Subcode supports in matroid theory

Relinde Jurrius

Eindhoven University of Technology, The Netherlands

RISC Seminar, March 26, 2010

Outline

Codes and supports

Linear $[n, k]$ code Linear subspace $C \subseteq \mathbb{F}_q^n$ of dimension k.
Generator matrix G, parity check matrix H.

Support The coordinates of a word that are nonzero.

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

Codes and supports

Linear $[n, k]$ code Linear subspace $C \subseteq \mathbb{F}_q^n$ of dimension k. Generator matrix G, parity check matrix H.

Support The coordinates of a word that 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 and supports

Minimal codeword

Every codeword with the same support is a scalar multiple, i.e. the support is minimal with respect to inclusion.

Codes and supports

Minimal codeword

Every codeword with the same support is a scalar multiple, i.e. the support is minimal with respect to inclusion.

Example

The $[7, 4]$ Hamming code over $\mathbb{F}_2$ has weight enumerator

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

All words of weight 3 and 4 are minimal.

Matroids

Matroid

A matroid is a pair $(M, \mathcal{I})$ where M is a finite set and $\mathcal{I}$ is a collection of subsets of M called the *independent sets*, satisfying the following properties:

1. The empty set is independent.
2. Every subset of an independent set is independent.
3. Let A, B be independent sets with $|A| > |B|$. Then there exists an $a \in A$ with $a \notin B$ and $B \cup \{a\}$ an independent set.

Matroids

Matroid

A matroid is a pair $(M, \mathcal{I})$ where M is a finite set and $\mathcal{I}$ is a collection of subsets of M called the *independent sets*, satisfying the following properties:

1. The empty set is independent.
2. Every subset of an independent set is independent.
3. Let A, B be independent sets with $|A| > |B|$. Then there exists an $a \in A$ with $a \notin B$ and $B \cup \{a\}$ an independent set.

$M(C)$ is the matroid represented by a generator matrix of C.

- Independent of the choice of G.
- The elements of $M(C)$ are the columns of G.

Tutte polynomial

The Tutte polynomial is defined by

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

Matroids

Tutte polynomial

The Tutte polynomial is defined by

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

Example

The matroid associated to the binary $[7,4]$ Hamming code has Tutte polynomial

$$T_M(X,Y) = X^4 + 3X^3 + Y^3 + 6X^2 + 7XY + 4Y^2 + 3X + 3Y.$$

Weight enumerator and Tutte polynomial

Theorem

The Tutte polynomial of a matroid defines the weight enumerator of the associated code via

$$W_C(X,Y) = (X-Y)^k Y^{n-k}\, T_{M(C)}\left(\frac{X+(q-1)Y}{X-Y}, \frac{X}{Y}\right).$$

Weight enumerator and Tutte polynomial

Theorem

The Tutte polynomial of a matroid defines the weight enumerator of the associated code via

$$W_C(X,Y) = (X-Y)^k Y^{n-k}\, T_{M(C)}\left(\frac{X+(q-1)Y}{X-Y}, \frac{X}{Y}\right).$$

- Gives a nice proof of the MacWilliams relations, because $T_M(X,Y) = T_{M^*}(Y,X)$.
- Opposite is *not* true. Counterexample: codes with the same generator matrix over $\mathbb{F}_q$ and $\mathbb{F}_{q^2}$.

Minimal codewords and cocircuits

Theorem

The supports of the minimal codewords of C are exactly the cocircuits of $M(C)$.

Minimal codewords and cocircuits

Theorem

The supports of the minimal codewords of C are exactly the cocircuits of $M(C)$.

Two equivalent statements follow:

- *Coding-way:* Every word $\mathbf{c}$ is a linear combination of minimal codewords whose support is a subset of the support of $\mathbf{c}$.
- *Matroid-way:* Every dependent set is the union of cocircuits.

Higher dimensional coding theory

- Every codeword spans a 1-dimensional subcode.
- Idea: replace words by subcodes of a given dimension.
- Extend definitions to subcodes:

Support Union of the supports of all words in the subcode, i.e. all coordinates which are not always zero.

Weight The size of the support.

Higher dimensional coding theory

Generalized weight enumerators

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

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

Higher dimensional coding theory

Generalized weight enumerators

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

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

Minimal subcode

The support of the subcode is minimal among subcodes of the same dimension.

Higher dimensional coding theory

Example

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

$$\begin{aligned} W_C^0(X,Y) &= X^7 \\ W_C^1(X,Y) &= 7X^4Y^3 + 7X^3Y^4 + Y^7 \\ W_C^2(X,Y) &= 21X^2Y^5 + 7XY^6 + 7Y^7 \\ W_C^3(X,Y) &= 7XY^6 + 8Y^7 \\ W_C^4(X,Y) &= Y^7 \end{aligned}$$

All subcodes of minimal weight are minimal, plus the 1-dimensional subcodes of weight 4.

Generalized weight enumerator

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

$$\begin{aligned} C(J) &= \{\mathbf{c} \in C : c_j = 0 \text{ for all } j \in J\} \\ l(J) &= \dim C(J) \\ B_J^r &= |\{D \subseteq C(J) : D \text{ subspace}, \dim D = r\}| \\ B_t^r &= \sum_{|J|=t} B_J^r \end{aligned}$$

Note: $C(J)$ is equivalent to the code C shortened on J, and $B_J^r(J) = \begin{bmatrix} l(J) \\ r \end{bmatrix}_q$.

