The extended coset leader weight enumerator

Relinde Jurrius Ruud Pellikaan

Eindhoven University of Technology, The Netherlands

Symposium on Information Theory in the Benelux, 2009

Outline

Basic definitions

Linear $[n, k]$ code	Linear subspace $C \subseteq \mathbb{F}_q^n$ 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.
Support	The coordinates of a word which are nonzero.
Weight	The number of nonzero coordinates of a word, i.e. the size of the support.

Basic definitions

Linear $[n, k]$ code Linear subspace $C \subseteq \mathbb{F}_q^n$ 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.

Support The coordinates of a word which are nonzero.

Weight The number of nonzero coordinates of a word, i.e. the size of the support.

Weight enumerator

The homogeneous polynomial counting the number of words of a given weight, notation:

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

Basic definitions

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

$$W_C(X, Y) = X^7 + 7X^4Y^3 + 7X^3Y^4 + Y^7.$$

Extended weight enumerator

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

Extended weight enumerator

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

Extended weight enumerator

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

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

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

Extended weight enumerator

Example

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

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

Cosets and weights

Coset	Translation of the code by some 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.
Covering radius	The maximum possible weight for a coset.

Cosets and weights

Coset	Translation of the code by some 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.
Covering radius	The maximum possible weight for a 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 with $T = q^m$ we have $\alpha_C(X, Y, q^m) = \alpha_{C \otimes \mathbb{F}_{q^m}}(X, Y)$.

Determination of coset weights

Parity check matrix	$(n-k) \times n$ matrix H such that $GH^T = 0$.
Syndrome of $\mathbf{y} \in \mathbb{F}_q^n$	The vector $\mathbf{s} = H\mathbf{y}^T$, zero for codewords.
Syndrome weight	Minimal number of columns which span contains $\mathbf{s}$.

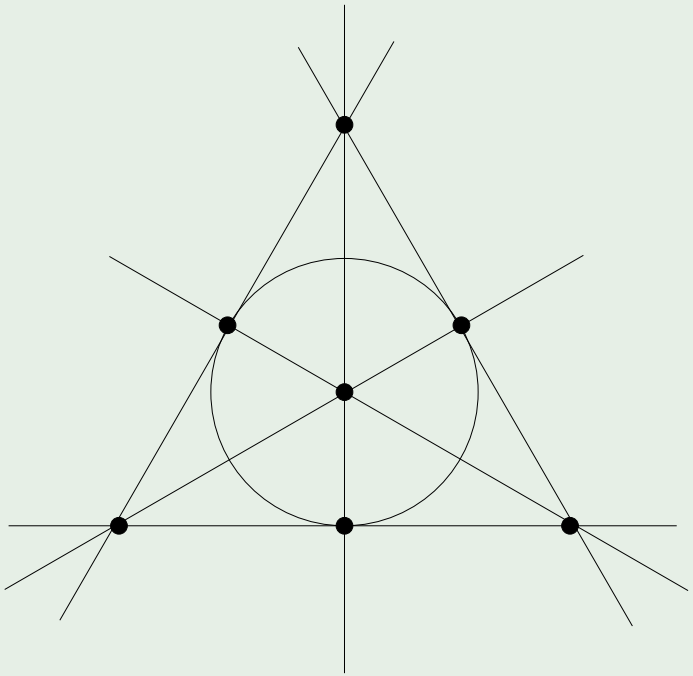
Determination of coset weights

Parity check matrix	$(n-k) \times n$ matrix H such that $GH^T = 0$.
Syndrome of $\mathbf{y} \in \mathbb{F}_q^n$	The vector $\mathbf{s} = H\mathbf{y}^T$, zero for codewords.
Syndrome weight	Minimal number of columns which 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 $[7, 4]$ 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 can be viewed as seven points in a projective plane.

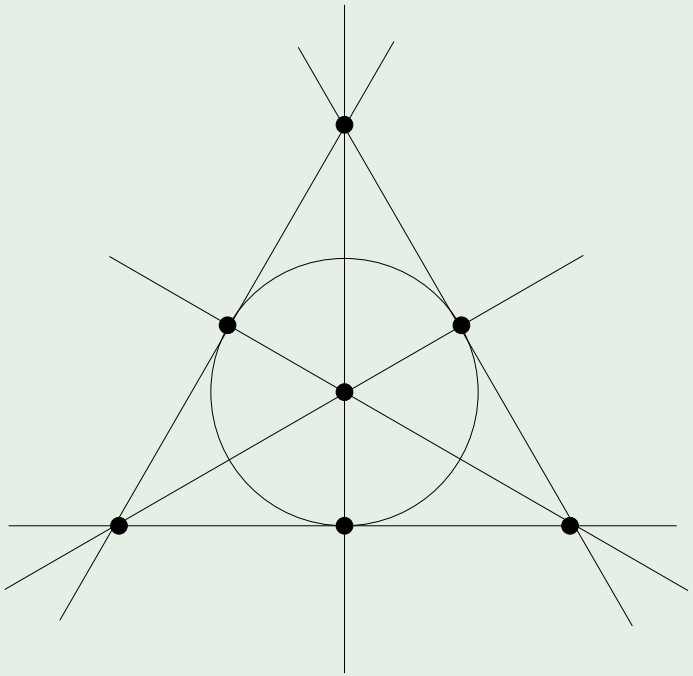
The extended coset leader weights are given by

$$\alpha_0(T) = 1$$

The code itself.

