

Weight enumeration of codes from finite spaces

Relinde Jurrius

Eindhoven University of Technology, The Netherlands

Fq10: Finite Fields and their Applications
July 11–15, 2011, Ghent, Belgium

Outline

Projective systems and weight enumeration

Generalized weight enumerator

Codes from finite spaces

- Finite projective space: simplex code

- Finite affine space: 1-st order Reed-Muller code

Extended weight enumerator

Further questions and applications

Projective systems

projective system n -tuple $\mathcal{P} = (P_1, \dots, P_n)$

points $P_j \in \text{PG}(r, q)$ in general position

Matrix $G_{\mathcal{P}}$ with coordinates of points of \mathcal{P} as columns generates linear $[n, r + 1]$ code.

$$\left\{ \begin{array}{l} \text{equiv. classes of} \\ \text{linear } [n, k] \text{ codes} \\ \text{over GF}(q) \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \text{equiv. classes of} \\ \text{proj. systems of length } n \\ \text{over PG}(k - 1, q) \end{array} \right\}$$

Weights in linear codes

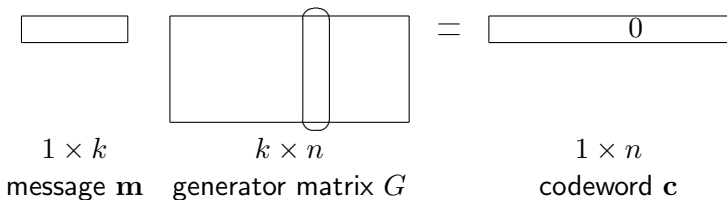
$1 \times k$
message \mathbf{m}

$k \times n$
generator matrix G

$=$

$1 \times n$
codeword \mathbf{c}

Weights in linear codes



Theorem

$$c_j = 0 \iff P_j \text{ is in nullspace of } \mathbf{m}$$

We can determine weights by counting points P_j on hyperplanes.

Generalized weight enumerator

For a subcode $D \subseteq C$ we define

support $\text{supp}(D)$ union of the support of all words in D

zero set $\text{zero}(D)$ complement of support, i.e., all coordinates that are always zero

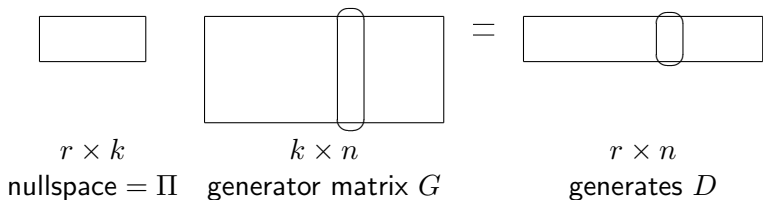
weight $\text{wt}(D)$ size of the support

Generalized weight enumerators

Polynomials counting for every dimension the number of subcodes of a given weight:

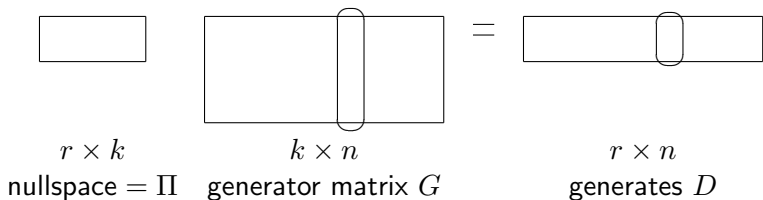
$$W_C^{(r)}(X, Y) = \sum_{\substack{D \subseteq C \\ \dim(D)=r}} X^{|\text{zero}(D)|} Y^{|\text{supp}(D)|}$$

Weight enumeration of subcodes



$$\begin{array}{l} \Pi \subseteq \text{PG}(k-1, q) \\ \text{codim}(\Pi) = r \end{array} \longleftrightarrow \begin{array}{l} D \subseteq C \\ \dim(D) = r \end{array}$$

Weight enumeration of subcodes



$$\begin{array}{l} \Pi \subseteq \text{PG}(k-1, q) \\ \text{codim}(\Pi) = r \end{array} \iff \begin{array}{l} D \subseteq C \\ \dim(D) = r \end{array}$$

Theorem

$$j \in \text{zero}(D) \iff P_j \in \Pi$$

Codes from finite spaces

Let \mathcal{P} contain all points in $\text{PG}(s-1, q)$. The corresponding code is the **simplex code** $\mathcal{S}_q(s)$. It has length $\frac{q^s - 1}{q - 1}$ and dimension s .

Example

$\mathcal{S}_2(3)$ has generator matrix

$$G_{\mathcal{P}} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}$$

Codes from finite spaces

$$\begin{array}{ccc} \Pi \subseteq \text{PG}(s-1, q) & \longleftrightarrow & D \subseteq C \\ \text{codim}(\Pi) = r & & \dim(D) = r \end{array}$$

- $j \in \text{zero}(D) \iff P_j \in \Pi$
- \mathcal{P} contains all points in $\text{PG}(s-1, q)$
- $|\text{zero}(D)| = |\Pi|$ for all D

Theorem

$$W_{\mathcal{S}_q(s)}^{(r)}(X, Y) = \begin{bmatrix} s \\ r \end{bmatrix}_q X^{(q^{s-r}-1)/(q-1)} Y^{(q^s-q^{s-r})/(q-1)}$$

Codes from finite spaces

Let \mathcal{P} contain all points in $AG(s-1, q)$, viewed as all points in $PG(s-1, q)$ not on a hyperplane H . The corresponding code is the **1-st order Reed Muller code** $\mathcal{RM}_q(1, s-1)$. It has length q^{s-1} and dimension s .

