the (GRS) code with parameters $[q+1, q-2, 4]$

Points in plane w.r.t. to $\mathcal{C}_2(\mathbb{F}_q)$ for q odd

- There are $\binom{q+1}{2}$ external points of $\mathcal{P}$, through such a point are
  2 tangents of $\mathcal{P}$
  $\frac{1}{2}(q-1)$ secants of $\mathcal{P}$ and
  $\frac{1}{2}(q-1)$ exterior lines of $\mathcal{P}$
- There are $q+1$ points on $\mathcal{P}$, through such a point there is
  1 tangent of $\mathcal{P}$ and
  q secants of $\mathcal{P}$
- There are $\binom{q}{2}$ internal points of $\mathcal{P}$, through such a point are
  0 tangents of $\mathcal{P}$
  $\frac{1}{2}(q+1)$ secants of $\mathcal{P}$ and
  $\frac{1}{2}(q+1)$ exterior lines of $\mathcal{P}$

Points in plane w.r.t. to $\mathcal{C}_2(\mathbb{F}_q)$ for q odd

- There are $\binom{q+1}{2}$ external points of $\mathcal{P}$, through such a point are
  2 tangents of $\mathcal{P}$
  $\frac{1}{2}(q-1)$ secants of $\mathcal{P}$ and
  $\frac{1}{2}(q-1)$ exterior lines of $\mathcal{P}$
- There are $q+1$ points on $\mathcal{P}$, through such a point there is
  1 tangent of $\mathcal{P}$ and
  q secants of $\mathcal{P}$
- There are $\binom{q}{2}$ internal points of $\mathcal{P}$, through such a point are
  0 tangents of $\mathcal{P}$
  $\frac{1}{2}(q+1)$ secants of $\mathcal{P}$ and
  $\frac{1}{2}(q+1)$ exterior lines of $\mathcal{P}$

Points in plane w.r.t. to $\mathcal{C}_2(\mathbb{F}_q)$ for q odd

- There are $\binom{q+1}{2}$ external points of $\mathcal{P}$, through such a point are
  2 tangents of $\mathcal{P}$
  $\frac{1}{2}(q-1)$ secants of $\mathcal{P}$ and
  $\frac{1}{2}(q-1)$ exterior lines of $\mathcal{P}$
- There are $q+1$ points on $\mathcal{P}$, through such a point there is
  1 tangent of $\mathcal{P}$ and
  q secants of $\mathcal{P}$
- There are $\binom{q}{2}$ internal points of $\mathcal{P}$, through such a point are
  0 tangents of $\mathcal{P}$
  $\frac{1}{2}(q+1)$ secants of $\mathcal{P}$ and
  $\frac{1}{2}(q+1)$ exterior lines of $\mathcal{P}$

Coset leader wt. enum. on conic for q odd

Suppose q is odd and $\mathcal{P}_H$ consists of the $q+1$ points of $\mathcal{C}_2(\mathbb{F}_q)$

Then

- $\bar{\alpha}_1(T) = q+1$
- $\bar{\alpha}_2(T) = (q^2+q+1-(q+1)) + \binom{q+1}{2}(T-q)$
- $\bar{\alpha}_3(T) = \text{remaining points}$

$$= T^2 + (1-\binom{q+1}{2})T - q(q+1) + q\binom{q+1}{2}$$

since

$$\bar{\alpha}_1(T) + \bar{\alpha}_2(T) + \bar{\alpha}_3(T) = T^2 + T + 1$$

Coset leader wt. enum. on conic for q odd

Suppose q is odd and $\mathcal{P}_H$ consists of the $q+1$ points of $\mathcal{C}_2(\mathbb{F}_q)$

