Properties of codes in rank metric

Pierre Loidreau

CELAR and IRMAR, Université de Rennes 1

June 18, 2008

Introduction

- Correcting criss-cross errors
- Related to the measure of diversity in MIMO channels
- Metric used in random network coding
- Used in cryptographic applications

Goal: Study properties of the metric

Outline of the talk

Definition of rank metric

Definition

- $\gamma_1, \ldots, \gamma_m$, *a basis of* $\mathbb{F}_{q^m}/\mathbb{F}_q$,
- $\mathbf{e} = (e_1, \ldots, e_n) \in (\mathbb{F}_{q^m})^n$, $e_i \mapsto (e_{1i}, \ldots, e_{mi})^T$,

$$\forall \mathbf{e} \in \mathbb{F}_{q^m}, \quad \mathrm{Rk}(\mathbf{e}) \stackrel{def}{=} \mathrm{Rk} \begin{pmatrix} e_{11} & \cdots & e_{1n} \\ \vdots & \ddots & \vdots \\ e_{m1} & \cdots & e_{mn} \end{pmatrix}$$

Definition

$\mathcal{C} \subset \mathbb{F}_{q^m}^n$ *is a* $(n, M, d)_r$*-code if*

- $M = |\mathcal{C}|$
- *Min. rank distance:* $d = \min_{\mathbf{c}_1 \neq \mathbf{c}_2 \in \mathcal{C}} \mathrm{Rk}(\mathbf{c}_1 - \mathbf{c}_2)$

Bounds in rank metric

Bounds on spheres and balls

- Volume of sphere: $q^{(m+n-1)t-t^2} \leq \mathcal{S}_t \leq q^{(m+n+1)t-t^2}$
- Volume of ball: $q^{(m+n-1)t-t^2} \leq \mathcal{B}_t \leq q^{(m+n+1)t-t^2+1}$

Upperbounds on $(n, M, d)_r$ codes

- Singleton: $M \leq q^{\min(m(n-d+1), n(m-d+1))} \longrightarrow$ MRD codes
- Sphere-packing: $M\mathcal{B}_{\lfloor (d-1)/2 \rfloor} \leq q^{mn} \longrightarrow$ perfect codes

Perfectitude

Proposition

There are no perfect codes in rank metric

Proof.

If a $(n, M, d)_r$ perfect code exist and $t \overset{def}{=} \lfloor (d-1)/2 \rfloor$

- Perfect $\Rightarrow$ $Mq^{(m+n+1)t-t^2+1} \geq M\mathcal{B}_t = q^{mn}$
- Singleton $\Rightarrow$ $q^{m(n-2t)} \geq q^{m(n-d+1)} \geq M$

Hence $q^{1+(n-m+1)t-t^2} \geq 1 \iff 1 + (n-m+1)t - t^2 \geq 0.$

Not possible if $(n < m)$ or $(n = m$ and $t \geq 2)$ □

GV-like bound

Proposition

$(M-1)\mathcal{B}_{d-1} < q^{mn} \implies \exists (n, M, d)_r$ *code*

Proof.

1. If $\mathcal{B}_{d-1} < q^{mn}$ there exists $(n, 2, d)_r$ code
2. By induction, let $\mathcal{C}$ be a $(n, M-1, d)_r$ code, and

$$\mathcal{V} = \cup_{\mathbf{c} \in \mathcal{C}} \mathcal{B}(\mathbf{c}, d-1)$$

   If $(M-1)\mathcal{B}_{d-1} < q^{mn}$, there exists a vector $\mathbf{z} \in \mathbb{F}_{q^m}^n \setminus \mathcal{V}$.
3. $\mathcal{C} \cup \{\mathbf{z}\}$ is $(n, M, d)_r$

□

Asymptotics and GV-bound

Definition

$\mathcal{C}$, $(n, M, d)_r$ is on GV if

$$(M-1) \times \mathcal{B}_{d-1} < q^{mn} \leq M \times \mathcal{B}_{d-1},$$

For $\mathcal{C}$ on GV:

Proposition

If $\log_q M = \lambda(n)m$

$$\frac{d}{m+n} \overset{n \to +\infty}{\sim} \frac{1}{2} - \frac{\sqrt{\log_q M}}{m+n} \sqrt{1 + \frac{(m-n)^2}{4 \log_q M}},$$

Sketch of proof

- From bounds on spheres and balls :

$$mn \leq (m+n+1)(d-1) - (d-1)^2 + 1 + \log_q M,$$
$$\log_q(M-1) + (m+n-2)(d-1) - (d-1)^2 < mn.$$

- Since $\log_q(M-1) \geq \log_q(M) - 1$ we have

$$0 \leq -d^2 + (m+n+3)d + \log_q M - mn - (m+n+1) \quad \Rightarrow \quad \Delta_1$$
$$0 \geq -d^2 + (m+n)d + \log_q M - mn - (m+n) \quad \Rightarrow \quad \Delta_2$$

- Therefore

$$\frac{1}{2} - \frac{-\sqrt{\Delta_1} + 3}{2(m+n)} \leq \frac{d}{m+n} \leq \frac{1}{2} - \frac{\sqrt{\Delta_2}}{2(m+n)}.$$

- Conditions on roots of second order equations

Example: $m = n$, $\log_q M = n^2 R$. In that case

$$\frac{d}{n} \sim 1 - \sqrt{R}.$$

Definition (MRD-codes)

A $(n, M, d)_r$-code over $\mathbb{F}_{q^m}$ is MRD if

- $M = q^{m(n-d+1)}$, *if* $n \leq m$.
- $M = q^{n(m-d+1)}$, *if* $n > m$

Rank weight distribution

$$A_{d+\ell}(n,d) = \begin{bmatrix} n \\ d+\ell \end{bmatrix}_q \sum_{t=0}^{\ell} (-1)^{t+\ell} \begin{bmatrix} d+\ell \\ \ell+t \end{bmatrix}_q q^{\binom{\ell-t}{2}} \left(q^{m(t+1)} - 1\right),$$

Packing density of MRD codes

Definition

The packing density of an $(n, M, d)_r$ code is

$$D = \frac{M\mathcal{B}_{\lfloor (d-1)/2 \rfloor}}{q^{mn}},$$

Proposition

Let $\mathcal{C}$ be a $(n, q^{m(n-2t)}, 2t+1)_r$ over $\mathbb{F}_{q^m}$.

$$\frac{1}{q^{(m-n+2)t+t^2}} \leq D \leq \frac{1}{q^{(m-n-1)t+t^2}},$$

Asymptotically perfect codes

- Consequence: if $m = n$ then $q^{-t^2-2t} \leq D$

Corollary

Let $\{\mathcal{C}_i\}_{i\geq 2}$ be a family of $(i, 2^{i-2}, 3)_r$ MRD-codes over $\mathbb{F}_{2^i}$.

$$\lim_{i\to\infty} D_i = 1.$$

Conclusion

- Going further: Random codes and GV-bound
- How to use results in rank metric applications
- Other bounds: Johnson for example