UNIVERSITY OF TROMSØ UiT

Linear codes and Betti numbers of Stanley-Reisner rings associated to matroids.

Based on parts of joint work with Jan N. Roksvold and H. Verdure

Trygve Johnsen

Department of Mathematics and Statistics

December 3, 2013

Content

Matroids, equivalent definitions

— Matroids initially arose from matrices M over a field F. The matroid associated to M is a pair

$$(E = \{1, 2, \cdots, n\}, \mathcal{N}),$$

where $\mathcal{N}$ is the set of subsets of E indexing those sets of columns of M that are linearly independent.

Matroids, equivalent definitions

— Matroids initially arose from matrices M over a field F. The matroid associated to M is a pair

$$(E = \{1, 2, \cdots, n\}, \mathcal{N}),$$

where $\mathcal{N}$ is the set of subsets of E indexing those sets of columns of M that are linearly independent.

— Example

$$M = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix},$$

over any field. Then $E = \{1, 2, 3, 4, 5\}$, and the maximal elements in $\mathcal{N}$ are

$$\{1, 2, 3\}, \{1, 3, 5\}, \{2, 3, 4\}, \{3, 4, 5\}.$$

The set $\mathcal{B}$ with these 4 subsets as elements, certainly determines $\mathcal{N}$, which contain of 14 additional, smaller subsets of E.

Matroids, equivalent definitions

— Matroids initially arose from matrices M over a field F. The matroid associated to M is a pair

$$(E = \{1, 2, \cdots, n\}, \mathcal{N}),$$

where $\mathcal{N}$ is the set of subsets of E indexing those sets of columns of M that are linearly independent.

— Example

$$M = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix},$$

over any field. Then $E = \{1, 2, 3, 4, 5\}$, and the maximal elements in $\mathcal{N}$ are

$$\{1, 2, 3\}, \{1, 3, 5\}, \{2, 3, 4\}, \{3, 4, 5\}.$$

The set $\mathcal{B}$ with these 4 subsets as elements, certainly determines $\mathcal{N}$, which contain of 14 additional, smaller subsets of E.

The elements I of $\mathcal{N}$ satisfy:

— 1. $\emptyset \in \mathcal{N}$

— 2. If $I \in \mathcal{N}$, and $I' \subset I$, then $I' \in \mathcal{N}$.

— 3. If I_1 and I_2 are in $\mathcal{N}$, and $|I_1| < |I_2|$, then there is an element e of $I_2 - I_1$ such that $I_1 \cup \{e\} \in \mathcal{N}$.

The elements I of $\mathcal{N}$ satisfy:

— 1. $\emptyset \in \mathcal{N}$

— 2. If $I \in \mathcal{N}$, and $I' \subset I$, then $I' \in \mathcal{N}$.

— 3. If I_1 and I_2 are in $\mathcal{N}$, and $|I_1| < |I_2|$, then there is an element e of $I_2 - I_1$ such that $I_1 \cup \{e\} \in \mathcal{N}$.

DEFINITION OF A MATROID:
A (finite) matroid is a pair $(E = \{1, 2, \cdots, n\}, \mathcal{N})$, where $\mathcal{N} \subset 2^E$ satisfies $(1), (2), (3)$. The basis $\mathcal{B}$ of a matroid are the maximal elements of $\mathcal{N}$. They all have the same cardinality and this cardinality is the RANK of the matroid. The elements of $\mathcal{N}$ are the called the INDEPENDENT subsets of E.

The elements I of $\mathcal{N}$ satisfy:

— 1. $\emptyset \in \mathcal{N}$

— 2. If $I \in \mathcal{N}$, and $I' \subset I$, then $I' \in \mathcal{N}$.

— 3. If I_1 and I_2 are in $\mathcal{N}$, and $|I_1| < |I_2|$, then there is an element e of $I_2 - I_1$ such that $I_1 \cup \{e\} \in \mathcal{N}$.

DEFINITION OF A MATROID:
A (finite) matroid is a pair $(E = \{1, 2, \cdots, n\}, \mathcal{N})$, where $\mathcal{N} \subset 2^E$ satisfies $(1), (2), (3)$. The basis $\mathcal{B}$ of a matroid are the maximal elements of $\mathcal{N}$. They all have the same cardinality and this cardinality is the RANK of the matroid. The elements of $\mathcal{N}$ are the called the INDEPENDENT subsets of E.
CAUTION: There are matroids that do not come from matrices (over any field). Example for $n = 9$.

— THE DUAL MATROID $M^* = (E = \{1, 2, \cdots, n\}, \mathcal{N}^*)$ is the one whose basis $\mathcal{B}^*$ consists of the complements of the elements of $\mathcal{B}$. In the example above: $\mathcal{B}^* = \{\{4, 5\}, \{2, 4\}, \{1, 5\}, \{1, 2\}.\}$ This is well defined. The rank of M^* is $n - rk(M)$.

— THE DUAL MATROID $M^* = (E = \{1, 2, \cdots, n\}, \mathcal{N}^*)$ is the one whose basis $\mathcal{B}^*$ consists of the complements of the elements of $\mathcal{B}$. In the example above: $\mathcal{B}^* = \{\{4, 5\}, \{2, 4\}, \{1, 5\}, \{1, 2\}.\}$ This is well defined. The rank of M^* is $n - rk(M)$.

— MATROID OF A LINEAR CODE:
If C is a linear code over a finite field let $M(C)$ be the matroid assosiated to any parity check matrix of C (well defined). Then C is an $[n, n - rk(M)]$-code, and $M(C)^*$ is the matroid associated to any generator matrix of C, i.e. it is $M(C^*)$, where C^* is the orthogonal complement of C.
Also the minimum distance and all higher weights of C are only dependent on, and are easily expressible in terms of properties of the matroid $M(C)$ (and/or $M(C)^*$.)

DEFINITION OF RANK FUNCTION OF A MATROID:

If $X \subset E$, then $rk(X) =$ largest cardinality of an independent subset of X. Moreover $rk(M) = rk(E)$. The rank function $2^E \to N_0$ satisfies:

DEFINITION OF RANK FUNCTION OF A MATROID:

If $X \subset E$, then $rk(X) =$ largest cardinality of an independent subset of X. Moreover $rk(M) = rk(E)$. The rank function $2^E \to N_0$ satisfies:

— R1. If $X \subset E$, then $0 \leq r(X) \leq |X|$.

DEFINITION OF RANK FUNCTION OF A MATROID:

If $X \subset E$, then $rk(X) =$ largest cardinality of an independent subset of X. Moreover $rk(M) = rk(E)$. The rank function $2^E \to N_0$ satisfies:

— R1. If $X \subset E$, then $0 \leq r(X) \leq |X|$.

— R2. If $X \subset Y \subset E$, then $rk(X) \leq rk(Y)$.

DEFINITION OF RANK FUNCTION OF A MATROID:

If $X \subset E$, then $rk(X) =$ largest cardinality of an independent subset of X. Moreover $rk(M) = rk(E)$. The rank function $2^E \to N_0$ satisfies:

— R1. If $X \subset E$, then $0 \leq r(X) \leq |X|$.

— R2. If $X \subset Y \subset E$, then $rk(X) \leq rk(Y)$.

— R3. If X and Y are subsets of E, then $rk(X \cup Y) + rk(X \cap Y) \leq rk(X) + rk(Y)$.

DEFINITION OF RANK FUNCTION OF A MATROID:

If $X \subset E$, then $rk(X) =$ largest cardinality of an independent subset of X. Moreover $rk(M) = rk(E)$. The rank function $2^E \to N_0$ satisfies:

— R1. If $X \subset E$, then $0 \leq r(X) \leq |X|$.

— R2. If $X \subset Y \subset E$, then $rk(X) \leq rk(Y)$.

— R3. If X and Y are subsets of E, then $rk(X \cup Y) + rk(X \cap Y) \leq rk(X) + rk(Y)$.

COMMENT: Any function $2^E \to N_0$ satisfying $(R1), (R2), (R3)$ determines a matroid: $\mathcal{N} =$ the set of those I with $rk(I) = |I|$.

DUAL RANK FUNCTION

Given a matroid M with rank function rk. Put

$$rk^*(X) = |X| - rk(E) + rk(E - X).$$

DUAL RANK FUNCTION

Given a matroid M with rank function rk. Put

$$rk^*(X) = |X| - rk(E) + rk(E - X).$$

Then rk^* is the rank function of the dual matroid M^*.

Matroids defined through cirquits

Definition

E is a finite set and $\mathcal{C} \subset 2^E$ such that :

Matroids defined through cirquits

Definition

E is a finite set and $\mathcal{C} \subset 2^E$ such that :

1. $\emptyset \notin \mathcal{C}$

Matroids defined through cirquits

Definition

E is a finite set and $\mathcal{C} \subset 2^E$ such that :

1. $\emptyset \notin \mathcal{C}$
2. If $C_1, C_2 \in \mathcal{C}$ and $C_1 \subseteq C_2$, then $C_1 = C_2$

Matroids defined through cirquits

Definition

E is a finite set and $\mathcal{C} \subset 2^E$ such that :

1. $\emptyset \notin \mathcal{C}$
2. If $C_1, C_2 \in \mathcal{C}$ and $C_1 \subseteq C_2$, then $C_1 = C_2$
3. If $C_1, C_2 \in \mathcal{C}$, $\forall e \in C_1 \cap C_2$, there exists $C_3 \in \mathcal{C}$ such that $C_3 \subseteq C_1 \cup C_2 - \{e\}$.

