A combinatorial-algebraic approach to the generalized Hamming weights of a linear code

ECCO 2016, Medellin

Mehdi Garrousian (U. los Andes)

with Ben Anzis and Stefan Tohaneanu (U. Idaho)

July 14, 2016

Generalized Star configurations, Linear codes and the Tutte Polynomial

ECCO 2016, Medellin
Mehdi Garrousian (U. los Andes)

with Ben Anzis and Stefan Tohaneanu (U. Idaho)

July 14, 2016

- Coding theory is the study of efficient and accurate methods of transferring data.
- A codeword is a block of data which we can think of as an element of a vector space.
- A rank k linear code $\mathcal{C}$ in $V = \mathbb{K}^n$ has the property that all linear combinations of codewords are again codewords.
- Codewords contain redundancies to allow error correction.
- An $[n, k, d]$-linear code consists k-bit messages using n-bit codewords where distinct codewords are different in at least d bits.

Example

Consider one bit codes over $\mathbb{K} = \mathbb{F}_2 = \{0, 1\}$, ie. $k = 1$

- If $n = 1$, then coding is useless.
- If $n = 2$, $0 \mapsto 00, 1 \mapsto 11$, then we can detect one error, ie. 10 and 01 have errors but we won't know how to correct them.
- If $n = 3$, then we can correct $110, 101, 011$ to 111 and $100, 010, 001$ to 000.
- Using $n = 4$ is too wasteful.

A metric on the codewords

Let $x, y \in \mathcal{C} \subset V = \mathbb{K}^n$,

$$d(x, y) = \#\{i : x_i \neq y_i\}.$$

Properties:

- $d(x, y) = 0$ if and only if $x = y$
- $d(x, y) = d(y, x)$
- $d(x, y) + d(y, z) \geq d(x, z)$

Linear Codes

A $[n, k, d]$-linear code $\mathcal{C}$ is determined by a generating matrix

$$G = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{k1} & a_{k2} & \cdots & a_{kn} \end{bmatrix}, a_{ij} \in \mathbb{K},$$

where $\mathbb{K}$ is any field and $\mathcal{C}$ is the image of G.

$$\mathcal{C} = \operatorname{im} G, \quad n = \operatorname{length} \mathcal{C}, \quad k = \dim \mathcal{C}$$

The minimum distance (or Hamming distance), the smallest number of non-zero entries in a non-zero codeword.

$$d = \min\{d(x, y) : x, y \in \mathcal{C}\} = \min\{wt(x) = d(0, x) : x \in \mathcal{C}\}$$

The minimum distance (or Hamming distance), the smallest number of non-zero entries in a non-zero codeword.

$$d = \min\{d(x, y) : x, y \in \mathcal{C}\} = \min\{wt(x) = d(0, x) : x \in \mathcal{C}\}$$

The goal of coding theory is to maximize the minimum distance.
If the minimum distance is $d = 2c + 1$, then any code with c errors can be corrected.

The minimum distance (or Hamming distance), the smallest number of non-zero entries in a non-zero codeword.

$$d = \min\{d(x,y) : x, y \in \mathcal{C}\} = \min\{wt(x) = d(0,x) : x \in \mathcal{C}\}$$

The goal of coding theory is to maximize the minimum distance.
If the minimum distance is $d = 2c + 1$, then any code with c errors can be corrected.
Goal: use commutative/homological algebra tools to study the minimum distance.

Generalized Hamming weights

Let $\mathcal{D} \subseteq \mathcal{C}$ be a subcode. The support of $\mathcal{D}$ is

$$Supp(\mathcal{D}) := \{i : \exists (x_1, \ldots, x_n) \in \mathcal{D} \text{ with } x_i \neq 0\}.$$

For any $r = 1, \ldots, k$, the r^{th} *generalized Hamming weight of* $\mathcal{C}$ is the positive number

$$d_r(\mathcal{C}) := \min_{\mathcal{D} \subseteq \mathcal{C},\, \dim \mathcal{D} = r} |Supp(\mathcal{D})|.$$

Note that $d_1(\mathcal{C}) = d$ and by convention, $d_0(\mathcal{C}) = 0$.

