Asymptotic behaviour of constant rate random codes in rank metric

Pierre Loidreau

DGA and IRMAR, Université de Rennes 1

June 17th, 2012

Outline of the talk

1. Definition of rank metric
2. Bounds in rank metric
3. Asymptotic behaviour of Random codes
   - General case
   - Linear case

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

Definition of rank metric

Definition

- $\gamma_1, \ldots, \gamma_m$, *a basis of* $\mathbb{F}_{q^m}/\mathbb{F}_q$,
- $\mathbf{e} = (e_1, \ldots, e_n) \in (\mathbb{F}_{q^m})^n$, $e_i \mapsto (e_{i1}, \ldots, e_{in})$,

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

Definition

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

- $M = |\mathcal{C}|$
- *Min. rank distance:* $d = \min_{\mathbf{c_1} \neq \mathbf{c_2} \in \mathcal{C}} \mathrm{Rk}(\mathbf{c_1} - \mathbf{c_2})$

Topology of rank metric

Bounds on spheres and balls:

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

GV-like bound

Definition

The $(n, M, d)_r$ code $\mathcal{C}$ reaches the GV-bound if

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

Let $\mathcal{F}$ a family of $(n, M_n = q^{\alpha n^2 R}, d_n)_r$ codes over $\mathbb{F}_{q^{\alpha n}}$ reaching GV-bound

$$\lim_{n \to \infty} d_n/n = \frac{\alpha + 1}{2} - \sqrt{(\alpha - 1)^2/4 + \alpha R}. \qquad (1)$$

Outline of the talk

Sampling space

- Parameters :
  - $0 < R < 1$,
  - $m = \alpha n$
  - $M = q^{\alpha R n^2}$
- Construct $\mathcal{C} = \{\mathbf{c}_1, \ldots, \mathbf{c}_M\}$, such that

$$\forall j \in [1..M], \quad \mathbf{c}_j \xleftarrow{U} \mathbb{F}_{q^{\alpha n}}^n$$

Therefore, for all $j \in [1..M]$ and all $0 \leq i \leq n$

$$\forall\ \mathbf{y} \in \mathbb{F}_{q^{\alpha n}}^n \Pr(\mathrm{Rk}(\mathbf{c}_j - \mathbf{y}) \leq i) = \frac{\mathcal{B}_i}{q^{\alpha n^2}} \leq q^{(\alpha+1)ni - i^2 - \alpha n^2 + \sigma(q)},$$

Random variable - (I)

- Definition

$$\mathcal{D}_i = \sum_{u=1}^{M} \sum_{v=1}^{u-1} \mathbf{1}_{\mathrm{Rk}(\mathbf{c}_u - \mathbf{c}_v) \leq i},$$

- Upper bound on minimum rank distance
  - $d \leq i \Rightarrow \mathcal{D}_i \geq 1$
  - Therefore $\Pr(d \leq i) \leq \Pr(\mathcal{D}_i \geq 1)$

Random variable (II)

Lower bound on the minimum rank distance

- $d \geq \ell \Rightarrow \mathcal{D}_{\ell-1} = 0$ or $\begin{cases} \mathcal{D}_{\ell-1} \geq 1 \\ \mathbf{c}_u = \mathbf{c}_v, \text{ for some } u,\ v \end{cases}$
- Therefore $\Pr(d \geq \ell) \leq \Pr(\mathcal{D}_{\ell-1} = 0) + \Pr(\exists u < v \mid \mathbf{c}_u = \mathbf{c}_v)$

  Birthday Paradox $\Rightarrow \Pr(\exists u < v \mid \mathbf{c}_u = \mathbf{c}_v) = \dfrac{\binom{M}{2}}{q^{\alpha n^2}} \leq \dfrac{M^2}{2q^{\alpha n^2}}.$

- Hence $\Pr(d \geq \ell) \leq \Pr(\mathcal{D}_{i-1} = 0) + \frac{M^2}{2q^{\alpha n^2}}$

Asymptotic equivalent

- Let $\Delta = \frac{\alpha+1}{2} - \sqrt{(\alpha-1)^2/4 + 2\alpha R}$,
  (Recall $\Delta_{GV} = \frac{\alpha+1}{2} - \sqrt{(\alpha-1)^2/4 + \alpha R}$)
- Proposition

Proposition

- *For ϵ not too small and $0 < R < 1$,* $\Pr(d/n \leq \Delta - \epsilon) \overset{n\to\infty}{\to} 0$
- *For ϵ small enough and $0 < R < 1/2$,* $\Pr(d/n \geq \Delta + \epsilon) \overset{n\to\infty}{\to} 0$

Sketch of proof

- From before with $i = n(\Delta - \epsilon)$ and $\ell = n(\Delta + \epsilon)$ we have

$$\Pr(d/n \leq \Delta - \epsilon) \leq \Pr(\mathcal{D}_i \geq 1)$$
$$\Pr(d/n \geq \Delta + \epsilon) \leq \Pr(\mathcal{D}_{\ell-1} = 0) + \frac{M^2}{2q^{\alpha n^2}}.$$