Then

- $\bar{\alpha}_1(T) = q+1$
- $\bar{\alpha}_2(T) = (q^2+q+1-(q+1)) + \binom{q+1}{2}(T-q)$
- $\bar{\alpha}_3(T) =$ remaining points

$$= T^2 + (1-\tbinom{q+1}{2})T - q(q+1) + q\tbinom{q+1}{2}$$

since

$$\bar{\alpha}_1(T) + \bar{\alpha}_2(T) + \bar{\alpha}_3(T) = T^2 + T + 1$$

Coset leader wt. enum. on conic for q odd

Suppose q is odd and $\mathcal{P}_H$ consists of the $q+1$ points of $\mathcal{C}_2(\mathbb{F}_q)$

Then

- $\bar{\alpha}_1(T) = q + 1$
- $\bar{\alpha}_2(T) = (q^2 + q + 1 - (q+1)) + \binom{q+1}{2}(T - q)$
- $\bar{\alpha}_3(T) =$ remaining points

$$= T^2 + (1 - \binom{q+1}{2})T - q(q+1) + q\binom{q+1}{2}$$

since

$$\bar{\alpha}_1(T) + \bar{\alpha}_2(T) + \bar{\alpha}_3(T) = T^2 + T + 1$$

Technische Universiteit Eindhoven University of Technology

Suppose q is odd and $\mathcal{P}_H$ consists of the $q+1$ points of $\mathcal{C}_2(\mathbb{F}_q)$

Then

- $\bar{\alpha}_1(T) = q+1$
- $\bar{\alpha}_2(T) = (q^2+q+1-(q+1)) + \binom{q+1}{2}(T-q)$
- $\bar{\alpha}_3(T) =$ remaining points

$$= T^2 + (1 - \binom{q+1}{2})T - q(q+1) + q\binom{q+1}{2}$$

since

$$\bar{\alpha}_1(T) + \bar{\alpha}_2(T) + \bar{\alpha}_3(T) = T^2 + T + 1$$

Coset leader wt. enum. on conic for q odd

Suppose q is odd and $\mathcal{P}_H$ consists of the $q+1$ points of $\mathcal{C}_2(\mathbb{F}_q)$

Then

- $\bar{\alpha}_1(T) = q+1$
- $\bar{\alpha}_2(T) = (q^2+q+1-(q+1)) + \binom{q+1}{2}(T-q)$
- $\bar{\alpha}_3(T) =$ remaining points

$$= T^2 + (1 - \binom{q+1}{2})T - q(q+1) + q\binom{q+1}{2}$$

since

$$\bar{\alpha}_1(T) + \bar{\alpha}_2(T) + \bar{\alpha}_3(T) = T^2 + T + 1$$

Coset leader wt. enum. on conic for q odd

Suppose q is odd and $\mathcal{P}_H$ consists of the $q+1$ points of $\mathcal{C}_2(\mathbb{F}_q)$

Then

- $\bar{\alpha}_1(T) = q + 1$
- $\bar{\alpha}_2(T) = (q^2 + q + 1 - (q+1)) + \binom{q+1}{2}(T - q)$
- $\bar{\alpha}_3(T) =$ remaining points

$$= T^2 + (1 - \binom{q+1}{2})T - q(q+1) + q\binom{q+1}{2}$$

since

$$\bar{\alpha}_1(T) + \bar{\alpha}_2(T) + \bar{\alpha}_3(T) = T^2 + T + 1$$

Code on the twisted cubic $\mathcal{C}_3$

$\mathcal{C}_3(\mathbb{F}_q)$ has $q+1$ points lying in general position in $\mathbb{P}^3(\mathbb{F}_q)$

Lines intersect $\mathcal{C}_3(\mathbb{F}_q)$ in 0, 1, 2 or 3 points
An i-plane, $i = 0, 1, 2, 3$, is a plane containing exactly i points of $\mathcal{C}_3(q)$

Consider the projective system $\mathcal{P}_H$ of these points in $\mathbb{P}^2(\mathbb{F}_q)$
coming from the $4 \times (q+1)$ parity check matrix H
of the (GRS) code with parameters $[q+1, q-3, 5]$