What are the higher weights good for?

Let Δ_s be the number of uncertain bits when s bits are tapped. V. K. Wei shows that

$$d_{n-s-\Delta_s}(\mathcal{C}^\perp) \leq n - s < d_{n-s-\Delta_s+1}(\mathcal{C}^\perp).$$

Hyperplane arrangements

A matrix such as G also determines an arrangement of hyperplanes

$$\mathcal{A} = \{H_1, \ldots, H_n\}, \quad H_i = \ker \ell_i,$$

where $\ell_i = \sum_j a_{ji} x_j$ the linear functional dual to the ith column of G. Every arrangement is a realization of a matroid which tells us how the hyperplanes intersect.

Hyperplane arrangements

A matrix such as G also determines an arrangement of hyperplanes

$$\mathcal{A} = \{H_1, \dots, H_n\}, \quad H_i = \ker \ell_i,$$

where $\ell_i = \sum_j a_{ji} x_j$ the linear functional dual to the ith column of G. Every arrangement is a realization of a matroid which tells us how the hyperplanes intersect.

A matroid on a ground set $[n]$ is given by a rank function $r : 2^{[n]} \to \mathbb{Z}_{\geq 0}$ subject to:

(R1) $r(A) \leq |A|$ for any $A \subseteq [n]$,

(R2) If $A \subseteq B \subseteq [n]$, then $r(A) \leq r(B)$,

(R3) (submodularity) $r(A \cup B) + r(A \cap B) \leq r(A) + r(B)$, for all $A, B \subseteq [n]$.

Matroids from linear codes

Our matrix G determines a rank k matroid $\mathsf{M}(\mathcal{C})$:

$$I \subseteq [n] \mapsto r(I) = \operatorname{rank} G_I$$

Example

Consider $G_1 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$. The rank function of $\mathsf{M}(\mathcal{C}) = U_{2,3}$ is

I	$\emptyset$	$1, 2, 3$	$12, 13, 23$	123
$r(I)$	0	1	2	2

The first Hamming distance is determined by rank $k-1$ elements of M.

$$d_1(\mathcal{C}) = n - \max\{|I| : r(I) = k-1\}$$

Matroids from linear codes

Our matrix G determines a rank k matroid $\mathsf{M}(\mathcal{C})$:

$$I \subseteq [n] \mapsto r(I) = \operatorname{rank} G_I$$

Example

Consider $G_1 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$. The rank function of $\mathsf{M}(\mathcal{C}) = U_{2,3}$ is

I	$\emptyset$	$1, 2, 3$	$12, 13, 23$	123
$r(I)$	0	1	2	2

The rth Hamming distance is determined by rank $k - r$ elements of M.

$$d_r(\mathcal{C}) = n - \max\{|I| : r(I) = k - r\}$$

Tutte Polynomial

The Tutte Polynomial of $\mathcal{C}$ is

$$T_{\mathcal{C}}(x,y) = \sum_{I \subseteq [n]} (x-1)^{k-r(I)} (y-1)^{|I|-r(I)}.$$

Tutte Polynomial

The Tutte Polynomial of $\mathcal{C}$ is

$$T_{\mathcal{C}}(x, y) = \sum_{I \subseteq [n]} (x-1)^{k-r(I)} (y-1)^{|I|-r(I)}.$$

Example

In the last example, the minimum distance is $d = 3 - 1 = 2$, and

$$\begin{aligned} T(x, y) &= \underbrace{(x-1)^2}_{\emptyset} + \underbrace{3(x-1)}_{1,2,3} + \underbrace{3}_{12,13,23} + \underbrace{(y-1)}_{123} \\ &= x^2 + x + y. \end{aligned}$$

Other reincarnations

A formula by Berget: if $I \subset [n]$, then let $\ell_I = \Pi_{i \in I} \ell_i$, and

$$P(\mathcal{C})_{i,j} = \mathrm{Span}_{\mathbb{K}}\{\ell_I : r([n]-I) = i \leq |[n]-I| = j\},$$

then

$$T(x+1,y) = \sum_{1 \leq i \leq j \leq n} \left(\dim P(\mathcal{C})_{i,j}\right) \, x^{k-i} y^{j-i}.$$

