Extended and generalized weight enumerators

Relinde Jurrius    Ruud Pellikaan

Eindhoven University of Technology, The Netherlands

International Workshop on Coding and Cryptography, 2009
Outline

Previous work

Codes, weights and weight enumerators
  Generalized weight enumerator
  Extended weight enumerator

Matroids and the Tutte polynomial

Overview of connections
  Application: MacWilliams relations

Coset leader and list weight enumerator

Further work
Previous work

- A. Barg
  Codes and matroids, generalized WE

- T. Britz
  Codes and matroids, Tutte polynomial

- C. Greene
  Connection Tutte polynomial and weight enumerator

- T. Helleseth
  Extended WE, coset leader WE

- G. Katsman and M. Tsfasman
  Determination of WE

- T. Kløve
  Extended WE, generalized WE, MacWilliams relations

- J. Simonis
  Generalized WE, MacWilliams relations
### Codes, weights and weight enumerators

<table>
<thead>
<tr>
<th>Linear $[n, k]$ code</th>
<th>Linear subspace $C \subseteq \mathbb{F}_q^n$ of dimension $k$. Elements are called <em>(code)words</em>, $n$ is called the <em>length</em>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generator matrix</td>
<td>The rows of this $k \times n$ matrix form a basis for $C$.</td>
</tr>
<tr>
<td>Support</td>
<td>The coordinates of a word which are nonzero.</td>
</tr>
<tr>
<td>Weight</td>
<td>The number of nonzero coordinates of a word, i.e. the size of the support.</td>
</tr>
</tbody>
</table>
Codes, weights and weight enumerators

**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:

\[
W_C(X, Y) = \sum_{w=0}^{n} A_w X^{n-w} Y^w.
\]
Codes, weights and weight enumerators

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

$$W_C(X, Y) = X^7 + 7X^4Y^3 + 7X^3Y^4 + Y^7.$$
For a subcode $D \subseteq C$ we define

**Support**  Union of the support of all words in $D$, i.e. all coordinates which are not always zero.

**Weight**  Size of the support.
Generalized weight enumerator

For a subcode $D \subseteq C$ we define

**Support** Union of the support of all words in $D$, i.e. all coordinates which are not always zero.

**Weight** Size of the support.

**Generalized weight enumerators**

The homogeneous polynomials counting for each dimension $r = 0, \ldots, k$ the number of subcodes of a given weight, notation:

$$W_C^r(X, Y) = \sum_{w=0}^{n} A_w^r X^{n-w} Y^w$$
Generalized weight enumerator

Example

The [7, 4] Hamming code has generalized weight enumerators

\[ W_C^0(X, Y) = X^7 \]
\[ W_C^1(X, Y) = 7X^4Y^3 + 7X^3Y^4 + Y^7 \]
\[ W_C^2(X, Y) = 21X^2Y^5 + 7XY^6 + 7Y^7 \]
\[ W_C^3(X, Y) = 7XY^6 + 8Y^7 \]
\[ W_C^4(X, Y) = Y^7 \]
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 polynomial “counting the number of words in an extension code”, 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

For all subsets $J \subseteq [n]$ define

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

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

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

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

So $C(J)$ is equivalent to the code $C$ shortened on $J$. 
Extended weight enumerator

For all subsets $J \subseteq [n]$ define

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

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

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

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

So $C(J)$ is equivalent to the code $C$ shortened on $J$.

Extended weight enumerator

The extended weight enumerator can be written as

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

Example

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

$$W_C(X, Y, T) = X^7 + 7(T - 1)X^4Y^3 + 7(T - 1)X^3Y^4 + 21(T - 1)(T - 2)X^2Y^5 + 7(T - 1)(T - 2)(T - 3)XY^6 + (T - 1)(T^3 - 6T^2 + 15T - 13)Y^7$$
We considered three ways to determine the extended weight enumerator:

- **Brute force and Lagrange interpolation**
  Look at all words of $k + 1$ extension codes. Terribly slow.

- **Geometric approach**
  Using $l(J)$ and $B_t(T)$, also applicable for generalized WE. Much faster for $W_C(X, Y, T)$ instead of $W_C(X, Y)$.

- **Deletion/contraction algorithm**
  Recursive algorithm, also used for matroids. Good for classifying codes up to a certain length.
Connections (1)

We can write the extended weight enumerator in terms of the generalized weight enumerator:

\[ W_C(X, Y, T) = \sum_{r=0}^{k} \left( \prod_{j=0}^{r-1} (T - q^j) \right) W_C^r(X, Y). \]
We can write the extended weight enumerator in terms of the generalized weight enumerator:

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

Because we use \( W_C(X, Y, T) \) instead of \( W_C \otimes \mathbb{F}_{q^m}(X, Y) \) we also find the inverse:

\[ W_C^r(X, Y) = \frac{1}{\prod_{i=0}^{r-1} (q^r - q^i)} \sum_{j=0}^{r} \begin{bmatrix} r \\ j \end{bmatrix} (-1)^{r-j} q^{r \binom{r}{j}} W_C(X, Y, q^j). \]
Matroids

*Matroid theory* generalizes the notion of “linear independence”.