Matroids defined through cirquits

Definition

E is a finite set and $\mathcal{C} \subset 2^E$ such that :

1. $\emptyset \notin \mathcal{C}$
2. If $C_1, C_2 \in \mathcal{C}$ and $C_1 \subseteq C_2$, then $C_1 = C_2$
3. If $C_1, C_2 \in \mathcal{C}$, $\forall e \in C_1 \cap C_2$, there exists $C_3 \in \mathcal{C}$ such that $C_3 \subseteq C_1 \cup C_2 - \{e\}$.

$$\text{Independent sets} : \mathcal{I} = \{\sigma \in 2^E |\ C \not\subseteq \sigma,\ \forall C \in \mathcal{C}\}$$

Matroids defined through cirquits

Definition

E is a finite set and $\mathcal{C} \subset 2^E$ such that :

1. $\emptyset \notin \mathcal{C}$
2. If $C_1, C_2 \in \mathcal{C}$ and $C_1 \subseteq C_2$, then $C_1 = C_2$
3. If $C_1, C_2 \in \mathcal{C}$, $\forall e \in C_1 \cap C_2$, there exists $C_3 \in \mathcal{C}$ such that $C_3 \subseteq C_1 \cup C_2 - \{e\}$.

$$\text{Independent sets} : \mathcal{I} = \{\sigma \in 2^E |\ C \not\subseteq \sigma,\ \forall C \in \mathcal{C}\}$$

$$\text{Rank function} : r(\sigma) = max\{\#I |\ I \in \mathcal{I}, I \subset \sigma\}.$$

$$\text{Nullity function} : n(\sigma) = \#\sigma - r(\sigma)$$

Generalized Hamming weights

C a $[n, k]$- linear code over a field $\mathbb{K}$.
The generalized Hamming weights are

$$d_i = Min\{\#Supp(D),\ D \subseteq C \text{ subcode of dimension } i\}.$$

Generalized Hamming weights

C a $[n, k]$- linear code over a field $\mathbb{K}$.
The generalized Hamming weights are

$$d_i = Min\{\#Supp(D),\ D \subseteq C \text{ subcode of dimension } i\}.$$

Definition

Let M be a matroid on the ground set E, The generalized Hamming weights of M are

$$d_i = Min\{\#\sigma |\ n(\sigma) = i\}.$$

Stanley-Reisner rings associated to matroids

Let M be a matroid on the ground set E.

Stanley-Reisner rings associated to matroids

Let M be a matroid on the ground set E.
Let $\mathbb{K}$ be any field, and $S = \mathbb{K}[\mathbf{X}] = \mathbb{K}[X_e, e \in E]$.

Stanley-Reisner rings associated to matroids

Let M be a matroid on the ground set E.
Let $\mathbb{K}$ be any field, and $S = \mathbb{K}[\mathbf{X}] = \mathbb{K}[X_e, e \in E]$.

Definition

The Stanley-Reisner ideal of M is

$$I_M = \left\langle \mathbf{X}^\sigma = \prod_{e \in \sigma} X_e \,|\, \sigma \in \mathcal{C} \right\rangle.$$

and the Stanley-Reisner ring

$$R_M = S/I_M.$$

Betti numbers

S/I_M has a minimal free resolution

Betti numbers

S/I_M has a minimal free resolution

$$0 \leftarrow S/I_M \leftarrow F_0 \leftarrow F_1 \leftarrow \cdots \leftarrow F_s \leftarrow 0$$

where

$$F_i = \bigoplus_{\alpha \in \mathbb{N}^E} S(-\alpha)^{\beta_{i,\alpha}}.$$

Betti numbers

S/I_M has a minimal free resolution

$$0 \leftarrow S/I_M \leftarrow F_0 \leftarrow F_1 \leftarrow \cdots \leftarrow F_s \leftarrow 0$$

where

$$F_i = \bigoplus_{\alpha \in \mathbb{N}^E} S(-\alpha)^{\beta_{i,\alpha}}.$$

3 types of Betti numbers:

$$\mathbb{N}^E\text{- or multigraded Betti numbers: } \beta_{i,\alpha}$$

$$\mathbb{N}\text{-graded Betti numbers: } \beta_{i,d} = \sum_{|\alpha|=d} \beta_{i,\alpha}$$

$$\text{global Betti numbers: } \beta_i = \sum_{d \geqslant 0} \beta_{i,d}$$

Betti numbers

S/I_M has a minimal free resolution

$$0 \leftarrow S/I_M \leftarrow F_0 \leftarrow F_1 \leftarrow \cdots \leftarrow F_s \leftarrow 0$$

where

$$F_i = \bigoplus_{\alpha \in \mathbb{N}^E} S(-\alpha)^{\beta_{i,\alpha}}.$$

3 types of Betti numbers:

$$\mathbb{N}^E\text{- or multigraded Betti numbers: } \beta_{i,\alpha}$$

$$\mathbb{N}\text{-graded Betti numbers: } \beta_{i,d} = \sum_{|\alpha|=d} \beta_{i,\alpha}$$

$$\text{global Betti numbers: } \beta_i = \sum_{d \geqslant 0} \beta_{i,d}$$

$$F_0 = S$$

$$\beta_{1,\sigma} = 1 \Leftrightarrow \sigma \in \mathcal{C}.$$

Betti table

The Betti table of a matroid is a matrix together with an integer n where the number in the i-th column and the j-th row represents $\beta_{i,i+j+c-2}$. The suffix c on the table denotes the minimal absolute values of a twist occuring.

Betti table

The Betti table of a matroid is a matrix together with an integer n where the number in the i-th column and the j-th row represents $\beta_{i,i+j+c-2}$. The suffix c on the table denotes the minimal absolute values of a twist occuring.

Example

Let M be the matroid with circuits $\{\{1,2,4\},\{1,2,3\},\{3,4\}\}$.

Betti table

The Betti table of a matroid is a matrix together with an integer n where the number in the i-th column and the j-th row represents $\beta_{i,i+j+c-2}$. The suffix c on the table denotes the minimal absolute values of a twist occuring.

Example

Let M be the matroid with circuits $\{\{1,2,4\},\{1,2,3\},\{3,4\}\}$.

$$0 \leftarrow R_M \leftarrow S \leftarrow S(-2) \oplus S(-3)^2 \leftarrow S(-4)^2 \leftarrow 0$$

Betti table

The Betti table of a matroid is a matrix together with an integer n where the number in the i-th column and the j-th row represents $\beta_{i,i+j+c-2}$. The suffix c on the table denotes the minimal absolute values of a twist occuring.

Example

Let M be the matroid with circuits $\{\{1,2,4\},\{1,2,3\},\{3,4\}\}$.

$$0 \leftarrow R_M \leftarrow S \leftarrow S(-2) \oplus S(-3)^2 \leftarrow S(-4)^2 \leftarrow 0$$

Betti table:

$$\begin{bmatrix} 1 & 0 \\ 2 & 2 \end{bmatrix}_2 .$$

Hochster's formula

Let M be a matroid on the ground set E. We give E any total order.

Hochster's formula

Let M be a matroid on the ground set E. We give E any total order.

The chain complex of M over $\mathbb{K}$ is

$$0 \leftarrow \mathbb{K} \xleftarrow{\partial_0} \bigoplus_{\substack{F \in M \\ \#F = 1}} \mathbb{K} \xleftarrow{\partial_1} \cdots \xleftarrow{\partial_{r-1}} \bigoplus_{\substack{F \in M \\ \#F = r}} \mathbb{K} \xleftarrow{\partial_r} \cdots \leftarrow 0.$$

Hochster's formula

Let M be a matroid on the ground set E. We give E any total order.

The chain complex of M over $\mathbb{K}$ is

$$0 \leftarrow \mathbb{K} \xleftarrow{\partial_0} \bigoplus_{\substack{F \in M \\ \#F = 1}} \mathbb{K} \xleftarrow{\partial_1} \cdots \xleftarrow{\partial_{r-1}} \bigoplus_{\substack{F \in M \\ \#F = r}} \mathbb{K} \xleftarrow{\partial_r} \cdots \leftarrow 0.$$

The boundary maps are: if $F = \{x_0 < \cdots < x_i\}$,

$$\partial_i(e_F) = \sum_{j=0}^{i} (-1)^j e_{\{x_0, \cdots, \check{x}_j, \cdots, x_i\}}.$$

Hochster's formula

Let M be a matroid on the ground set E. We give E any total order.
The chain complex of M over $\mathbb{K}$ is

$$0 \leftarrow \mathbb{K} \overset{\partial_0}{\leftarrow} \bigoplus_{\substack{F \in M \\ \#F = 1}} \mathbb{K} \overset{\partial_1}{\leftarrow} \cdots \overset{\partial_{r-1}}{\leftarrow} \bigoplus_{\substack{F \in M \\ \#F = r}} \mathbb{K} \overset{\partial_r}{\leftarrow} \cdots \leftarrow 0.$$

The boundary maps are: if $F = \{x_0 < \cdots < x_i\}$,

$$\partial_i(e_F) = \sum_{j=0}^{i} (-1)^j e_{\{x_0, \cdots, \check{x}_j, \cdots, x_i\}}.$$

Definition

The i-th reduced homology of M over $\mathbb{K}$ is the $\mathbb{K}$ vector space

$$\tilde{H}_i(M, \mathbb{K}) = \ker(\partial_i)/\mathrm{im}(\partial_{i+1})$$

and its dimension is denoted by $\tilde{h}_i(M, \mathbb{K})$.