Code on the twisted cubic $\mathcal{C}_3$

$\mathcal{C}_3(\mathbb{F}_q)$ has $q+1$ points lying in general position in $\mathbb{P}^3(\mathbb{F}_q)$

Lines intersect $\mathcal{C}_3(\mathbb{F}_q)$ in 0, 1, 2 or 3 points
An *i*-plane, $i = 0, 1, 2, 3$, is a plane containing exactly i points of $\mathcal{C}_3(q)$

Consider the projective system $\mathcal{P}_H$ of these points in $\mathbb{P}^2(\mathbb{F}_q)$
coming from the $4 \times (q+1)$ parity check matrix H
of the (GRS) code with parameters $[q+1, q-3, 5]$

Code on the twisted cubic $\mathcal{C}_3$

$\mathcal{C}_3(\mathbb{F}_q)$ has $q+1$ points lying in general position in $\mathbb{P}^3(\mathbb{F}_q)$

Lines intersect $\mathcal{C}_3(\mathbb{F}_q)$ in 0, 1, 2 or 3 points
An *i*-plane, $i = 0, 1, 2, 3$, is a plane containing exactly i points of $\mathcal{C}_3(q)$

Consider the projective system $\mathcal{P}_H$ of these points in $\mathbb{P}^2(\mathbb{F}_q)$
coming from the $4 \times (q+1)$ parity check matrix H
of the (GRS) code with parameters $[q+1, q-3, 5]$

Coset leader wt. enum. on twisted cubic

The number of points on the twisted cubic
so

$$\bar{\alpha}_1(T) = q + 1$$

There are $\frac{1}{2}q(q+1)$ secants, each one of them contributes

$$(T+1) - 2 = T - 1$$

Hence

$$\bar{\alpha}_2(T) = \frac{1}{2}q(q+1)(T-1)$$

The number of points on the twisted cubic
so

$$\bar{\alpha}_1(T) = q + 1$$

There are $\frac{1}{2}q(q+1)$ secants, each one of them contributes

$$(T+1) - 2 = T - 1$$

Hence

$$\bar{\alpha}_2(T) = \frac{1}{2}q(q+1)(T-1)$$

The number of points on the twisted cubic
so

$$\bar{\alpha}_1(T) = q + 1$$

There are $\frac{1}{2}q(q+1)$ secants, each one of them contributes

$$(T+1) - 2 = T - 1$$

Hence

$$\bar{\alpha}_2(T) = \frac{1}{2}q(q+1)(T-1)$$

Value of $\bar{\alpha}_3(q)$

What is the number of points that are on a 3-plane
that is a plane containing three points of the twisted cubic $\mathcal{C}_3(\mathbb{F}_q)$
not already counted under $\bar{\alpha}_1$ or $\bar{\alpha}_2$?

In $\mathbb{P}^3(\mathbb{F}_q)$ the answer is easy:
the rest, so $\frac{1}{2}q(q+1)^2$
since a point that does not lie on the curve or on a secant or on a 3-plane
can be used to extend the arc
But it is well known that the arc is maximal (for $q > 3$)

Hence

$$\bar{\alpha}_3(q) = \frac{1}{2}q(q+1)^2$$

Value of $\bar{\alpha}_3(q)$

What is the number of points that are on a 3-plane
that is a plane containing three points of the twisted cubic $\mathcal{C}_3(\mathbb{F}_q)$
not already counted under $\bar{\alpha}_1$ or $\bar{\alpha}_2$?

In $\mathbb{P}^3(\mathbb{F}_q)$ the answer is easy:
the rest, so $\frac{1}{2}q(q+1)^2$
since a point that does not lie on the curve or on a secant or on a 3-plane
can be used to extend the arc
But it is well known that the arc is maximal (for $q > 3$)

Hence

$$\bar{\alpha}_3(q) = \frac{1}{2}q(q+1)^2$$

Value of $\bar{\alpha}_3(q)$

What is the number of points that are on a 3-plane
that is a plane containing three points of the twisted cubic $\mathcal{C}_3(\mathbb{F}_q)$
not already counted under $\bar{\alpha}_1$ or $\bar{\alpha}_2$?