Other reincarnations

A formula by Berget: if $I \subset [n]$, then let $\ell_I = \Pi_{i \in I} \ell_i$, and

$$P(\mathcal{C})_{i,j} = \mathrm{Span}_{\mathbb{K}}\{\ell_I : r([n] - I) = i \leq |[n] - I| = j\},$$

then

$$T(x+1, y) = \sum_{1 \leq i \leq j \leq n} (\dim P(\mathcal{C})_{i,j})\ x^{k-i} y^{j-i}.$$

A consequence of a formula by Crapo:

$$T(x+1, y) = \sum_{X \in \mathcal{L}(\mathsf{M}), i \geq 0} |Q_{i,I,X}|\ x^{k-r(I)} y^{i-r(I)},$$

where $Q_{i,I,X} = \{I \subseteq [n] : I \text{ is independent}, \mathrm{cl}(I) = X, |I \cup \mathrm{ex}(I)| = i\}$.

Tutte

Lemma

The first minimum distance is determined by the largest power of y in a term of the form xy^p that appears in $T_{\mathcal{C}}(x+1, y)$.

$$d_1(\mathcal{C}) = n - p - k + 1$$

Also the coefficient of xy^p gives the number of projective codewords of minimum weight.

Tutte

Lemma

The rth minimum distance is determined by the largest power of y in a term of the form $x^r y^{p_r}$ that appears in $T_{\mathcal{C}}(x+1, y)$.

$$d_r(\mathcal{C}) = n - p_r - k + r$$

Also the coefficient of xy^p gives the number of projective codewords of minimum weight.

Tutte

Lemma

The rth minimum distance is determined by the largest power of y in a term of the form $x^r y^{p_r}$ that appears in $T_{\mathcal{C}}(x+1, y)$.

$$d_r(\mathcal{C}) = n - p_r - k + r$$

Also the coefficient of xy^p gives the number of projective codewords of minimum weight. (?)

Example

Back to example G_1:

$$T(x+1, y) = x^2 + 3x + y + 2.$$

Evidently, $p_1 = p_2 = 0$, $d_1 = 3 - 2 - 0 + 1 = 2$ and $d_2 = 3 - 2 - 0 + 2 = 3$. There are exactly 3 codewords of distance 2 and one 2-dim subcode of distance 3.

A bigger example - A_5

Example

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & -1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & -1 & 0 & -1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & -1 & 0 & -1 & -1 \end{bmatrix}$$

The parametrization $T(x+1,y)$ of the Tutte polynomial is

$$\begin{aligned} T(x+1,y) \quad = \quad & y^6 + 4y^5 + 10y^4 + x^4 + 5xy^3 + 15xy^2 + 40xy \\ & + 10x^2y + 35x^2 + 10x^3 + 20y^3 + 30y^2 + 50x + 36y + 24. \end{aligned}$$

We have, $p_1 = 3$, $p_2 = 1$ and $p_3 = p_4 = 0$.

$$\begin{aligned} d_1 = 10 - 4 - 3 + 1 = 4, \quad & \boxed{d_2 = 10 - 4 - 1 + 2 = 7} \\ d_3 = 10 - 4 - 0 + 3 = 9, \quad & d_4 = 10 - 4 - 0 + 4 = 10 \end{aligned}$$

(example to be continued)

Generalized star configuration ideals

Let $\Lambda_{\mathcal{C}} = (\ell_1, \ldots, \ell_n)$ be the linear forms in $R := \mathbb{K}[x_1, \ldots, x_k]$ dual to the columns of G. Let $I_a(\mathcal{C}) \subset R$ be the ideal generated by all a-fold products, i.e.

$$I_a(\mathcal{C}) = \langle \ell_{i_1} \cdots \ell_{i_a} | 1 \leq i_1 < \cdots < i_a \leq n \rangle.$$