Hochster's formula

Theorem

$$\beta_{i,\sigma}(\mathbb{K}) = \tilde{h}_{|\sigma|-i-1}(M|_\sigma, \mathbb{K})$$

Hochster's formula

Theorem

$$\beta_{i,\sigma}(\mathbb{K}) = \tilde{h}_{|\sigma|-i-1}(M|_\sigma, \mathbb{K})$$

Theorem

Let M be a matroid on E of rank r. Then

$$\tilde{h}_i(M, \mathbb{K}) = \begin{cases} (-1)^r \chi(M) & \text{if } i = r-1 \\ 0 & \text{otherwise} \end{cases}$$

Hochster's formula

Theorem

$$\beta_{i,\sigma}(\mathbb{K}) = \tilde{h}_{|\sigma|-i-1}(M|_\sigma, \mathbb{K})$$

Theorem

Let M be a matroid on E of rank r. Then

$$\tilde{h}_i(M, \mathbb{K}) = \begin{cases} (-1)^r \chi(M) & \text{if } i = r-1 \\ 0 & \text{otherwise} \end{cases}$$

Corollary

The Betti numbers of a matroid are independent of the field $\mathbb{K}$.

Goal

Look at relations between matroids, their Betti numbers and their generalized Hamming weights.

Goal

Look at relations between matroids, their Betti numbers and their generalized Hamming weights.

Remark 1:The $\mathbb{N}^E$-graded case:

Goal

Look at relations between matroids, their Betti numbers and their generalized Hamming weights.

Remark 1:The $\mathbb{N}^E$-graded case:

$$\beta_{1,\sigma} = \begin{cases} 1 & \text{if } \sigma \in \mathcal{C} \\ 0 & \text{otherwise} \end{cases}$$

Outline

1. Matroids - Hamming weights - Betti numbers

Outline

1. Matroids - Hamming weights - Betti numbers
2. Relation between the nullity function and non-redundancy of circuits

Outline

1. Matroids - Hamming weights - Betti numbers
2. Relation between the nullity function and non-redundancy of circuits
3. Betti numbers and generalized Hamming weights

Outline

1. Matroids - Hamming weights - Betti numbers
2. Relation between the nullity function and non-redundancy of circuits
3. Betti numbers and generalized Hamming weights
4. Dualities

Outline

1. Matroids - Hamming weights - Betti numbers
2. Relation between the nullity function and non-redundancy of circuits
3. Betti numbers and generalized Hamming weights
4. Dualities
5. Examples and preliminary summary

Outline

1. Matroids - Hamming weights - Betti numbers
2. Relation between the nullity function and non-redundancy of circuits
3. Betti numbers and generalized Hamming weights
4. Dualities
5. Examples and preliminary summary
6. Constant weight codes

Outline

1. Matroids - Hamming weights - Betti numbers
2. Relation between the nullity function and non-redundancy of circuits
3. Betti numbers and generalized Hamming weights
4. Dualities
5. Examples and preliminary summary
6. Constant weight codes
7. Weight enumerators of matroids

Outline

1. Matroids - Hamming weights - Betti numbers
2. Relation between the nullity function and non-redundancy of circuits
3. Betti numbers and generalized Hamming weights
4. Dualities
5. Examples and preliminary summary
6. Constant weight codes
7. Weight enumerators of matroids
8. Algebraic geometric codes

Content

Non-redundancy

An ingredient in understanding the role of cirquits for the nullity of subsets of E.

Definition

Let M be a matroid, and $\Sigma \subseteq \mathcal{C}$. We say that Σ is not redundant if

$$\forall \sigma \in \Sigma, \quad \bigcup_{\tau \in \Sigma - \{\sigma\}} \tau \subsetneq \bigcup_{\tau \in \Sigma} \tau.$$

Non-redundancy

An ingredient in understanding the role of cirquits for the nullity of subsets of E.

Definition

Let M be a matroid, and $\Sigma \subseteq \mathcal{C}$. We say that Σ is not redundant if

$$\forall \sigma \in \Sigma, \quad \bigcup_{\tau \in \Sigma - \{\sigma\}} \tau \subsetneq \bigcup_{\tau \in \Sigma} \tau.$$

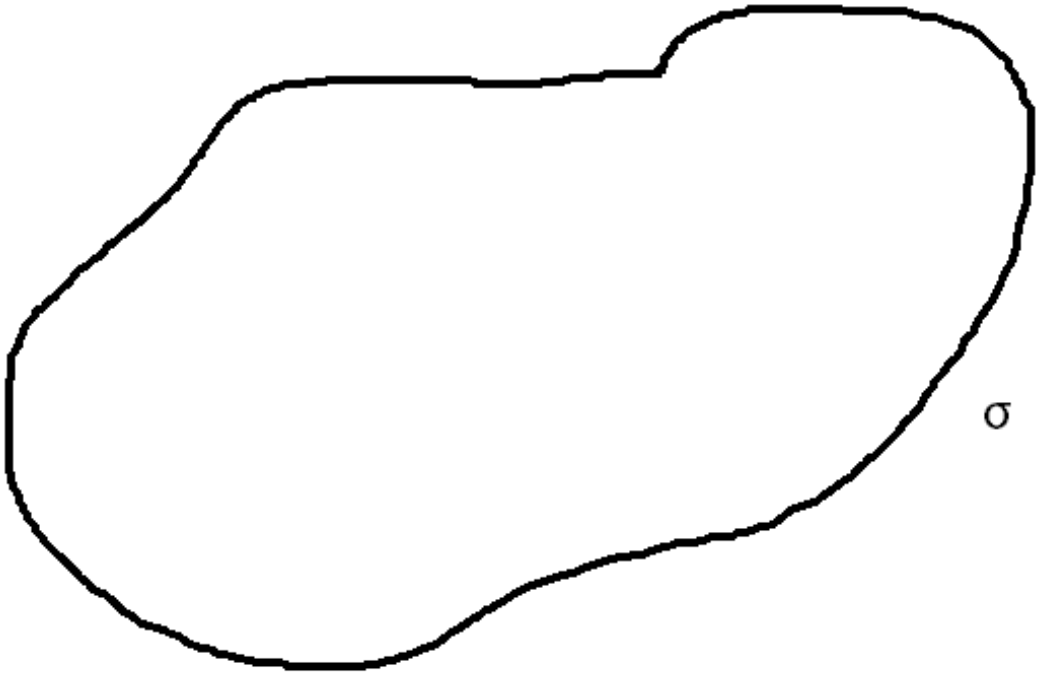
Definition

Let M be a matroid on the ground set E, and $\sigma \subseteq E$. The degree of non-redundancy of σ is

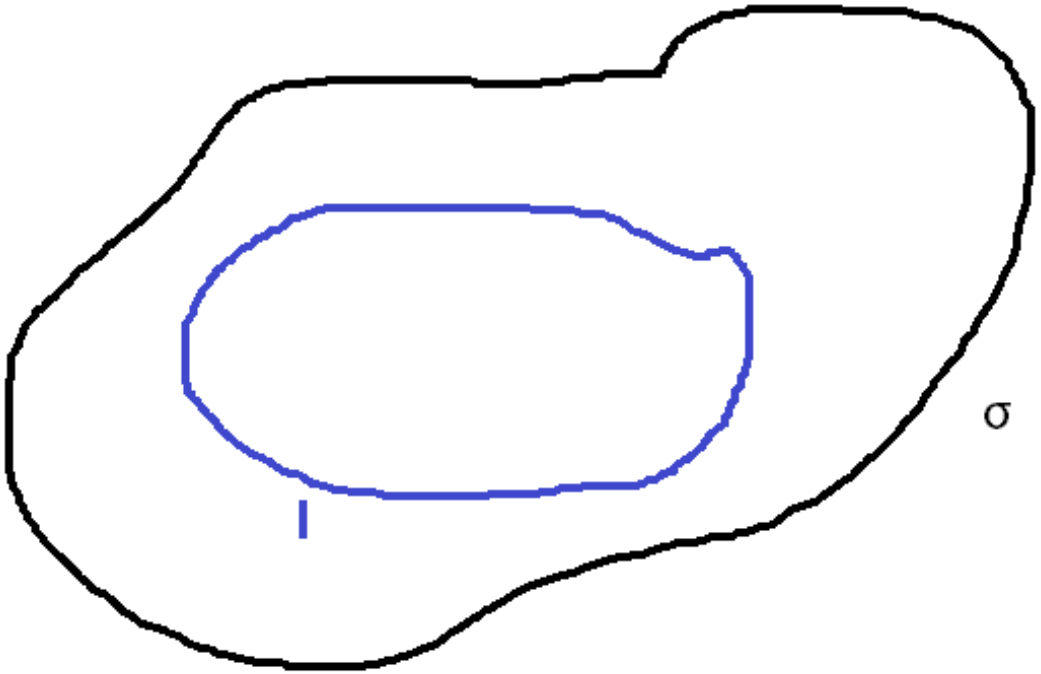
$$\deg(\sigma) = Max\{\#\Sigma |\ \Sigma \text{ non-redundant and } \bigcup_{\tau \in \Sigma} \tau \subseteq \sigma\}.$$

We have $n(\sigma) = deg(\sigma)$.