- Vector space: linear independent vectors, basis
- Graph: tree, minimal spanning tree
- Matroid: independent set, basis

A matroid consists of a finite set $E$ and a set of independent sets from $2^E$ having some defining properties.
Matroids

*Matroid theory* generalizes the notion of “linear independence”.

- Vector space: linear independent vectors, basis
- Graph: tree, minimal spanning tree
- Matroid: independent set, basis

A matroid consist of a finite set $E$ and a set of independent sets from $2^E$ having some defining properties.

**Example**

A code can be viewed as a matroid by considering the columns of a generator matrix and their dependance in $\mathbb{F}_q^k$. 
A matroid has a *rank function*, notation $r(A)$, associating a non-negative integer to every subset $A$ of $E$.

**Example**

For matroid from a generator matrix $G$ of a code, $r(A)$ is the rank of the submatrix formed by the columns of $G$ indexed by $A$. Furthermore, $r(E) = k$. 

**Tutte polynomial**

The Tutte polynomial is defined by

$$t_G(X,Y) = \sum_{A \subseteq E} (X-1)^{|A|} r(E) - r(A) (Y-1)^{|A|}.$$
A matroid has a rank function, notation $r(A)$, associating a non-negative integer to every subset $A$ of $E$.

**Example**

For matroid from a generator matrix $G$ of a code, $r(A)$ is the rank of the submatrix formed by the columns of $G$ indexed by $A$. Furthermore, $r(E) = k$.

**Tutte polynomial**

The Tutte polynomial is defined by

$$t_G(X, Y) = \sum_{A \subseteq E} (X - 1)^{r(E) - r(A)}(Y - 1)^{|A| - r(A)}.$$
The extended weight enumerator can be given in terms of the Tutte polynomial:

\[ W_C(X, Y, T) = (X - Y)^k Y^{n-k} t_G \left( \frac{X + (T - 1)Y}{X - Y}, \frac{X}{Y} \right). \]

Due to the earlier connection, we have similar formulas for \( W_C^r(X, Y) \) and \( t_G(X, Y) \).
Overview of connections

$W_C(X, Y)$

$W_C(X, Y, T)$

$\{W^r_C(X, Y)\}_{r=0}^{k} \rightleftharpoons t_G(X, Y)$

$\{W^r_C(X, Y, T)\}_{r=0}^{k}$
Duality for matroids

For a matroid $G$ and its dual $G^*$ we have

$$t_G(X, Y) = t_{G^*}(Y, X).$$
Application: MacWilliams relations

Duality for matroids

For a matroid $G$ and its dual $G^*$ we have

$$t_G(X, Y) = t_{G^*}(Y, X).$$

With this and the connections, the proofs of the MacWilliams relations for $W_C(X, Y, T)$ and $W_{C^r}(X, Y)$ reduce to rewriting.

MacWilliams relations

For a code $C$ and its dual $C^\perp$ we have

$$W_{C^\perp}(X, Y, T) = T^{-k}W_C(X + (T-1)Y, X - Y, T).$$
Cosets and weights

- **Coset**: Translation of the code by some vector \( y \in \mathbb{F}_q^n \).
- **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 $y \in \mathbb{F}_q^n$.
- **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.

- $\alpha_i$ The number of cosets of weight $i$.
- $\lambda_i$ The number of vectors of weight $i$ which are of minimal weight in their coset, i.e. the number of possible coset leaders of weight $i$. 
Coset leader and list weight enumerator

**Extended coset leader weight enumerator**

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

**Extended list weight enumerator**

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

The [7, 4] Hamming code has extended coset leader and extended list weight enumerator

\[ \alpha_C(X, Y, T) = X^7 + 7(T - 1)X^6Y + 7(T - 1)(T - 2)X^5Y^2 + (T - 1)(T - 2)(T - 4)X^4Y^3, \]

\[ \lambda_C(X, Y, T) = X^7 + 7(T - 1)X^6Y + 21(T - 1)(T - 2)X^5Y^2 + 28(T - 1)(T - 2)(T - 4)X^4Y^3. \]
Connections (3)

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?
Further work

- Determination of $\alpha_C(X, Y, T)$ and $\lambda_C(X, Y, T)$ via arrangements of hyperplanes and their characteristic polynomial
- Generalized coset leader weight enumerator?
- Connection with zeta-functions of codes and arrangements of hyperplanes
- Extend known theory to extended weight enumerator
- Concrete computations for special classes of codes
- Characterization of the various weight enumerators
- Complexity issues / implementation
- ...