Generalized star configuration ideals

Let $\Lambda_{\mathcal{C}} = (\ell_1, \ldots, \ell_n)$ be the linear forms in $R := \mathbb{K}[x_1, \ldots, x_k]$ dual to the columns of G. Let $I_a(\mathcal{C}) \subset R$ be the ideal generated by all a-fold products, i.e.

$$I_a(\mathcal{C}) = \langle \ell_{i_1} \cdots \ell_{i_a} | 1 \leq i_1 < \cdots < i_a \leq n \rangle.$$

De Boer and Pellikaan had observed that the minimum distance satisfies

$$\begin{aligned} d &= \max\{a | \operatorname{codim}(I_a(\mathcal{C})) = k\} \\ &= \min\{a | V(I_{a+1}(\mathcal{C})) \neq \emptyset \text{ in } \mathbb{P}^{k-1}\}. \end{aligned}$$

This is simply because a vector has $n - j$ entries equal to zero, then all $j + 1$-fold products vanish.

Back to the A_5 example:

a	$1,\dots,4$	$5,\dots,7$	$8,\dots,9$	10
$\operatorname{codim} I_a(\mathcal{C})$	4	3	2	1

Back to the A_5 example:

a	$1,\dots,4$	$5,\dots,7$	$8,\dots,9$	10
$\operatorname{codim} I_a(\mathcal{C})$	4	3	2	1

In fact, this can be made more precise. For $1 \leq a \leq 4$, we have

$$I_a(\mathcal{C}) = \mathfrak{m}^a,$$

where $\mathfrak{m} = \langle x_1, x_2, x_3, x_4 \rangle$, and

$$V(I_5(\mathcal{C})) = \{\text{minimal codewords of length } 4\} \subset \mathbb{P}^3.$$

Back to the A_5 example:

a	$1,\ldots,4$	$5,\ldots,7$	$8,\ldots,9$	10
$\operatorname{codim} I_a(\mathcal{C})$	4	3	2	1

In fact, this can be made more precise. For $1 \leq a \leq 4$, we have

$$I_a(\mathcal{C}) = \mathfrak{m}^a,$$

where $\mathfrak{m} = \langle x_1, x_2, x_3, x_4 \rangle$, and

$$V(I_5(\mathcal{C})) = \{\text{minimal codewords of length } 4\} \subset \mathbb{P}^3.$$

Proposition

For $1 \leq r \leq k$, we have

$$d_r(\mathcal{C}) = \max\{a : \operatorname{codim}(I_a(\mathcal{C})) = k - r + 1\}.$$

How to find these minimal subcodes?

Let I be maximal flat of rank $k-r$.

- Compute $\ker G_I = \mathrm{span}\{v_1, \ldots, v_r\}$.
- Find $w_i = v_i G$.
- $\mathcal{C}_I = \mathrm{Span}\{w_1, \ldots, w_r\}$.

How to find these minimal subcodes?

Let I be maximal flat of rank $k-r$.

- Compute $\ker G_I = \mathrm{span}\{v_1, \ldots, v_r\}$.
- Find $w_i = v_i G$.
- $\mathcal{C}_I = \mathrm{Span}\{w_1, \ldots, w_r\}$.

0	1	2	3	4	5	6	7	8	9
x_1	x_2	x_3	x_4	$x_1 - x_2$	$x_1 - x_3$	$x_1 - x_4$	$x_2 - x_3$	$x_2 - x_4$	$x_3 - x_4$

Back to our example, 014 is a maximal rank two flat. The kernel of the minor is generated by e_3 and e_4. So,

$$\mathcal{C}_{014} = \mathrm{RowSpace}\begin{bmatrix} 0 & 0 & 1 & 0 & 0 & -1 & 0 & -1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & -1 & 0 & -1 & -1 \end{bmatrix}$$

and this has weight 7.

Hilbert polynomials

Let $X = V(I)$ be a projective variety in $\mathbb{P}^{k-1}$ defined by the homogeneous ideal $I \subset \mathbb{K}[x_1, \ldots, x_k]$ of codimension (height) c. The values of $\dim_{\mathbb{K}}(R/I)_t$ for large enough t are given by a polynomial, called the *Hilbert Polynomial*.

$$\begin{aligned} HP(R/I, t) &= \deg(X) P_{k-c-1} + \cdots \\ &= \frac{\deg(X)}{(k-c-1)!} t^{k-c-1} + \cdots \end{aligned}$$

Here, $P_m = \binom{t+m}{m}$ denotes the Hilbert polynomial of $\mathbb{P}^m$.