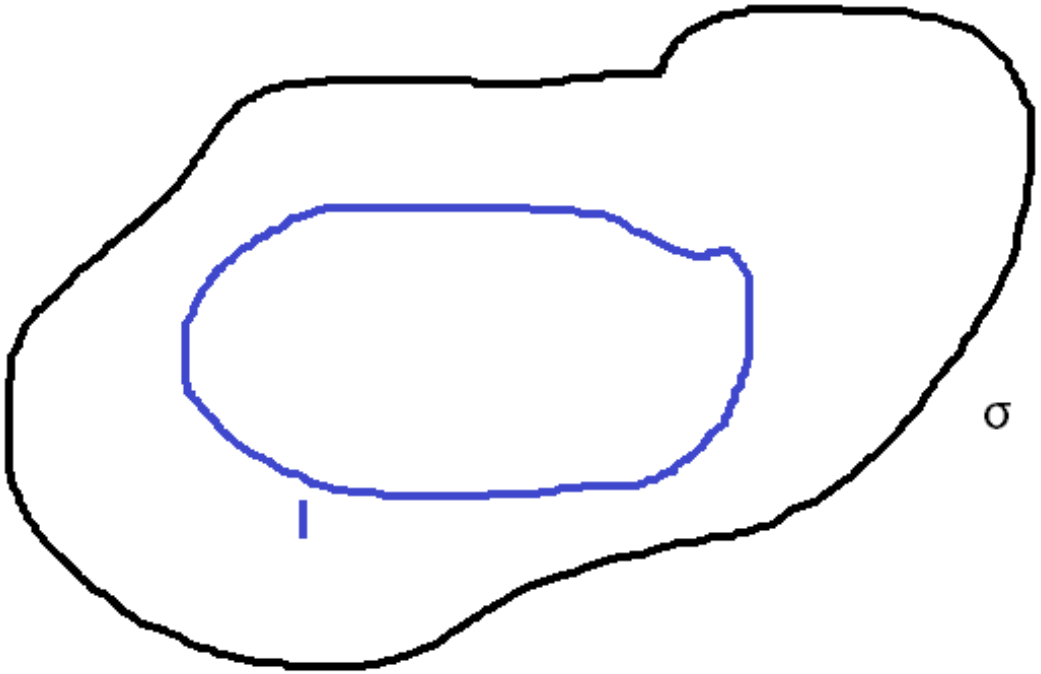
$$n(\sigma) \leqslant deg(\sigma)$$



$$n(\sigma) \leqslant deg(\sigma)$$

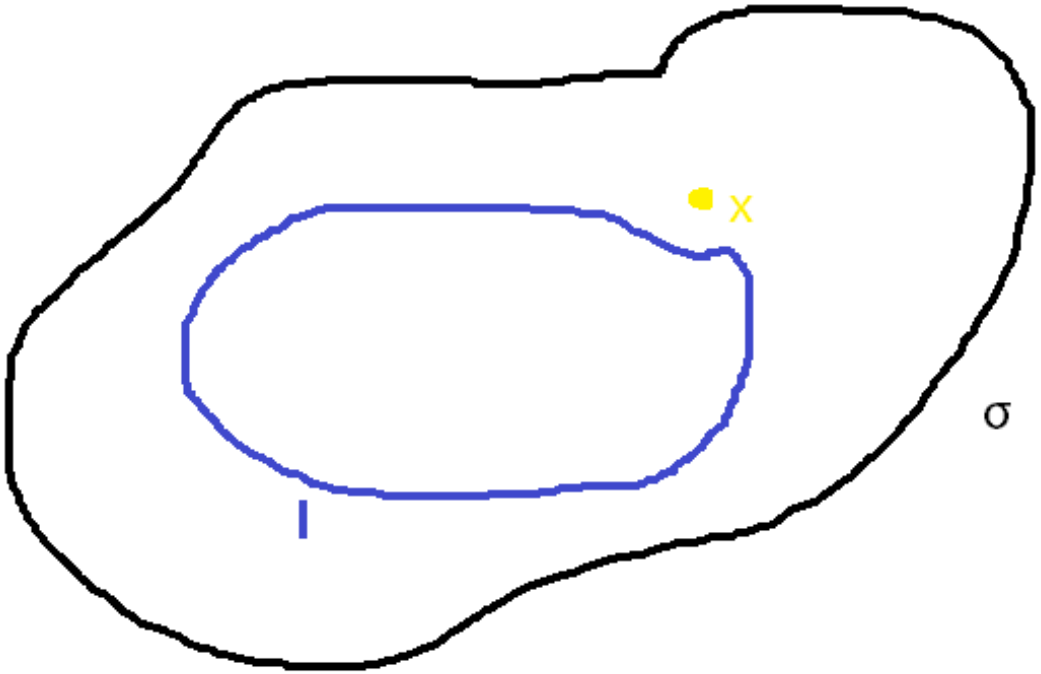


$n(\sigma) \leqslant deg(\sigma)$



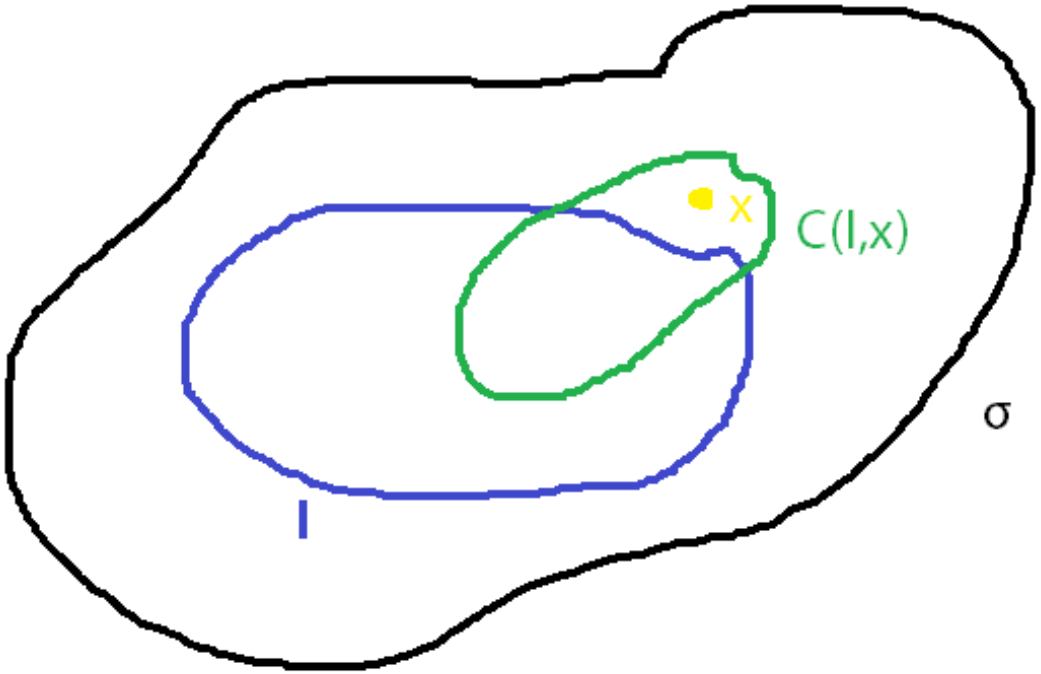
$r(\sigma) = \#I \Rightarrow n(\sigma)=\#(\sigma\text{-}I)$

$n(\sigma) \leqslant deg(\sigma)$



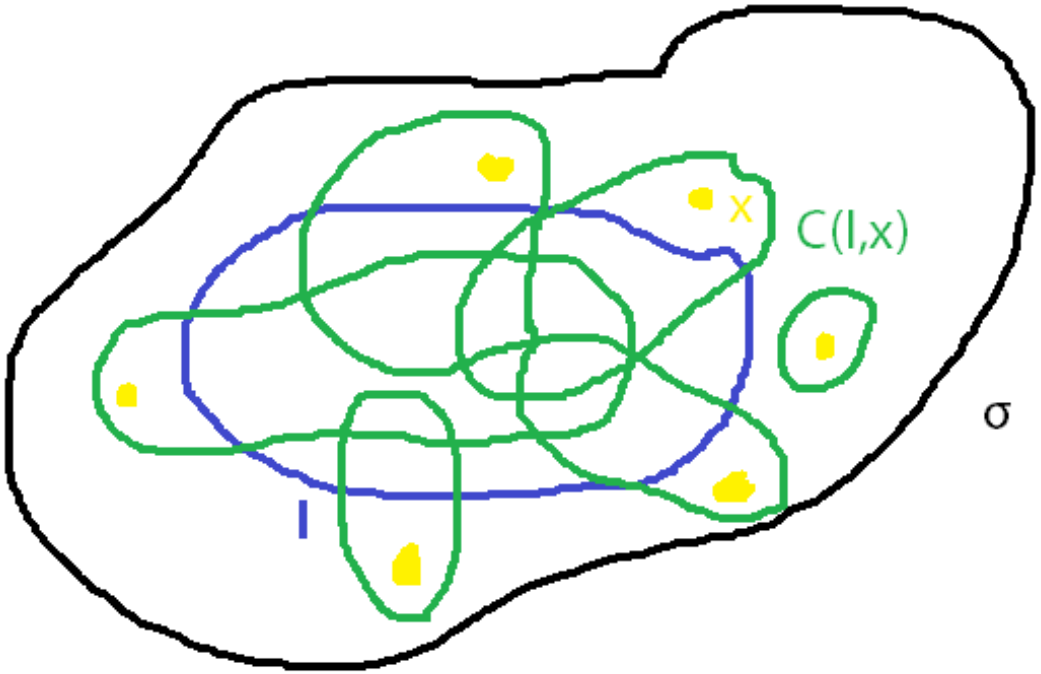
$r(\sigma) = \#I \Rightarrow n(\sigma)=\#(\sigma\text{-}I)$

$n(\sigma) \leqslant deg(\sigma)$



$r(\sigma) = \#I \Rightarrow n(\sigma)=\#(\sigma\text{-}I)$

$n(\sigma) \leqslant deg(\sigma)$



$r(\sigma) = \#I \Rightarrow n(\sigma)=\#(\sigma\text{-}I)$

$n(\sigma) \geqslant deg(\sigma)$

Important elements in proof:

Proposition

Let M be a matroid and $X, Y \subseteq E$. Then

$$n(X \cup Y) + n(X \cap Y) \geqslant n(X) + n(Y)$$

$n(\sigma) \geqslant deg(\sigma)$

Important elements in proof:

Proposition

Let M be a matroid and $X, Y \subseteq E$. Then

$$n(X \cup Y) + n(X \cap Y) \geqslant n(X) + n(Y)$$

Corollary

If $\Sigma \subset \mathcal{C}$ is non redundant, then

$$n\left(\bigcup_{\tau \in \Sigma} \tau\right) \geqslant \#\Sigma.$$

$n(\sigma) \geqslant deg(\sigma)$

Important elements in proof:

Proposition

Let M be a matroid and $X, Y \subseteq E$. Then

$$n(X \cup Y) + n(X \cap Y) \geqslant n(X) + n(Y)$$

Corollary

If $\Sigma \subset \mathcal{C}$ is non redundant, then

$$n\left(\bigcup_{\tau \in \Sigma} \tau\right) \geqslant \#\Sigma.$$

$$n\left(\bigcup_{\tau \in \Sigma} \tau\right) \geqslant n\left(\bigcup_{\tau \in \Sigma - \{\sigma\}} \tau\right) + n(\sigma) - n\left(\left(\bigcup_{\tau \in \Sigma - \{\sigma\}} \tau\right) \cap \sigma\right).$$

Content

When do we have $\beta_{i,\sigma} \neq 0$?

Hochster and Björner: $\beta_{i,\sigma} \neq 0 \Rightarrow i = n(\sigma)$.

When do we have $\beta_{i,\sigma} \neq 0$?

Hochster and Björner: $\beta_{i,\sigma} \neq 0 \Rightarrow i = n(\sigma)$.

Moreover, $\beta_{n(\sigma),\sigma} = (-1)^{r(\sigma)-1}\chi(M|_\sigma)$.

When do we have $\beta_{i,\sigma} \neq 0$?

Hochster and Björner: $\beta_{i,\sigma} \neq 0 \Rightarrow i = n(\sigma)$.

Moreover, $\beta_{n(\sigma),\sigma} = (-1)^{r(\sigma)-1}\chi(M|_\sigma)$.

Theorem

Let M be a matroid on the ground set E, and let $\sigma \subseteq E$. Then

$$\beta_{i,\sigma} \neq 0 \Leftrightarrow \sigma \text{ is minimal with } n(\sigma) = i.$$

The Betti numbers decide the weight hierarchy

[J-V]:

Theorem

Let M be a matroid on the ground set E of rank r. Then the generalized Hamming weights are given by

$$d_i = \min\{d \mid \beta_{i,d} \neq 0\} \text{ for } 1 \leqslant i \leqslant \#E - r.$$

The Betti numbers decide the weight hierarchy

[J-V]:

Theorem

Let M be a matroid on the ground set E of rank r. Then the generalized Hamming weights are given by

$$d_i = \min\{d \mid \beta_{i,d} \neq 0\} \text{ for } 1 \leqslant i \leqslant \#E - r.$$

Example

Let $\mathcal{C} = \{\{1,2,3,4\},\{1,4,5\},\{1,6\},\{2,3,4,6\},\{2,3,5\},\{4,5,6\}\}$.
The Betti table is

$$\begin{bmatrix} 1 & 0 & 0 \\ 3 & 2 & 0 \\ 2 & 7 & 4 \end{bmatrix}_2$$

The Betti numbers decide the weight hierarchy

[J-V]:

Theorem

Let M be a matroid on the ground set E of rank r. Then the generalized Hamming weights are given by

$$d_i = \min\{d \mid \beta_{i,d} \neq 0\} \text{ for } 1 \leqslant i \leqslant \#E - r.$$

Example

Let $\mathcal{C} = \{\{1,2,3,4\},\{1,4,5\},\{1,6\},\{2,3,4,6\},\{2,3,5\},\{4,5,6\}\}$.
The Betti table is

$$\begin{bmatrix} 1 & 0 & 0 \\ 3 & 2 & 0 \\ 2 & 7 & 4 \end{bmatrix}_2$$

The weight hierarchy is therefore $2, 4, 6$

MDS-codes

A linear $[n, k]$-code satisfies $d \leq r + 1 = n - k + 1$. If equality, the code is called MDS ($n - k$ is pr. def. the redundancy r of the code). Such codes correspond to uniform matroids $U(r, n)$.

MDS-codes

A linear $[n, k]$-code satisfies $d \leq r + 1 = n - k + 1$. If equality, the code is called MDS ($n - k$ is pr. def. the redundancy r of the code). Such codes correspond to uniform matroids $U(r, n)$. The resolution of the uniform matroid $U(r, n)$ is:

$$0 \longleftarrow R_{U(r,n)} \longleftarrow S \longleftarrow S(-(r+1))^{\binom{r}{r}\binom{n}{r+1}}$$

$$\longleftarrow S(-(r+2))^{\binom{r+1}{r}\binom{n}{r+2}} \longleftarrow S(-(r+3))^{\binom{r+2}{r}\binom{n}{r+3}}$$

$$\longleftarrow \ldots \longleftarrow S(-(n-1))^{\binom{n-2}{r}\binom{n}{n-1}} \longleftarrow S(-n)^{\binom{n-1}{r}\binom{n}{n}} \longleftarrow 0.$$

MDS-codes

A linear $[n,k]$-code satisfies $d \leq r+1 = n-k+1$. If equality, the code is called MDS ($n-k$ is pr. def. the redundancy r of the code). Such codes correspond to uniform matroids $U(r,n)$. The resolution of the uniform matroid $U(r,n)$ is:

$$0 \longleftarrow R_{U(r,n)} \longleftarrow S \longleftarrow S(-(r+1))^{\binom{r}{r}\binom{n}{r+1}}$$

$$\longleftarrow S(-(r+2))^{\binom{r+1}{r}\binom{n}{r+2}} \longleftarrow S(-(r+3))^{\binom{r+2}{r}\binom{n}{r+3}}$$

$$\longleftarrow \ldots \longleftarrow S(-(n-1))^{\binom{n-2}{r}\binom{n}{n-1}} \longleftarrow S(-n)^{\binom{n-1}{r}\binom{n}{n}} \longleftarrow 0.$$

and the Betti diagram is:

	1	$\cdots$	s	$\cdots$	$n-r$
r	$\binom{r}{r}\binom{n}{r+1}$	$\cdots$	$\binom{r+s-1}{r}\binom{n}{r+s}$	$\cdots$	$\binom{n-1}{r}\binom{n}{n}$

MDS-codes

A linear $[n,k]$-code satisfies $d \leq r+1 = n-k+1$. If equality, the code is called MDS ($n-k$ is pr. def. the redundancy r of the code). Such codes correspond to uniform matroids $U(r,n)$. The resolution of the uniform matroid $U(r,n)$ is:

$$0 \longleftarrow R_{U(r,n)} \longleftarrow S \longleftarrow S(-(r+1))^{\binom{r}{r}\binom{n}{r+1}}$$

$$\longleftarrow S(-(r+2))^{\binom{r+1}{r}\binom{n}{r+2}} \longleftarrow S(-(r+3))^{\binom{r+2}{r}\binom{n}{r+3}}$$

$$\longleftarrow \ldots \longleftarrow S(-(n-1))^{\binom{n-2}{r}\binom{n}{n-1}} \longleftarrow S(-n)^{\binom{n-1}{r}\binom{n}{n}} \longleftarrow 0.$$

and the Betti diagram is:

	1	$\cdots$	s	$\cdots$	$n-r$
r	$\binom{r}{r}\binom{n}{r+1}$	$\cdots$	$\binom{r+s-1}{r}\binom{n}{r+s}$	$\cdots$	$\binom{n-1}{r}\binom{n}{n}$

Hence the weight hierarchy is $\{n-k+1, \ldots, n-1, n\}$.

Some negative results

— $\beta_i \not\Rightarrow d_i$

Some negative results

- $\beta_i \not\Rightarrow d_i$
- $d_i \not\Rightarrow \beta_i,\ \beta_{i,d},\ \beta_{i,\sigma}$

Content

Dual of a matroid - Wei duality

Definition

Let M be a matroid. Its dual $\overline{M}$ has the same ground set, and its set of bases is the set of complements of bases of M.

Dual of a matroid - Wei duality

Definition

Let M be a matroid. Its dual $\overline{M}$ has the same ground set, and its set of bases is the set of complements of bases of M.

Theorem

Let M be a matroid on E of cardinality n with weight hierarchy $d_1 < \cdots < d_s$. Then the weight hierarchy of $\overline{M}$ is $d'_1 < \cdots < d'_{n-s}$

Dual of a matroid - Wei duality

Definition

Let M be a matroid. Its dual $\overline{M}$ has the same ground set, and its set of bases is the set of complements of bases of M.

Theorem

Let M be a matroid on E of cardinality n with weight hierarchy $d_1 < \cdots < d_s$. Then the weight hierarchy of $\overline{M}$ is $d'_1 < \cdots < d'_{n-s}$ and is such that

$$\{d_1, \cdots, d_s, n - d'_1 + 1, \cdots, n - d'_{n-s} + 1\} = E.$$

Dual of a matroid - Wei duality

Definition

Let M be a matroid. Its dual $\overline{M}$ has the same ground set, and its set of bases is the set of complements of bases of M.