Example

$\mathcal{RM}_2(1, 3)$ has generator matrix

$$G_{\mathcal{P}} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}$$

Codes from finite spaces

$$\begin{array}{ccc} \Pi \subseteq \text{PG}(s-1, q) & \longleftrightarrow & D \subseteq C \\ \text{codim}(\Pi) = r & & \dim(D) = r \end{array}$$

- $j \in \text{zero}(D) \iff P_j \in \Pi$
- if $\Pi \subseteq H$, no P_j is in Π , so $\text{wt}(D) = n$
- if $\Pi \not\subseteq H$, all of the P_j in Π form a subspace of $\text{AG}(s-1, q)$ of codimension r

Theorem

$$W_{\mathcal{RM}_q(1, s-1)}^{(r)}(X, Y) = \begin{bmatrix} s-1 \\ r-1 \end{bmatrix}_q Y^n + q^r \begin{bmatrix} s-1 \\ r \end{bmatrix}_q X^{q^{s-1-r}} Y^{q^{s-1}-q^{s-1-r}}$$

Extended weight enumerator

For every linear $[n, k]$ code C with generator matrix G we have:

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

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

Extended weight enumerator

For every linear $[n, k]$ code C with generator matrix G we have:

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

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

Extended weight enumerator

Polynomial counting “for all extension codes” the number of words of a given weight:

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

So for $T = q^m$ we have $W_C(X, Y, q^m) = W_{C \otimes \text{GF}(q^m)}(X, Y)$.

Extended weight enumerator

The extended weight enumerator is completely determined by the set of generalized weight enumerators (and vice versa):

Theorem

$$W_C(X, Y, T) = \sum_{r=0}^k \left(\prod_{j=0}^{r-1} (T - q^j) \right) W_C^{(r)}(X, Y).$$

Moreover, their sets of supports are the same.

Supports

Theorem (Simplex code)

*Let $\mathbf{c} \in \mathcal{S}_q(s) \otimes \text{GF}(q^m)$ with $\text{wt}(\mathbf{c}) = (q^s - q^{s-r})/(q-1)$, $r < m$.
Then the points in \mathcal{P} indexed by $\text{zero}(\mathbf{c})$ are all the points in a subspace of $\text{PG}(s-1, q)$ of codimension r .*

Supports

Theorem (Simplex code)

Let $\mathbf{c} \in \mathcal{S}_q(s) \otimes \text{GF}(q^m)$ with $\text{wt}(\mathbf{c}) = (q^s - q^{s-r})/(q-1)$, $r < m$. Then the points in \mathcal{P} indexed by $\text{zero}(\mathbf{c})$ are all the points in a subspace of $\text{PG}(s-1, q)$ of codimension r .

Theorem (1-st order Reed-Muller code)

Let $\mathbf{c} \in \mathcal{RM}_q(1, s) \otimes \text{GF}(q^m)$ with $\text{wt}(\mathbf{c}) = q^{s-1} - q^{s-1-r}$, $r < m$. Then the points in \mathcal{P} indexed by $\text{zero}(\mathbf{c})$ are all the points in a subspace of $\text{AG}(s-1, q)$ of codimension r .

Supports

Theorem (Simplex code)

Let $\mathbf{c} \in \mathcal{S}_q(s) \otimes \text{GF}(q^m)$ with $\text{wt}(\mathbf{c}) = (q^s - q^{s-r})/(q-1)$, $r < m$. Then the points in \mathcal{P} indexed by $\text{zero}(\mathbf{c})$ are all the points in a subspace of $\text{PG}(s-1, q)$ of codimension r .

Theorem (1-st order Reed-Muller code)

Let $\mathbf{c} \in \mathcal{RM}_q(1, s) \otimes \text{GF}(q^m)$ with $\text{wt}(\mathbf{c}) = q^{s-1} - q^{s-1-r}$, $r < m$. Then the points in \mathcal{P} indexed by $\text{zero}(\mathbf{c})$ are all the points in a subspace of $\text{AG}(s-1, q)$ of codimension r .

So: the sets $\text{zero}(\mathbf{c})$ for all codewords contains the incidence design of a finite geometry.

Further questions and applications

- Weight enumeration of higher order Reed-Muller codes

Further questions and applications

- Weight enumeration of higher order Reed-Muller codes
- Generalized Hamming weights of Reed-Muller codes

Further questions and applications

- Weight enumeration of higher order Reed-Muller codes
- Generalized Hamming weights of Reed-Muller codes
- Link with perfect matroid designs and associated polynomials

Further questions and applications

- Weight enumeration of higher order Reed-Muller codes
- Generalized Hamming weights of Reed-Muller codes
- Link with perfect matroid designs and associated polynomials
- Two weight codes: quadratic extension code of simplex code

Further questions and applications

- Weight enumeration of higher order Reed-Muller codes
- Generalized Hamming weights of Reed-Muller codes
- Link with perfect matroid designs and associated polynomials
- Two weight codes: quadratic extension code of simplex code
- Dimension of a design (generalization of p -rank)

Thank you for your attention.