Determination of coset weights

Example



The $[7, 4]$ 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 can be viewed as seven points in a projective plane.

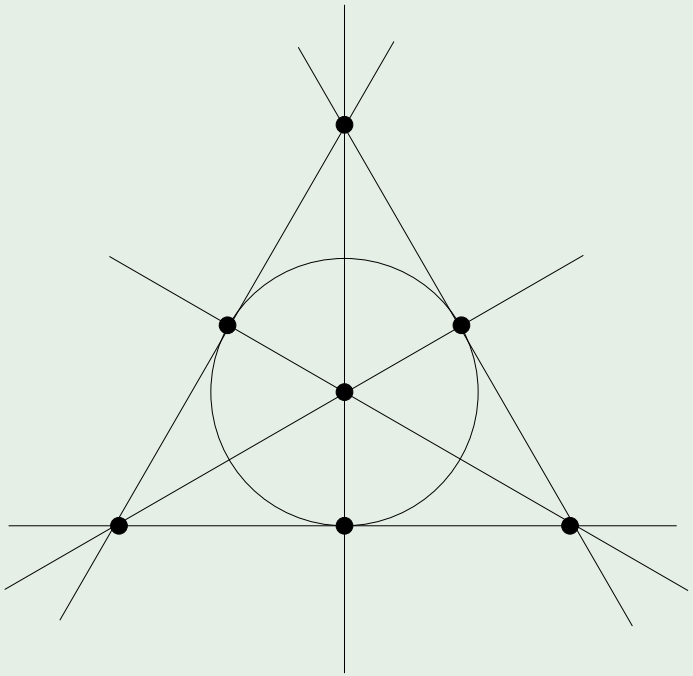
The extended coset leader weights are given by

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

Seven projective points.

Determination of coset weights

Example



The $[7, 4]$ 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 can be viewed as seven points in a projective plane.

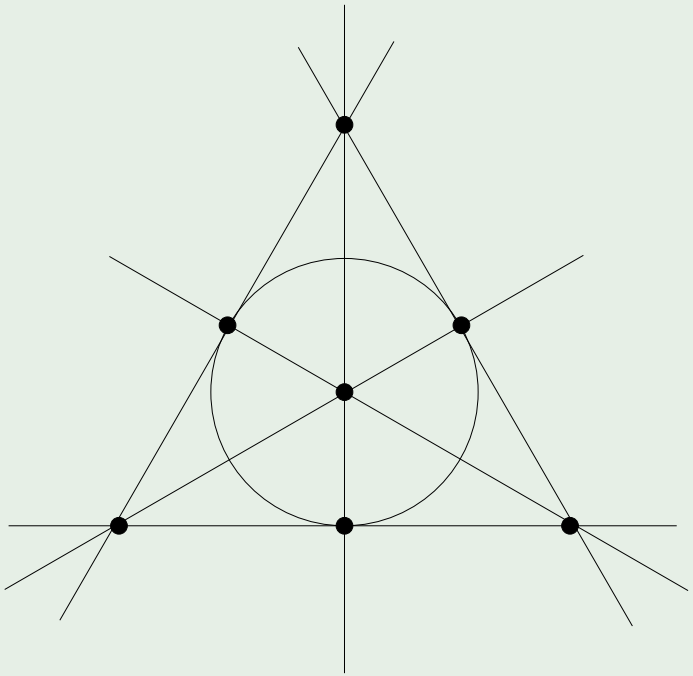
The extended coset leader weights are given by

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

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

Determination of coset weights

Example



The $[7, 4]$ 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 can be viewed as seven points in a 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.

List weight enumerator

Extended list weight enumerator

The polynomial counting the number of vectors of a given weight which are of minimal weight in their coset "for all extension codes", notation:

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

So $\lambda_i(T)$ is the number of possible coset leaders of weight i.

We determine the extended list weight enumerator similar to the extended coset leader weight enumerator.

List weight enumerator

Example

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

$$\begin{aligned}\lambda_C(X, Y, T) &= X^7 + \\ &\quad 7(T-1)X^6Y + \\ &\quad 21(T-1)(T-2)X^5Y^2 + \\ &\quad 28(T-1)(T-2)(T-4)X^4Y^3.\end{aligned}$$

Connections

The extended coset leader weight enumerator $\alpha_C(X, Y, T)$ does NOT determine

- the extended coset leader weight enumerator $\alpha_{C^\perp}(X, Y, T)$ of the dual code;
- the extended list weight enumerator $\lambda_C(X, Y, T)$;
- the extended weight enumerator $W_C(X, Y, T)$.

This can be shown by counterexamples.

Open question: does the extended list weight enumerator $\lambda_C(X, Y, T)$ determine one of the above?

Some applications

Weight enumerator

- Probability of undetected error in error-detection
- Probability of decoding error in bounded distance decoding

Some applications

Weight enumerator

- Probability of undetected error in error-detection
- Probability of decoding error in bounded distance decoding

Coset leader weight enumerator

- Probability of correct decoding in coset leader decoding
- Steganography: average of changed symbols

Some applications

Weight enumerator

- Probability of undetected error in error-detection
- Probability of decoding error in bounded distance decoding

Coset leader weight enumerator

- Probability of correct decoding in coset leader decoding
- Steganography: average of changed symbols

List weight enumerator

- Probability of correct decoding in list decoding