Theorem

Let M be a matroid on E of cardinality n with weight hierarchy $d_1 < \cdots < d_s$. Then the weight hierarchy of $\overline{M}$ is $d'_1 < \cdots < d'_{n-s}$ and is such that

$$\{d_1, \cdots, d_s, n - d'_1 + 1, \cdots, n - d'_{n-s} + 1\} = E.$$

Corollary

The $\mathbb{N}$-graded Betti numbers of $\overline{M}$ give the weight hierarchy of M.

Alexander dual of a matroid

Definition

Let Δ be a simplicial complex, with set of faces $\mathcal{F}$. Then its Alexander dual $\Delta^\star$ has set of faces $\mathcal{F}^\star = \{\overline{\tau} | \, \tau \notin \mathcal{F}\}$.

Alexander dual of a matroid

Definition

Let Δ be a simplicial complex, with set of faces $\mathcal{F}$. Then its Alexander dual $\Delta^\star$ has set of faces $\mathcal{F}^\star = \{\overline{\tau} | \ \tau \notin \mathcal{F}\}$.

Eagon-Reiner: the Alexander dual of a matroid has a linear resolution.

Alexander dual of a matroid

Definition

Let Δ be a simplicial complex, with set of faces $\mathcal{F}$. Then its Alexander dual $\Delta^\star$ has set of faces $\mathcal{F}^\star = \{\overline{\tau} | \ \tau \notin \mathcal{F}\}$.

Eagon-Reiner: the Alexander dual of a matroid has a linear resolution.

Example

$\mathcal{C} = \{\{1,4\},\{2,3\}\}$

Alexander dual of a matroid

Definition

Let Δ be a simplicial complex, with set of faces $\mathcal{F}$. Then its Alexander dual $\Delta^\star$ has set of faces $\mathcal{F}^\star = \{\overline{\tau} | \ \tau \notin \mathcal{F}\}$.

Eagon-Reiner: the Alexander dual of a matroid has a linear resolution.

Example

$\mathcal{C} = \{\{1,4\},\{2,3\}\}$

Alexander dual of a matroid

Definition

Let Δ be a simplicial complex, with set of faces $\mathcal{F}$. Then its Alexander dual $\Delta^\star$ has set of faces $\mathcal{F}^\star = \{\overline{\tau} | \ \tau \notin \mathcal{F}\}$.

Eagon-Reiner: the Alexander dual of a matroid has a linear resolution.

Example

$\mathcal{C} = \{\{1,4\},\{2,3\}\}$
Betti table of the Alexander dual $M^\star$: $\begin{bmatrix} 4 & 4 & 1 \end{bmatrix}_2$.

Alexander dual of a matroid

Definition

Let Δ be a simplicial complex, with set of faces $\mathcal{F}$. Then its Alexander dual $\Delta^\star$ has set of faces $\mathcal{F}^\star = \{\overline{\tau} | \, \tau \notin \mathcal{F}\}$.

Eagon-Reiner: the Alexander dual of a matroid has a linear resolution.

Example

$\mathcal{C} = \{\{1,4\},\{2,3\}\}$
Betti table of the Alexander dual $M^\star$: $\begin{bmatrix} 4 & 4 & 1 \end{bmatrix}_2$.

The $\mathbb{N}$-graded Betti numbers of the Alexander dual don't in general give the weight hierarchy of M.

Content

h-MDS codes

Definition

A linear code C of length n and dimension k is h-MDS if $d_h = n - k + h$

h-MDS codes

Definition

A linear code C of length n and dimension k is h-MDS if $d_h = n - k + h$

Corollary

C is h-MDS if and only if the right part

$$F_h \leftarrow F_{h+1} \leftarrow \cdots \leftarrow F_k$$

of the resolution is linear, and $M(C)$ has no isthmus.

h-MDS codes

Definition

A linear code C of length n and dimension k is h-MDS if $d_h = n - k + h$

Corollary

C is h-MDS if and only if the right part

$$F_h \leftarrow F_{h+1} \leftarrow \cdots \leftarrow F_k$$

of the resolution is linear, and $M(C)$ has no isthmus.

Corollary

If C is non-degenerate, then it is MDS if and only if the Alexander dual of $M(C)$ is also a matroid.

An example from algebraic codes

Let X be an algebraic curve over $\mathbb{F}_q$ of genus g in $\mathbb{P}^{g-1}$ embedded by the canonical divisor K.

An example from algebraic codes

Let X be an algebraic curve over $\mathbb{F}_q$ of genus g in $\mathbb{P}^{g-1}$ embedded by the canonical divisor K.
Take (all) n distinct $\mathbb{F}_q$-rational points $P_1, \cdots, P_n$ and define a $[n \times g]$ matrix H where each column is a representative of P_i. Let $D = P_1 + \cdots P_n$.

An example from algebraic codes

Let X be an algebraic curve over $\mathbb{F}_q$ of genus g in $\mathbb{P}^{g-1}$ embedded by the canonical divisor K.
Take (all) n distinct $\mathbb{F}_q$-rational points $P_1, \cdots, P_n$ and define a $[n \times g]$ matrix H where each column is a representative of P_i. Let $D = P_1 + \cdots P_n$.
Let M be the matroid associated to this matrix on the ground set $\{1, \cdots, n\}$.

An example from algebraic codes

Let X be an algebraic curve over $\mathbb{F}_q$ of genus g in $\mathbb{P}^{g-1}$ embedded by the canonical divisor K.
Take (all) n distinct $\mathbb{F}_q$-rational points $P_1, \cdots, P_n$ and define a $[n \times g]$ matrix H where each column is a representative of P_i. Let $D = P_1 + \cdots P_n$.
Let M be the matroid associated to this matrix on the ground set $\{1, \cdots, n\}$.
$A \subseteq E$ corresponds to a subdivisor $A = P_{i_1} + \cdots + P_{i_s}$.

An example from algebraic codes

Let X be an algebraic curve over $\mathbb{F}_q$ of genus g in $\mathbb{P}^{g-1}$ embedded by the canonical divisor K.
Take (all) n distinct $\mathbb{F}_q$-rational points $P_1, \cdots, P_n$ and define a $[n \times g]$ matrix H where each column is a representative of P_i. Let $D = P_1 + \cdots P_n$.
Let M be the matroid associated to this matrix on the ground set $\{1, \cdots, n\}$.
$A \subseteq E$ corresponds to a subdivisor $A = P_{i_1} + \cdots + P_{i_s}$.
Riemann-Roch :

$$r(A) = l(K) - l(K - A) \Rightarrow n(A) = l(A) - 1.$$

Here r and n are matroid, and l is R.R. notation.

An example from algebraic codes

Let X be an algebraic curve over $\mathbb{F}_q$ of genus g in $\mathbb{P}^{g-1}$ embedded by the canonical divisor K.
Take (all) n distinct $\mathbb{F}_q$-rational points $P_1, \cdots, P_n$ and define a $[n \times g]$ matrix H where each column is a representative of P_i. Let $D = P_1 + \cdots P_n$.
Let M be the matroid associated to this matrix on the ground set $\{1, \cdots, n\}$.
$A \subseteq E$ corresponds to a subdivisor $A = P_{i_1} + \cdots + P_{i_s}$.
Riemann-Roch :

$$r(A) = l(K) - l(K - A) \Rightarrow n(A) = l(A) - 1.$$

Here r and n are matroid, and l is R.R. notation.
A "quasi-t-gonality" disregarding divisors with repeated points:

$$t_D := \min\{\deg A | l(A) = t + 1\} = d_t = \min\{j | \ \beta_{j,t} \neq 0\}.$$

An example from algebraic codes

Let X be the same algebraic curve of genus g.
Take n distinct points $P_1, \cdots, P_n$ and define a $[n \times g]$ matrix H where each column is a representative of P_i. Let $D = P_1 + \cdots P_n$.
Let M be the matroid associated to this matrix on the ground set $\{1, \cdots, n\}$.
$A \subseteq E$ corresponds to a subdivisor $A = P_{i_1} + \cdots + P_{i_s}$.

An example from algebraic codes

Let X be the same algebraic curve of genus g.
Take n distinct points $P_1, \cdots, P_n$ and define a $[n \times g]$ matrix H where each column is a representative of P_i. Let $D = P_1 + \cdots P_n$.
Let M be the matroid associated to this matrix on the ground set $\{1, \cdots, n\}$.
$A \subseteq E$ corresponds to a subdivisor $A = P_{i_1} + \cdots + P_{i_s}$.

$$Cl_D(A) := \deg(A) - 2(l(A) - 1)) = \#A - 2n(A).$$

An example from algebraic codes

Let X be the same algebraic curve of genus g.
Take n distinct points $P_1, \cdots, P_n$ and define a $[n \times g]$ matrix H where each column is a representative of P_i. Let $D = P_1 + \cdots P_n$.
Let M be the matroid associated to this matrix on the ground set $\{1, \cdots, n\}$.
$A \subseteq E$ corresponds to a subdivisor $A = P_{i_1} + \cdots + P_{i_s}$.

$$Cl_D(A) := \deg(A) - 2(l(A) - 1)) = \#A - 2n(A).$$

A "quasi-Clifford index" is:

$$\begin{aligned} Cl_D(X) &:= \min\{CL_D(A) |\ h^0(A) \geqslant 2, h^1(A) \geqslant 2\} \\ &= \min\{j - 2i |\ i \geqslant 1, j \leqslant g - 2 + i, \beta_{i,j} \neq 0\} \end{aligned}$$

Summary

	M	$\overline{M}$	$M^\star$	$\overline{M}^\star$
$\beta_{i,\sigma}$				
$\beta_{i,d}$				
β_i				

