Generalized minimum distance functions for linear codes

Alexandra Seceleanu

and

Susan Cooper, Stefan Tohăneanu, Maria Vaz Pinto, Rafael Villarreal

2018 CMS Winter Meeting

Linear codes and Hamming distance

Let K be an arbitrary field (usually finite in practice).

Definition

A **linear code** C of length s and dimension $n+1$ is the image of an injective K-linear map
$$K^{n+1} \to K^s.$$

Definition

The weight of a codeword is $||x|| = \#\{i \mid x_i \neq 0\}$.
The **minimum Hamming distance** of C is

$$d(C) = \min\{||x|| \mid x \in C, x \neq 0\}.$$

Points from generating matrices

Then

$$C = \text{Image}\left(K^{n+1} \to K^s\right) = \text{Row}(G),$$

where G is a $(n+1) \times s$ matrix called a **generating matrix** for C.

Points from generating matrices

Then

$$C = \mathrm{Image}\left(K^{n+1} \to K^s\right) = \mathrm{Row}(G),$$

where G is a $(n+1) \times s$ matrix called a **generating matrix** for C.

Take the columns of G and turn them into points:

Define **the set of points associated to** C to be

$$\mathbb{X}_C = \{P_1, \ldots, P_s\} \subset \mathbb{P}^n, \text{where}$$

P_i is the point with coordinates given by the i-th column of G.

Example

The code $C = \mathrm{Row}(G)$ with generating matrix

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

has

- length 7, dimension 4
- Hamming distance $d(C) = 3$.

Example - the Hamming $[7,4,3]_2$–code

Example

The code $C = \mathrm{Row}(G)$ with generating matrix

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

has

- length 7, dimension 4
- Hamming distance $d(C) = 3$.

The set of points associated to C is

$$\mathbb{X}_C = \{P_1, P_2, P_3, P_4, P_5, P_6, P_7\},$$

where P_2, P_3, P_4, P_5 lie on the hyperplane $t_1 = 0$.

Hamming distance and hyp-functions

Definition

For a finite set $\mathbb{X}$, let $\mathrm{hyp}(\mathbb{X})$ denote the maximum number of points of $\mathbb{X}$ contained in a hyperplane.

Proposition [Tohăneanu–van Tuyl]

$$d(C) = |\mathbb{X}_C| - \mathrm{hyp}(\mathbb{X}_C)$$

Hamming distance and hyp-functions

Definition

For a finite set $\mathbb{X}$, let $\mathrm{hyp}(\mathbb{X})$ denote the maximum number of points of $\mathbb{X}$ contained in a hyperplane.

Proposition [Tohăneanu–van Tuyl]

$$d(C) = |\mathbb{X}_C| - \mathrm{hyp}(\mathbb{X}_C)$$

$$\begin{aligned} &= \deg(\mathbb{X}_C) - \max\{\deg(\mathbb{X}_C \cap H) \mid H \text{ a hyperplane}\} \\ &= \deg(S/I(\mathbb{X}_C)) - \max\{\deg(S/(I(\mathbb{X}_C), F) \mid F \in S_1\}. \end{aligned}$$

Generalized minimum distance (GMD)

Definition

For any homogeneous ideal $I \subset S$, the family of **generalized minimum distance functions** is defined by

$$\delta_I(d,r) := \deg(S/I) - \max\{\deg(S/(I,\underline{F}))|\, \underline{F} \in \mathcal{F}_{d,r}\}$$

where $\mathcal{F}_{d,r}$ is the set of all r-tuples of forms of degree d in S that are linearly independent over K modulo the ideal I.

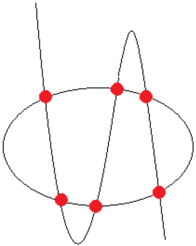
Definition

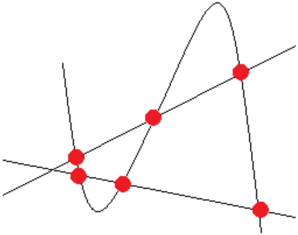
The **generalized hyp function** is

$$\mathrm{hyp}_I(d,r) := \max\{\deg(S/(I,\underline{F}))|\, \underline{F} \in \mathcal{F}_{d,r}\}.$$

Example

I = reduced complete intersection of type (2,3).





hyp$(1,1)$	2	$\delta(1,1)$	4
hyp$(2,1)$	4	$\delta(2,1)$	2
hyp$(3,1)$	5	$\delta(3,1)$	1

hyp$(1,1)$	3	$\delta(1,1)$	3
hyp$(2,1)$	4	$\delta(2,1)$	2
hyp$(3,1)$	5	$\delta(3,1)$	1

What do GMD functions measure?

Let $\mathbb{X}_C$ be a reduced set of points corresponding to a linear code C.

- $\delta_{I(\mathbb{X}_C)}(1,1)$ recovers the Hamming distance of C

What do GMD functions measure?