Still the A_5 example

$$
\begin{aligned}
T(x+1,y) &= y^6+4y^5+10y^4+x^4+5xy^3+15xy^2+40xy \\
&\quad +10x^2y+35x^2+10x^3+20y^3+30y^2+50x+36y+24
\end{aligned}
$$

a	$HP(R/I_a(\mathcal{C}),t)$
5	$5P_0$
6	$(5+15)P_0$
7	$(5+15+40)P_0$
8	$10P_1+40P_0$
9	$(10+35)P_1-240P_0$
10	$10P_2-45P_1+120P_0$

The degree of a star configuration

The primary decomposition of $I_a(\mathcal{C})$ is partly determined by $\mathsf{M}(\mathcal{C})$. Let $\nu(\mathfrak{p})$ to be the number of linear forms ℓ of $\mathcal{C}$ with $\ell \in \mathfrak{p}$.

Proposition

Let $r = 0, \ldots, k-1$, *and let* $a = d_r(\mathcal{C}) + j \leq d_{r+1}(\mathcal{C})$. *Then,*

$$I_a(\mathcal{C}) = \mathfrak{p}_1^{a-n+\nu(\mathfrak{p}_1)} \cap \cdots \cap \mathfrak{p}_s^{a-n+\nu(\mathfrak{p}_s)} \cap K,$$

where $\mathrm{Min}_{k-r}(I_a(\mathcal{C})) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\} = \{\mathfrak{p}_X : X \in \mathcal{L}_{k-r}(\mathsf{M})\}$, *and* K *is an ideal of codimension* $> k - r$.

$$\mathcal{L}_3(\mathsf{M}) = \{0149, 0257, 0368, 0789, 1357, 1569, 1268, 2349, 3458, 2467, 013467, 012458, 023569, 123789, 456789\}$$

0	1	2	3	4	5	6	7	8	9
x_1	x_2	x_3	x_4	$x_1 - x_2$	$x_1 - x_3$	$x_1 - x_4$	$x_2 - x_3$	$x_2 - x_4$	$x_3 - x_4$

For instance, $\mathfrak{p}_{0149} = \langle x_1, x_2, x_3 - x_4 \rangle$ and $a - n + \nu = 7 - 10 + 4 = 1$, and $\mathfrak{p}_{013467} = \langle x_1, x_2, x_4 \rangle$ and $a - n + \nu = 7 - 10 + 6 = 3$.

$$\begin{aligned} I_7(\mathcal{C}) = \; & \langle x_1, x_2, x_3 - x_4 \rangle \cap \langle x_1, x_3, x_2 - x_4 \rangle \cap \langle x_1, x_4, x_2 - x_3 \rangle \cap \\ & \langle x_1, x_3 - x_4, x_2 - x_4 \rangle \cap \langle x_4, x_2, x_1 - x_3 \rangle \cap \langle x_2, x_1 - x_4, x_3 - x_4 \rangle \cap \\ & \langle x_2, x_3, x_1 - x_4 \rangle \cap \langle x_3, x_4, x_1 - x_2 \rangle \cap \langle x_4, x_2 - x_3, x_1 - x_3 \rangle \cap \\ & \langle x_3, x_2 - x_4, x_1 - x_4 \rangle \cap \\ & \langle x_1, x_2, x_4 \rangle^3 \cap \langle x_1, x_2, x_3 \rangle^3 \cap \langle x_1, x_3, x_4 \rangle^3 \cap \langle x_2, x_3, x_4 \rangle^3 \cap \\ & \langle x_1 - x_2, x_1 - x_3, x_1 - x_4, x_2 - x_4, x_2 - x_3, x_3 - x_4 \rangle^3 \cap \mathfrak{m}^7 \end{aligned}$$

Recall that

$$T(x+1,y) = \sum_{i,j} c_{i,j} x^i y^i,$$

and p_r is the largest power of y in a term of the form $x^r y^*$ that appears in $T_{\mathcal{C}}(x+1,y)$.