- Let $f(x) = -x^2 + (\alpha + 1)nx - (1 - 2R)\alpha n^2$, thus $f(n\Delta) = 0$
- We can show that
  - $\Pr(\mathcal{D}_i \geq 1) = \binom{M}{2} \Pr(\mathrm{Rk}(\mathbf{c}_u - \mathbf{c}_v) \leq i) \leq 0.5 q^{f(i)+\sigma(q)}$
  - $\Pr(\mathcal{D}_{\ell-1} = 0) = \left(1 - \frac{\mathcal{B}_{\ell-1}}{q^{\alpha n^2}}\right)^{\binom{M}{2}} \leq \lambda e^{-q^{f(\ell-1)}}$
  - Since $M = q^{\alpha R n^2}$, then $\frac{M^2}{2q^{\alpha n^2}} \leq q^{(2R-1)\alpha n^2}/2$

Outline of the talk

Sampling space

- Parameters : $0 < R < 1$, $\alpha > 0$, $M = q^{\alpha n^2 R}$
- Pick up $\mathbf{G} \xleftarrow{U} \mathbb{F}_{q^{\alpha n}}^{nR \times R}$
- Construct $\mathcal{C} = \{\mathbf{x}_1\mathbf{G}, \ldots, \mathbf{x}_M\mathbf{G}\}$, where
  - $\mathbf{x}_j$ describles $\mathbb{F}_{q^{\alpha n}}^{nR}$
  - $\mathbf{x}_1 = \mathbf{0}$

Therefore, for all $j \in [2..M]$ and all $0 \leq i \leq n$

$$\Pr(\mathrm{Rk}(\mathbf{x}_j\mathbf{G}) \leq i) = \frac{\mathcal{B}_i}{q^{\alpha n^2}} \leq q^{(\alpha+1)ni - i^2 - \alpha n^2 + \sigma(q)},$$

Random variable - (I)

- Definition

$$\mathcal{D}_i = \sum_{j=2}^{M} \mathbf{1}_{\mathrm{Rk}(\mathbf{x}_j\mathbf{G})\leq i}$$

- Upper bound on minimum rank distance
  - $d \leq i \Rightarrow \mathcal{D}_i \geq 1$
  - Therefore $\Pr(d \leq i) \leq \Pr(\mathcal{D}_i \geq 1)$

Random variable (II)

Lower bound on the minimum rank distance

- $d \geq \ell \Rightarrow \mathcal{D}_{\ell-1} = 0$ or $\begin{cases} \mathcal{D}_{\ell-1} \geq 1 \\ \mathbf{x}_u \mathbf{G} = \mathbf{0}, \text{ for some } u \geq 2 \end{cases}$
- Therefore $\Pr(d \geq \ell) \leq \Pr(\mathcal{D}_{\ell-1} = 0) + \Pr(\mathrm{Rk}(\mathbf{G}) < nR)$
- Hence $\Pr(d \geq \ell) \leq \Pr(\mathcal{D}_{\ell-1} = 0) + q^{\alpha n^2 (R-1)}$

Asymptotic equivalent

- Le $\Delta_{GV} = \frac{\alpha+1}{2} - \sqrt{(\alpha-1)^2/4 + \alpha R)}$
- Proposition

Proposition

- *For ϵ not too small,* $\Pr(d/n \leq \Delta_{GV} - \epsilon) \overset{n\to\infty}{\to} 0$
- *For ϵ small enough,* $\Pr(d/n \geq \Delta_{GV} + \epsilon) \overset{n\to\infty}{\to} 0$

Sketch of proof

- From before with $i = n(\Delta - \epsilon)$ and $\ell = n(\Delta + \epsilon)$ we have

$$\Pr(d/n \leq \Delta_{GV} - \epsilon) \leq \Pr(\mathcal{D}_i \geq 1)$$
$$\Pr(d/n \geq \Delta_{GV} + \epsilon) \leq \Pr(\mathcal{D}_{\ell-1} = 0) + q^{\alpha n^2 (R-1)}$$

- Let $g(x) = -x^2 + (\alpha+1)nx - (1-R)\alpha n^2$, thus $g(n\Delta_{GV}) = 0$
- We can show that
  - $\Pr(\mathcal{D}_i \geq 1) = (M-1)\Pr(\mathrm{Rk}(\mathbf{xG}) \leq i) \leq 0.5 q^{g(i)+\sigma(q)}$
  - $\Pr(\mathcal{D}_{\ell-1} = 0) = \left(1 - \frac{\mathcal{B}_{\ell-1}}{q^{\alpha n^2}}\right)^{M-1} \leq \lambda e^{-q^{g(\ell-1)}}$

Conclusion

- Exact asymptotic behaviour of random codes in rank metric
- If $\alpha = 1$, similar to Johnson bound