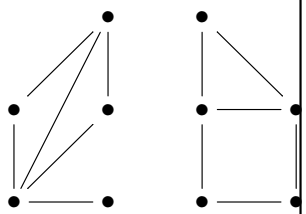
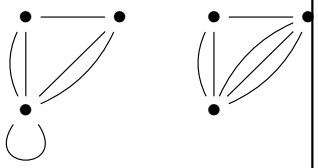
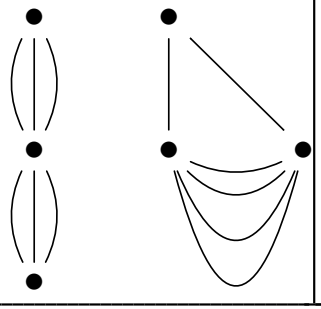
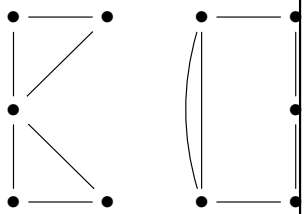
Summary

	M	$\overline{M}$	$M^\star$	$\overline{M}^\star$
$\beta_{i,\sigma}$	M	M	M	M
$\beta_{i,d}$				
β_i				

Summary

	M	$\overline{M}$	$M^\star$	$\overline{M}^\star$
$\beta_{i,\sigma}$	M	M	M	M
$\beta_{i,d}$	d_i	d_i		
β_i				

Summary

	M	$\overline{M}$	$M^\star$	$\overline{M}^\star$
$\beta_{i,\sigma}$	M	M	M	M
$\beta_{i,d}$	d_i	d_i		
β_i				

Content

A (linear $\mathbb{F}_q$-ary $[n, k]$) code is called a constant weight code if the support of all codeword have the same cardinality d.

A (linear $\mathbb{F}_q$-ary $[n, k]$) code is called a constant weight code if the support of all codeword have the same cardinality d.

Result: If a linear code C has constant weight, then the cardinalities of the supports of all sub-linear spaces of C of dimension i are the same number, which we of course call d_i, for $i = 1, \cdots, k$. So it is "constant weight in all dimensions".

A (linear $\mathbb{F}_q$-ary $[n, k]$) code is called a constant weight code if the support of all codeword have the same cardinality d.

Result: If a linear code C has constant weight, then the cardinalities of the supports of all sub-linear spaces of C of dimension i are the same number, which we of course call d_i, for $i = 1, \cdots, k$. So it is "constant weight in all dimensions".

Result: If a linear code C has constant weight, then

$$d_i = d\frac{q^k - q^{k-i}}{q^k - q^{k-1}},$$

for all i.

This implies that : $d_k = \frac{q^k - 1}{q^{k-i}(q^i - 1)} d_i$, for all $1 \leq i < k$.

A (linear $\mathbb{F}_q$-ary $[n, k]$) code is called a constant weight code if the support of all codeword have the same cardinality d.

Result: If a linear code C has constant weight, then the cardinalities of the supports of all sub-linear spaces of C of dimension i are the same number, which we of course call d_i, for $i = 1, \cdots, k$. So it is "constant weight in all dimensions".

Result: If a linear code C has constant weight, then

$$d_i = d\frac{q^k - q^{k-i}}{q^k - q^{k-1}},$$

for all i.

This implies that : $d_k = \frac{q^k-1}{q^{k-i}(q^i-1)} d_i$, for all $1 \leq i < k$.

Moreover: If $d_k = \frac{q^k-1}{q^{k-i}(q^i-1)} d_i$, for some $1 \leq i < k$, then C has constant weight.

A (linear $\mathbb{F}_q$-ary $[n, k]$) code is called a constant weight code if the support of all codeword have the same cardinality d.

Result: If a linear code C has constant weight, then the cardinalities of the supports of all sub-linear spaces of C of dimension i are the same number, which we of course call d_i, for $i = 1, \cdots, k$. So it is "constant weight in all dimensions".

Result: If a linear code C has constant weight, then

$$d_i = d\frac{q^k - q^{k-i}}{q^k - q^{k-1}},$$

for all i.

This implies that : $d_k = \frac{q^k-1}{q^{k-i}(q^i-1)} d_i$, for all $1 \leq i < k$.

Moreover: If $d_k = \frac{q^k-1}{q^{k-i}(q^i-1)} d_i$, for some $1 \leq i < k$, then C has constant weight.

Constant weight linear codes are repetitions of simplex codes.

We show:
Constant weight codes have pure resolutions (of the Stanley-Reisner ring of the parity check matroid simplicial complex).

We show:
Constant weight codes have pure resolutions (of the Stanley-Reisner ring of the parity check matroid simplicial complex).
Main point: Let M be a matroid on the ground set E, and let $\sigma \subseteq E$. Then

$$\beta_{i,\sigma} \neq 0 \Leftrightarrow \sigma \text{ is minimal with } n(\sigma) = i.$$

We show:
Constant weight codes have pure resolutions (of the Stanley-Reisner ring of the parity check matroid simplicial complex).
Main point: Let M be a matroid on the ground set E, and let $\sigma \subseteq E$. Then

$$\beta_{i,\sigma} \neq 0 \Leftrightarrow \sigma \text{ is minimal with } n(\sigma) = i.$$

Since all subcodes of dimension i have the same support weight, all minimal elements of N_i (the supports of these subcodes) will have the same cardinalities.

We show:
Constant weight codes have pure resolutions (of the Stanley-Reisner ring of the parity check matroid simplicial complex).
Main point: Let M be a matroid on the ground set E, and let $\sigma \subseteq E$. Then

$$\beta_{i,\sigma} \neq 0 \Leftrightarrow \sigma \text{ is minimal with } n(\sigma) = i.$$

Since all subcodes of dimension i have the same support weight, all minimal elements of N_i (the supports of these subcodes) will have the same cardinalities.
[J-V]: The Betti-numbers satisfy: $\beta_{i,d_i} = g(i,k)q^{\frac{i(i-1}{2}}$.

We show:
Constant weight codes have pure resolutions (of the Stanley-Reisner ring of the parity check matroid simplicial complex).
Main point: Let M be a matroid on the ground set E, and let $\sigma \subseteq E$. Then

$$\beta_{i,\sigma} \neq 0 \Leftrightarrow \sigma \text{ is minimal with } n(\sigma) = i.$$

Since all subcodes of dimension i have the same support weight, all minimal elements of N_i (the supports of these subcodes) will have the same cardinalities.
[J-V]: The Betti-numbers satisfy: $\beta_{i,d_i} = g(i,k)q^{\frac{i(i-1}{2}}$.
Proof: Special argument using properties of constant weight codes in a profound way, or:
The Herzog-Kuhl equations for Betti numbers associated to pure Cohen-Macaulay resolutions.

Last approach: $\beta_{1,\sigma} = 1$, for cirquits σ.

Last approach: $\beta_{1,\sigma} = 1$, for cirquits σ.
More details: Count cirquits (supports of codewords) to obtain β_{1,d_1}. Set $d_0 = 0$.

Last approach: $\beta_{1,\sigma} = 1$, for cirquits σ.
More details: Count cirquits (supports of codewords) to obtain β_{1,d_1}. Set $d_0 = 0$. Then we use a formula

$$\beta_{i,d_i} = \prod_{j \neq 0,i} |\frac{d_j - d_0}{d_j - d_i}|,$$

for $i \geq 1$ obtained from The Herzog-Kuhl equations, which are the ones imposed on the $\beta_{i,j}(S/I)$ by the vanishing of the first c coefficients of the Hilbert polynomial of M, corresponding to the fact that the support of S/I has codimension c.

Content

We want to study the polynomial

$$P_{M,j}(Z) = (-1)^j \sum_{|\sigma|=j} \sum_{\gamma \subseteq \sigma} (-1)^{|\gamma|} Z^{n_M(\gamma)} \text{ for } 1 \leq j \leq n,$$

which we refer to as the generalized weight enumerator of M.

We want to study the polynomial

$$P_{M,j}(Z) = (-1)^j \sum_{|\sigma|=j} \sum_{\gamma \subseteq \sigma} (-1)^{|\gamma|} Z^{n_M(\gamma)} \text{ for } 1 \leq j \leq n,$$

which we refer to as the generalized weight enumerator of M. Why ?

We want to study the polynomial

$$P_{M,j}(Z) = (-1)^j \sum_{|\sigma|=j} \sum_{\gamma \subseteq \sigma} (-1)^{|\gamma|} Z^{n_M(\gamma)} \text{ for } 1 \leq j \leq n,$$

which we refer to as the generalized weight enumerator of M. Why ?
After an argument similar to one of Jurrius/Pellikaan one shows that:

$$P_{M(H),i}(q^m)$$

is the number of codewords of weight i in $C \otimes_{\mathbb{F}_q} \mathbb{F}_{q^m}$ for a linear code C with parity check matrix H.

Result: $P_{M,i}(Z)$ is determined by Betti numbers of M, and so-called elongations of M.