Theorem

Let $\mathcal{C}$ be an $[n,k]$-linear code in $R := \mathbb{K}[x_1,\dots,x_k]$. Let $a = d_r(\mathcal{C}) + j$, where $r = 1,\dots,k$ and $j = 1,\dots,d_{r+1}(\mathcal{C}) - d_r(\mathcal{C})$. Then the degree of $I_a(\mathcal{C})$ is determined by the coefficients of the Tutte polynomial:

$$\deg(I_a(\mathcal{C})) = c_{r,p_r} + c_{r,p_r-1} + \cdots + c_{r,p_r-j+1}.$$

Proof.

Use the primary decomposition, exact sequences and some combinatorial magic ... □

Minimal generators

Proposition

Let $\mathcal{C}$ be an $[n,k]-$linear code. Then, with the previous notations, for any $a \in \{1,\ldots,n\}$, one has

$$\mu(I_a(\mathcal{C})) = \sum_{u=0}^{\min\{k,n-a\}} c_{k-u,n-a-u}.$$

Minimal generators

Proposition

Let $\mathcal{C}$ be an $[n,k]-$linear code. Then, with the previous notations, for any $a \in \{1,\dots,n\}$, one has

$$\mu(I_a(\mathcal{C})) = \sum_{u=0}^{\min\{k,n-a\}} c_{k-u,n-a-u}.$$

Proof.

Since $I_a(\mathcal{C})$ is generated in degree a, $\mu(I_a(\mathcal{C})) = \dim(I_a(\mathcal{C}))_a$. On the other hand,

$$(I_a(\mathcal{C}))_a = \bigoplus_{0 \le u \le n-a} P(\mathcal{C})_{u,n-a}.$$

Then, look at Berget's formula:

$$T(x+1,y) = \sum_{1 \le i \le j \le n} \left(\dim P(\mathcal{C})_{i,j}\right)\, x^{k-i} y^{j-i}.$$

$\square$

$$T(x+1,y) = y^6 + 4y^5 + 10y^4 + x^4 + 5xy^3 + 15xy^2 + 40xy + 10x^2y + 35x^2 + 10x^3 + 20y^3 + 30y^2 + 50x + 36y + 24$$

$$\mu(I_7(\mathcal{C})) = \sum_{u=0}^{\min\{4,10-7\}} u_{4-u,3-u} = c_{4,3} + c_{3,2} + c_{2,1} + c_{1,0} = 0 + 0 + 10 + 50$$

The Betti table of $I_7(\mathcal{C})$:

	0	1	2	3	4
total:	1	60	135	100	24
0:	1	.	.	.	.
1:	.	.	.	.	.
2:	.	.	.	.	.
3:	.	.	.	.	.
4:	.	.	.	.	.
5:	.	.	.	.	.
6:	.	60	135	100	24

Conjecture (1)

For any linear code $\mathcal{C}$ and any a, the ideal $I_a(\mathcal{C})$ has a linear graded free resolution.

Equivalently, the Castelnuovo-Mumford regularity, $\mathrm{reg}(R/I_a(\mathcal{C}))$, equals $a-1$.

Deletion-contraction

Every linear code determines a Fitting module $\mathrm{Fitt}(\mathcal{C})$. Let $\mathcal{C}'$ and $\mathcal{C}''$ denote the deletion and contraction of $\mathcal{C}$ wrt a given element, say the first column of G.

Conjecture (2)

When ℓ is not a coloop,

$$0 \to \mathrm{Fitt}(\mathcal{C}')(-1) \xrightarrow{\cdot \ell} \mathrm{Fitt}(\mathcal{C}) \to \mathrm{Fitt}(\mathcal{C}'') \to 0$$

is exact.

Deletion-contraction

Every linear code determines a Fitting module $\mathrm{Fitt}(\mathcal{C})$. Let $\mathcal{C}'$ and $\mathcal{C}''$ denote the deletion and contraction of $\mathcal{C}$ wrt a given element, say the first column of G.

