Generalized weight enumerators

Relinde Jurrius

Technische Universiteit Eindhoven

November 26, 2008
Outline

What is coding theory?

Formal definitions of codes and weights
  Generalized weight enumerator
  Extended weight enumerator

Matroids and the Tutte polynomial

Connections

Further work
What is coding theory?

Shannon's communication diagram

message → channel → message

noise
What is coding theory?

Shannon's communication diagram
Formal definitions of codes and weights

**Linear \([n, k]\) code**  Linear subspace \(C \subseteq \mathbb{F}_q^n\) of dimension \(k\). Elements are called \((code)\)words, \(n\) is called the \textit{length}.  

**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:

\[
W_C(X, Y) = \sum_{w=0}^{n} A_w X^{n-w} Y^w.
\]
Formal definitions of codes and weights

**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 \(C\).
Formal definitions of codes and weights

**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.
Formal definitions of codes and weights

**Linear \([n, k]\) code**
Linear subspace \(C \subseteq \mathbb{F}_q^n\) of dimension \(k\). Elements are called \((code)words\), \(n\) is called the \emph{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:
\[
W_C(X, Y) = \sum_{w=0}^{n} A_w X^{n-w} Y^w.
\]
Formal definitions of codes and weights

Linear \([n, k]\) code

Linear subspace \(C \subseteq \mathbb{F}_q^n\) of dimension \(k\). Elements are called \((code)words\), \(n\) is called the \textit{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:

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

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

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

\[
\begin{align*}
W_C^0(X, Y) &= X^7 \\
W_C^1(X, Y) &= 7X^4Y^3 + 7X^3Y^4 + Y^7 \\
W_C^2(X, Y) &= 21X^2Y^5 + 7XY^6 + 7Y^7 \\
W_C^3(X, Y) &= 7XY^6 + 8Y^7 \\
W_C^4(X, Y) &= Y^7
\end{align*}
\]
**Extension code**  Code over some extension field $\mathbb{F}_{q^m}$ having the same generator matrix as $C$, notation: $C \otimes \mathbb{F}_{q^m}$. 
Extended weight enumerator

**Extension code** Code over some extension field \( \mathbb{F}_{q^m} \) having the same generator matrix as \( C \), 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 \( W_C(X, Y, q^m) = W_{C \otimes \mathbb{F}_{q^m}}(X, Y) \).
Example

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

\[
W_C(X, Y, T) = X^7 + \\
7(T - 1)X^4Y^3 + \\
7(T - 1)X^3Y^4 + \\
21(T - 1)(T - 2)X^2Y^5 + \\
7(T - 1)(T - 2)(T - 3)XY^6 + \\
(T - 1)(T^3 - 6T^2 + 15T - 13)Y^7
\]
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.
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

$$t_G(X, Y) = \sum_{A \subseteq E} (X-1)^{r(E)} - (Y-1)^{|A| - r(A)}.$$
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

\[
t_G(X, Y) = \sum_{A \subseteq E} (X - 1)^{r(E) - r(A)} (Y - 1)^{|A| - r(A)}.
\]
Connections – some formulas

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

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

and in terms of the Tutte polynomial:

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

\[ WC(X, Y) \]

\[ \{ WR_C(X, Y) \}_{r=0}^k \leftrightarrow t_G(X, Y) \]

\[ WC(X, Y, T) \]

\[ \{ WR_C(X, Y, T) \}_{r=0}^k \]
Further work

- Connections with other classifying polynomials:
  - Codes and zeta-function
  - Arrangement of hyperplanes and Poincaré polynomial
  - Arrangement of hyperplanes and zeta-function
  - Lattices and theta-function
- Concrete computations for special classes of codes
  - Cyclic codes
  - Algebraic geometry codes
- Characterization of extended weight enumerator
Further work

- Extend known theory to extended weight enumerator:
  - Gleason’s theory for self-dual codes
  - Codes over rings
- Probability of correct decoding
- Complexity issues