Result: $P_{M,i}(Z)$ is determined by Betti numbers of M, and so-called elongations of M.
As a simple illustration we show that the constant term of $P_{M,n}(Z)$ is equal to

$$(-1)^{n-r}\beta_{n-r(M),n}.$$

Recall that

$$P_{M,n}(Z) = \sum_{\gamma \subseteq E} (-1)^{|\gamma|} Z^{n_M(\gamma)},$$

and note that the constant term of this polynomial is

$$\sum_{n_M(\gamma)=0} (-1)^{|\gamma|} = (-1)^{n+1} \chi(M),$$

where $\chi(M)$ is the reduced Euler characteristic of M. Let f_i be the number of independent sets in M of cardinality i.

$$\chi(M) = -1 + f_1 - f_2 + \cdots + (-1)^{r(M)-1} f_{r(M)}.$$

Let $H_i(M;\mathbb{K})$ denote the ith reduced homology of M over $\mathbb{K}$. According to Björner (1992), we have

$$(-1)^{n+1}\chi(M) = (-1)^{n-r(M)} \dim H_{r(M)-1}(M).$$

From *Hochster's formula*, we see that the dimension of $H_{r(M)-1}(M)$ is equal to $\beta_{n-r(M),n}((S/I)_M)$, thus

$$\begin{aligned}\sum_{n_M(\gamma)=0} (-1)^{|\gamma|} &= (-1)^{n+1}\chi(M)\\ &= (-1)^{n-r(M)} \dim H_{r(M)-1}(M)\\ &= (-1)^{n-r(M)}\beta_{n-r(M),n}((S/I)_M),\end{aligned}$$

which was what we wanted to prove.
Hochster's formula

$$\beta_{i,\sigma}((S/I)_M) = \dim H_{|\sigma|-i-1}(M_{|\sigma}).$$

To find the remaining coefficients of $P_{M,n}$, we shall need the Betti numbers of so called *elongations* of M:

To find the remaining coefficients of $P_{M,n}$, we shall need the Betti numbers of so called *elongations* of M:
The elongation M_i of M to rank $r(M) + i$. For $1 \leq i \leq n - r(M)$, the set $\mathcal{I}_i = \{\sigma \in E : n(\sigma) \leq i\}$ forms the set of independent sets of a matroid M_i on E. Note that $M = M_0$

Let n_{M_i} denote the nullity function of M_i. Then, for $\sigma \subseteq E$, we have

$$n_{M_i}(\sigma) = \max\{n(\sigma) - i, 0\}$$

We shall make use of the following observation:

$$n^{-1}(l) = n_{M_l}^{-1}(0) \setminus n_{M_{l-1}}^{-1}(0).$$

Let $\beta^{(i)}$ distinguish the Betti numbers of M_i from those of $M(= M_0)$. (And let $\beta^{(i)} = 0$ whenever $i \notin [i, n - r(M)]$.)

Proposition

The coefficient of Z^l in $P_{M,n}(Z)$ is equal to

$$(-1)^{n-r-l}\left[\beta^{(l-1)}_{n-r-l+1,n} + \beta^{(l-1)}_{n-r-l,n}\right].$$

Since

$$P_{M,n}(Z) = (-1)^n \sum_{\gamma \subseteq E} (-1)^{|\gamma|} Z^{n_M(\gamma)},$$

it is clear that the coefficient of Z^l is equal to

$$(-1)^n \sum_{n_M(\gamma)=l} (-1)^{|\gamma|}.$$

But

$$\sum_{n_M(\gamma)=l} (-1)^{|\gamma|} = \Big[\sum_{n_{M_l}(\gamma)=0} (-1)^{|\gamma|} - \sum_{n_{M_{l-1}}(\gamma)=0} (-1)^{|\gamma|} \Big],$$

and the result follows as for the constant term.

To find $P_{M,j}$ for $0 \leq j \leq n-1$ we proceed in an analogous fashion; first we find the constant term for each j, then we use the elongations to find the remaining coefficients. The final results being:
[J-R-V]:

Theorem

For $1 \leq j \leq n$ the coefficient of Z^l in $P_{M,j}$ is equal to

$$\sum_{i=0}^{n}(-1)^{i+1}\left(\beta_{i+1,j}^{(l-1)} - \beta_{i+1,j}^{(l)}\right).$$

Corollary

Let C be an $[n,k]$-code over $\mathbb{F}_q$. For $1 \leq j \leq n$, the number of words of weight j in $C \otimes_{\mathbb{F}_q} \mathbb{F}_{q^m}$ is

$$\sum_{l=0}^{k}\left(\sum_{i=0}^{n}(-1)^{i+1}\left(\beta_{i+1,j}^{(l-1)} - \beta_{i+1,j}^{(l)}\right)\right)(q^m)^l.$$

Content

Construction of codes from algebraic geometry

— X be any subset of the projective space $\mathbb{P}^{k-1}$ over $\mathbb{F}_q$, for example the set of $\mathbb{F}_q$-rational points of a projective variety defined over $\mathbb{F}_q$.

Construction of codes from algebraic geometry

— X be any subset of the projective space $\mathbb{P}^{k-1}$ over $\mathbb{F}_q$, for example the set of $\mathbb{F}_q$-rational points of a projective variety defined over $\mathbb{F}_q$.

— Let $P_1, \ldots, P_n$ be the $\mathbb{F}_q$-rational points on X, and for each P_i, choose coordinates $P_{i,1}, \ldots, P_{i,k}$.

Construction of codes from algebraic geometry

- X be any subset of the projective space $\mathbb{P}^{k-1}$ over $\mathbb{F}_q$, for example the set of $\mathbb{F}_q$-rational points of a projective variety defined over $\mathbb{F}_q$.
- Let $P_1, \ldots, P_n$ be the $\mathbb{F}_q$-rational points on X, and for each P_i, choose coordinates $P_{i,1}, \ldots, P_{i,k}$.
- We define the corresponding code to be the row-space of the matrix

$$G = \begin{pmatrix} P_{1,1} & P_{2,1} & \ldots & P_{n,1} \\ P_{1,2} & P_{2,2} & \ldots & P_{n,2} \\ \vdots & \vdots & \ddots & \vdots \\ P_{1,k} & P_{2,k} & \ldots & P_{n,k} \end{pmatrix}.$$

The code is only defined up to equivalence, but the code parameters are the same up to such equivalence.

Construction of codes from algebraic geometry

- X be any subset of the projective space $\mathbb{P}^{k-1}$ over $\mathbb{F}_q$, for example the set of $\mathbb{F}_q$-rational points of a projective variety defined over $\mathbb{F}_q$.
- Let $P_1, \ldots, P_n$ be the $\mathbb{F}_q$-rational points on X, and for each P_i, choose coordinates $P_{i,1}, \ldots, P_{i,k}$.
- We define the corresponding code to be the row-space of the matrix

$$G = \begin{pmatrix} P_{1,1} & P_{2,1} & \ldots & P_{n,1} \\ P_{1,2} & P_{2,2} & \ldots & P_{n,2} \\ \vdots & \vdots & \ddots & \vdots \\ P_{1,k} & P_{2,k} & \ldots & P_{n,k} \end{pmatrix}.$$

  The code is only defined up to equivalence, but the code parameters are the same up to such equivalence.
- How are the d_i determined by the geometry of X?

Find the d_i from properties of X

For each $h = 1, \ldots, k$, let
$J_h = \max\{\#\mathbb{F}_q$-rational points on X in $S \mid S$ is a codim. h subspace in $\mathbb{P}_q^{k-1}\}$. We recall: $n = \#\mathbb{F}_q$-rational points on X.

$$d_h = n - J_h. \tag{1}$$

Find the d_i from properties of X

For each $h = 1, \ldots, k$, let
$J_h = \max\{\#\mathbb{F}_q$-rational points on X in $S \mid S$ is a codim. h subspace in $\mathbb{P}_q^{k-1}\}$. We recall: $n = \#\mathbb{F}_q$-rational points on X.

$$d_h = n - J_h. \tag{1}$$

Dually: If instead we use G as a parity check matrix H for C, then:
d_i is the smallest t such that there exist t points of X only spanning a $(t - i - 1)$-dimensional subspace of $\mathbb{P}_q^{k-1}$.
Reflects the existence of t-secant $(t - i - 1)$-planes.

Simplex codes

Let X be the set of <u>all</u> points in a projective space $\mathbb{P}^s$. This gives the socalled simplex code $\mathbb{S}_q(s)$. Then all codimension r spaces contain the same number of points, and this code is therefore of constant weight.

$$d_r = \frac{q^s - 1}{q - 1} - \frac{q^{s-r} - 1}{q - 1}.$$

Simplex codes

Let X be the set of <u>all</u> points in a projective space $\mathbb{P}^s$. This gives the socalled simplex code $\mathbb{S}_q(s)$. Then all codimension r spaces contain the same number of points, and this code is therefore of constant weight.

$$d_r = \frac{q^s - 1}{q - 1} - \frac{q^{s-r} - 1}{q - 1}.$$

The Betti-numbers follow from the Herzog-Kuhl equations.
Example with $\mathbb{R}_2(3)$. Use

$$\beta_{i,d_i} = \prod_{j \neq 0,i} |\frac{d_j - d_0}{d_j - d_i}|,$$

for $(d_1 = 4, d_2 = 6, d_3 = 7)$. we obtain

$$0 \leftarrow R_M \leftarrow S \leftarrow S(-4)^7 \leftarrow S(-6)^{14} \leftarrow S(-7)^8 \leftarrow 0.$$

The two (only interesting) elongation matroids are uniform, and their Betti-tables are then known. Putting the information from all Betti-tables together and using the Corollary by [J-R-V] above one finds the $A_i(q^m)$ (number of code words of weight m over $\mathbb{F}_q$) for all m, as already done by other methods, e.g. in Example 14 of "Weight enumeration of codes from finite spaces", Jurrius, DCC, 2012. One can then also find the higher weight enumerator polynomials of the code by Theorem 3 in that article.

(The matroid simplicial complexes of) Reed-Muller codes of the first order are not of constant weight (2 weights), but have pure resolutions, as have their elongations, and they may be treated in a very similar way.