In $\mathbb{P}^3(\mathbb{F}_q)$ the answer is easy:
the rest, so $\frac{1}{2}q(q+1)^2$
since a point that does not lie on the curve or on a secant or on a 3-plane
can be used to extend the arc
But it is well known that the arc is maximal (for $q > 3$)

Hence

$$\bar{\alpha}_3(q) = \frac{1}{2}q(q+1)^2$$

Value of $\bar{\alpha}_3(q)$

What is the number of points that are on a 3-plane
that is a plane containing three points of the twisted cubic $\mathcal{C}_3(\mathbb{F}_q)$
not already counted under $\bar{\alpha}_1$ or $\bar{\alpha}_2$?

In $\mathbb{P}^3(\mathbb{F}_q)$ the answer is easy:
the rest, so $\frac{1}{2}q(q+1)^2$
since a point that does not lie on the curve or on a secant or on a 3-plane
can be used to extend the arc
But it is well known that the arc is maximal (for $q > 3$)

Hence

$$\bar{\alpha}_3(q) = \frac{1}{2}q(q+1)^2$$

Value of $\bar{\alpha}_3(T)$

Now outside $\mathbb{P}^3(\mathbb{F}_q)$ we argue as follows
If a point is on more than one 3-plane
then it must be on a line of $\mathbb{P}^3(\mathbb{F}_q)$
so forgetting about these points for the moment
This means that each of the $(q+1)q(q-1)/6$ different 3-planes contributes

$$T^2 + T + 1 - (q^2+q+1) - (q^2+q+1)(T-q)$$

points that are in this 3-plane only
So

$$\bar{\alpha}_3(T) = \frac{1}{2}q(q+1)^2 +$$

$$+\frac{1}{6}(q+1)q(q-1)\left(T^2+T+1-(q^2+q+1)(T-q+1)\right)+$$

$$(T-q)\mu_q$$

Value of $\bar{\alpha}_3(T)$

Now outside $\mathbb{P}^3(\mathbb{F}_q)$ we argue as follows
If a point is on more than one 3-plane
then it must be on a line of $\mathbb{P}^3(\mathbb{F}_q)$
so forgetting about these points for the moment
This means that each of the $(q+1)q(q-1)/6$ different 3-planes contributes

$$T^2 + T + 1 - (q^2 + q + 1) - (q^2 + q + 1)(T - q)$$

points that are in this 3-plane only
So

$$\bar{\alpha}_3(T) = \frac{1}{2}q(q+1)^2 +$$

$$+\frac{1}{6}(q+1)q(q-1)\left(T^2 + T + 1 - (q^2+q+1)(T-q+1)\right) +$$

$$(T-q)\mu_q$$

Value of $\bar{\alpha}_3(T)$

Now outside $\mathbb{P}^3(\mathbb{F}_q)$ we argue as follows
If a point is on more than one 3-plane
then it must be on a line of $\mathbb{P}^3(\mathbb{F}_q)$
so forgetting about these points for the moment
This means that each of the $(q+1)q(q-1)/6$ different 3-planes contributes

$$T^2 + T + 1 - (q^2 + q + 1) - (q^2 + q + 1)(T - q)$$

points that are in this 3-plane only
So

$$\bar{\alpha}_3(T) = \frac{1}{2}q(q+1)^2 +$$

$$+\frac{1}{6}(q+1)q(q-1)\left(T^2 + T + 1 - (q^2 + q + 1)(T - q + 1)\right) +$$

$$(T - q)\mu_q$$

Value of $\bar{\alpha}_3(T)$

Now outside $\mathbb{P}^3(\mathbb{F}_q)$ we argue as follows
If a point is on more than one 3-plane
then it must be on a line of $\mathbb{P}^3(\mathbb{F}_q)$
so forgetting about these points for the moment
This means that each of the $(q+1)q(q-1)/6$ different 3-planes contributes