Generalized weight enumerator

Lemma

$$B_t^r = \sum_{w=0}^{n} \binom{n-w}{t} A_w^r.$$

Proof: count the following set in two ways.

$$\{(D, J) : J \subseteq [n],\ |J| = t, D \subseteq C(J) \text{ subspace}, \dim D = r\}$$

Generalized weight enumerator

Lemma

$$B_t^r = \sum_{w=0}^{n} \binom{n-w}{t} A_w^r.$$

Proof: count the following set in two ways.

$$\{(D, J) : J \subseteq [n],\ |J| = t, D \subseteq C(J) \text{ subspace}, \dim D = r\}$$

Theorem

The generalized weight enumerator is given by

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

Generalized weight enumerator and Tutte polynomial

Lemma

We have $l(J) = k - r(J)$ with r the rank function of the associated matroid.

Proof: Let C_J be the code C with all positions not in J replaced by zero's (i.e. C punctured on $[n] - J$). Then $C_J = C/C(J)$.

Generalized weight enumerator and Tutte polynomial

Lemma

We have $l(J) = k - r(J)$ with r the rank function of the associated matroid.

Proof: Let C_J be the code C with all positions not in J replaced by zero's (i.e. C punctured on $[n] - J$). Then $C_J = C/C(J)$.

Theorem

The Tutte polynomial of a matroid associated to a code is

$$T_{M(C)}(X,Y) = \sum_{t=0}^{n} \sum_{|J|=t} (X-1)^{l(J)} (Y-1)^{l(J)-(k-t)}.$$

Generalized weight enumerator and Tutte polynomial

The weight enumerator does not define the Tutte polynomial, but the generalized weight enumerators do:

Theorem

The Tutte polynomial associated to a code is completely determined by the generalized weight enumerators of the code and vice versa.

The proof is rewriting. Least ugly formula: $T_{M(C)}(X,Y)$ is equal to

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

Minimal subcodes in matroid theory

- The supports of minimal codewords are cocircuits of the associated matroid.
- Are the supports of minimal subcodes the cocircuits of some matroid?

Minimal subcodes in matroid theory

- The supports of minimal codewords are cocircuits of the associated matroid.
- Are the supports of minimal subcodes the cocircuits of some matroid?
- Yes, they are.

r-th truncated matroid

The matroid $T^r(M)$ defined by the rank function

$$r_{T^r(M)}(A) = \min\{r_M(A), r(M) - r\}.$$

We get this matroid by *truncating* r times.

Minimal subcodes in matroid theory

Theorem

The supports of de r-dimensional minimal subcodes of a code are exactly the cocircuits of the $(r-1)$-th truncation of the matroid associated to the code.

Minimal subcodes in matroid theory

Theorem

The supports of de r-dimensional minimal subcodes of a code are exactly the cocircuits of the $(r-1)$-th truncation of the matroid associated to the code.

Proof possible with this lemma:

Lemma

Every support of an r-dimensional subcode is a union of cocircuits of $T^{r-1}(M(C))$.

Minimal subcodes in matroid theory

Why the truncated matroid?

- To find supports of minimal codewords, we fix $l(J) = 1$ and minimalize the support of $C(J)$ w.r.t. inclusion.

Minimal subcodes in matroid theory

Why the truncated matroid?

- To find supports of minimal codewords, we fix $l(J) = 1$ and minimalize the support of $C(J)$ w.r.t. inclusion.
- In complement, we maximize J w.r.t. inclusion.

Minimal subcodes in matroid theory

Why the truncated matroid?

- To find supports of minimal codewords, we fix $l(J) = 1$ and minimalize the support of $C(J)$ w.r.t. inclusion.
- In complement, we maximize J w.r.t. inclusion.
- In matroid-terms: we maximize J for $r(J) = k - l(J) = k - 1$.

Minimal subcodes in matroid theory

Why the truncated matroid?

- To find supports of minimal codewords, we fix $l(J) = 1$ and minimalize the support of $C(J)$ w.r.t. inclusion.
- In complement, we maximize J w.r.t. inclusion.
- In matroid-terms: we maximize J for $r(J) = k - l(J) = k - 1$.
- J is a hyperplane.

Minimal subcodes in matroid theory

Why the truncated matroid?

- To find supports of minimal codewords, we fix $l(J) = 1$ and minimalize the support of $C(J)$ w.r.t. inclusion.
- In complement, we maximize J w.r.t. inclusion.
- In matroid-terms: we maximize J for $r(J) = k - l(J) = k - 1$.
- J is a hyperplane.
- The complement of J, i.e. the support of $C(J)$, is a cocircuit.

Minimal subcodes in matroid theory

Why the truncated matroid?

- To find supports of minimal codewords, we fix $l(J) = 1$ and minimalize the support of $C(J)$ w.r.t. inclusion.
- In complement, we maximize J w.r.t. inclusion.
- In matroid-terms: we maximize J for $r(J) = k - l(J) = k - 1$.
- J is a hyperplane.
- The complement of J, i.e. the support of $C(J)$, is a cocircuit.
- To generalize for fixed $l(J) = r$, the closed sets of rank $k - r$ should be hyperplanes.

Minimal subcodes in matroid theory

Why the truncated matroid?

- To find supports of minimal codewords, we fix $l(J) = 1$ and minimalize the support of $C(J)$ w.r.t. inclusion.
- In complement, we maximize J w.r.t. inclusion.
- In matroid-terms: we maximize J for $r(J) = k - l(J) = k - 1$.
- J is a hyperplane.
- The complement of J, i.e. the support of $C(J)$, is a cocircuit.
- To generalize for fixed $l(J) = r$, the closed sets of rank $k - r$ should be hyperplanes.
- This gives the $(r-1)$-th truncated matroid.

Summary

- Two properties of codes: weight enumerator, minimal codewords
- Links with matroid theory
- Generalization from words to subcodes
- Determination of generalized weight enumerators: $l(J)$ and B_t^r
- Generalized weight enumerator and Tutte polynomial: two-way equivalence
- Supports of minimal subcodes are cocircuits of the truncated matroid