Conjecture (2)

When ℓ is not a coloop,

$$0 \to \mathrm{Fitt}(\mathcal{C}')(-1) \xrightarrow{\cdot\ell} \mathrm{Fitt}(\mathcal{C}) \to \mathrm{Fitt}(\mathcal{C}'') \to 0$$

is exact.

Recall, $I : f = \{g : fg \in I\}$. This is equivalent to understanding the SES:

$$0 \xrightarrow{?} \frac{R}{I'_{a-1}} \xrightarrow{\cdot\ell} \frac{R}{I_a} \longrightarrow \frac{R''}{I''_a} \longrightarrow 0,$$

Deletion-contraction

Every linear code determines a Fitting module $\mathrm{Fitt}(\mathcal{C})$. Let $\mathcal{C}'$ and $\mathcal{C}''$ denote the deletion and contraction of $\mathcal{C}$ wrt a given element, say the first column of G.

Conjecture (2)

When ℓ is not a coloop,

$$0 \to \mathrm{Fitt}(\mathcal{C}')(-1) \xrightarrow{\cdot\ell} \mathrm{Fitt}(\mathcal{C}) \to \mathrm{Fitt}(\mathcal{C}'') \to 0$$

is exact.

Recall, $I : f = \{g : fg \in I\}$. This is equivalent to understanding the SES:

$$0 \to \frac{R}{I_a : \ell}(-1) \xrightarrow{\cdot\ell} \frac{R}{I_a} \longrightarrow \frac{R}{I_a + \langle\ell\rangle} \longrightarrow 0,$$

Theorem (Tohaneanu and G., 2015)

This is true when $\mathcal{C}$ is MDS (maximum distance separable, $d = n - k + 1$), or equivalently when $\mathsf{M}(\mathcal{C}) = U_{k,n}$.

Theorem (Tohaneanu and G., 2015)

This is true when $\mathcal{C}$ is MDS (maximum distance separable, $d = n - k + 1$), or equivalently when $\mathsf{M}(\mathcal{C}) = U_{k,n}$.

Conjecture (3)

For any $[n, k]-$linear code $\mathcal{C}$ and any $\ell \in \mathcal{C}$ one has

$$I_a(\mathcal{C}) : \ell = I_{a-1}(\mathcal{C}'),$$

for all $1 \leq a \leq n$.

Clearly, $\ell I_{a-1}(\mathcal{C}') \subseteq I_a(\mathcal{C})$.

Theorem

Conjecture 3 $\Rightarrow$ Conjecture 1.

Weak versions

Proposition

Let $\mathcal{C}$ be an $[n, k]$-linear code. If ℓ is a coloop in $\mathsf{M}(\mathcal{C})$, then

$$I_a(\mathcal{C}) : \ell = I_{a-1}(\mathcal{C}'),$$

for all $a = 1, \ldots, n$.

Weak versions

Proposition

Let $\mathcal{C}$ be an $[n,k]$-linear code. If ℓ is a coloop in $\mathsf{M}(\mathcal{C})$, then

$$I_a(\mathcal{C}) : \ell = I_{a-1}(\mathcal{C}'),$$

for all $a = 1, \ldots, n$.

Proposition

For any $a = 2, \ldots, n$, and any $\ell \in \mathcal{C}$ one has:

$$\sqrt{I_a(\mathcal{C}) : \ell} = \sqrt{I_{a-1}(\mathcal{C}')},$$

where $\mathcal{C}' = \mathcal{C} \setminus \{\ell\}$.

The challenge part is controlling the embedded components of the primary decomposition.

Preguntas

- Compute the Hilbert polynomial entirely from the Tutte polynomial.
- Compute all Betti numbers of any star configuration ideal. Are they even combinatorially determined?
- Redo the whole story/theory over polynomial rings and use the theory of matroids over rings.

Preguntas

- Compute the Hilbert polynomial entirely from the Tutte polynomial.
- Compute all Betti numbers of any star configuration ideal. Are they even combinatorially determined?
- Redo the whole story/theory over polynomial rings and use the theory of matroids over rings.