Let $\mathbb{X}_C$ be a reduced set of points corresponding to a linear code C.

- $\delta_{I(\mathbb{X}_C)}(1,1)$ recovers the Hamming distance of C
- $\delta_{I(\mathbb{X}_C)}(d,1)$ is the Hamming distance of a Reed-Muller code C', where $\mathbb{X}_{C'} = V_d(\mathbb{X}_C)$ is the image of C under a Veronese map

What do GMD functions measure?

Let $\mathbb{X}_C$ be a reduced set of points corresponding to a linear code C.

- $\delta_{I(\mathbb{X}_C)}(1,1)$ recovers the Hamming distance of C
- $\delta_{I(\mathbb{X}_C)}(d,1)$ is the Hamming distance of a Reed-Muller code C', where $\mathbb{X}_{C'} = V_d(\mathbb{X}_C)$ is the image of C under a Veronese map
- $\delta_{I(\mathbb{X}_C)}(1,r)$ measures the the size of the smallest support of an r-dimensional linear subcode of C

What do GMD functions measure?

Let $\mathbb{X}_C$ be a reduced set of points corresponding to a linear code C.

- $\delta_{I(\mathbb{X}_C)}(1,1)$ recovers the Hamming distance of C
- $\delta_{I(\mathbb{X}_C)}(d,1)$ is the Hamming distance of a Reed-Muller code C', where $\mathbb{X}_{C'} = V_d(\mathbb{X}_C)$ is the image of C under a Veronese map
- $\delta_{I(\mathbb{X}_C)}(1,r)$ measures the the size of the smallest support of an r-dimensional linear subcode of C
- $\delta_{I(\mathbb{X}_C)}(d,r)$ measures the smallest degree of a residual subscheme

$$\delta_{I(\mathbb{X}_C)}(d,r) = \min\{\deg(S/I : (\underline{F})) \mid \underline{F} \in \mathcal{F}_{d,r}\}$$

Example

Let $I = (t_1^3, t_2t_3) \subset S = K[t_1, t_2, t_3]$. We obtain:

$$(\delta_I(d,r))_{d,r} = \begin{bmatrix} 3 & 5 & 6 & 6 & 6 & 6 & \ldots \\ 2 & 3 & 4 & 5 & 6 & 6 & \ldots \\ 1 & 2 & 3 & 4 & 5 & 6 & \ldots \end{bmatrix}.$$

The regularity and the degree of S/I are 3 and 6.

Monotonicity of the GMD functions

Example

Let $I = (t_1^3, t_2t_3) \subset S = K[t_1, t_2, t_3]$. We obtain:

$$(\delta_I(d, r))_{d,r} = \begin{bmatrix} 3 & 5 & 6 & 6 & 6 & 6 & \dots \\ 2 & 3 & 4 & 5 & 6 & 6 & \dots \\ 1 & 2 & 3 & 4 & 5 & 6 & \dots \end{bmatrix}.$$

The regularity and the degree of S/I are 3 and 6.

Theorem (CSTVV)

Let I be unmixed. Then

- $\delta_I(d, r)$ *is non-decreasing as a function of r stabilizing to* $\deg(S/I)$ *for* $r \geq H_I(d)$
- $\delta_I(d, r)$ *is non-increasing as a function of d stabilizing to 1.*

Bounding GMD functions

1. Singleton bound

Theorem (CSTVV)

If I is unmixed, $\dim(S/I) = 1$, all associated primes of I are generated by linear forms and there exists $h \in S_1$ regular on S/I then

$$\delta_I(d, 1) \leq \deg(S/I) - H_I(d) + 1, \ \textit{for } d \geq 1.$$

Bounding GMD functions

2. Cayley-Bacharach type conjecture

Conjecture

Let $I \subset S$ be a complete intersection of type $(d_1, \dots, d_c)$ with $\dim(S/I) = 1$ *and the associated primes of I generated by linear forms. Then*

$$\delta_I(d) \geq (d_{k+1} - \ell) d_{k+2} \cdots d_c \quad \text{if} \quad 1 \leq d \leq \sum_{i=1}^{c} (d_i - 1) - 1,$$

where $0 \leq k \leq c-1$ and ℓ are integers such that

$$d = \sum_{i=1}^{k} (d_i - 1) + \ell \text{ and } 1 \leq \ell \leq d_{k+1} - 1.$$

The regularity of the δ function

Theorem (CSTVV)

Let I be an unmixed graded ideal whose associated primes are generated by linear forms. Then $\delta_I(d,1) = 1$ for

$$d \geq \min\{\alpha\left((I : \mathfrak{p})/I\right) \mid \mathfrak{p} \in \mathrm{Ass}(I)\}.$$

In particular, if I is level, then $\delta_I(d,1) = 1$ for

$$d \geq \mathrm{reg}(S/I).$$

Thank You !