$$T^2 + T + 1 - (q^2 + q + 1) - (q^2 + q + 1)(T - q)$$

points that are in this 3-plane only
So

$$\bar{\alpha}_3(T) = \frac{1}{2}q(q+1)^2 +$$

$$+\frac{1}{6}(q+1)q(q-1)\left(T^2 + T + 1 - (q^2 + q + 1)(T - q + 1)\right) +$$

$$(T-q)\mu_q$$

Value of $\bar{\alpha}_3(T)$

Now outside $\mathbb{P}^3(\mathbb{F}_q)$ we argue as follows
If a point is on more than one 3-plane
then it must be on a line of $\mathbb{P}^3(\mathbb{F}_q)$
so forgetting about these points for the moment
This means that each of the $(q+1)q(q-1)/6$ different 3-planes contributes

$$T^2 + T + 1 - (q^2 + q + 1) - (q^2 + q + 1)(T - q)$$

points that are in this 3-plane only
So

$$\bar{\alpha}_3(T) = \frac{1}{2} q(q+1)^2 +$$

$$+ \frac{1}{6}(q+1)q(q-1)\left(T^2 + T + 1 - (q^2+q+1)(T - q + 1)\right) +$$

$$(T - q)\mu_q$$

Value of μ_q

$$\mu_q = \begin{cases} q^4 + \frac{1}{2}q^3 - \frac{3}{2}q^2 - q & \text{if} \quad q = 1 \mod 6 \\ q^4 + q^3 - \frac{3}{2}q^2 - \frac{1}{2}q & \text{if} \quad q = 2 \mod 6 \\ q^4 + \frac{1}{2}q^3 + \frac{3}{2}q^2 - 1 & \text{if} \quad q = 3 \mod 6 \\ q^4 - q^3 + \frac{1}{2}q^2 - \frac{1}{2}q - 1 & \text{if} \quad q = 4 \mod 6 \\ q^4 + \frac{1}{2}q^3 + \frac{1}{2}q^2 & \text{if} \quad q = 5 \mod 6 \end{cases}$$

Conclusion

Computing the weight enumerator is hard

Computing the coset leader weight enumerator is very hard

Even the case of the twisted cubic is complicated

What about the normal rational curve of degree $r > 3$?

New ideas are needed!

Hopefully you will contribute

THANKS YOU!

Conclusion

Computing the weight enumerator is hard

Computing the coset leader weight enumerator is very hard

Even the case of the twisted cubic is complicated

What about the normal rational curve of degree $r > 3$?

New ideas are needed!

Hopefully you will contribute

THANKS YOU!

Conclusion

Computing the weight enumerator is hard

Computing the coset leader weight enumerator is very hard

Even the case of the twisted cubic is complicated

What about the normal rational curve of degree $r > 3$?

New ideas are needed!

Hopefully you will contribute

THANKS YOU!

Conclusion

Computing the weight enumerator is hard

Computing the coset leader weight enumerator is very hard

Even the case of the twisted cubic is complicated

What about the normal rational curve of degree $r > 3$?

New ideas are needed!

Hopefully you will contribute

THANKS YOU!

Conclusion

Computing the weight enumerator is hard

Computing the coset leader weight enumerator is very hard

Even the case of the twisted cubic is complicated

What about the normal rational curve of degree $r > 3$?

New ideas are needed!

Hopefully you will contribute

THANKS YOU!

Conclusion

Computing the weight enumerator is hard

Computing the coset leader weight enumerator is very hard

Even the case of the twisted cubic is complicated

What about the normal rational curve of degree $r > 3$?

New ideas are needed!

Hopefully you will contribute

THANKS YOU!

Conclusion

Computing the weight enumerator is hard

Computing the coset leader weight enumerator is very hard

Even the case of the twisted cubic is complicated

What about the normal rational curve of degree $r > 3$?

New ideas are needed!

Hopefully you will contribute

THANKS YOU!

Technische Universiteit Eindhoven University of Technology