Thirteenth International Workshop on Algebraic and Combinatorial Coding Theory
June 15-21, 2012, Pomorie, Bulgaria *pp. 240–245*

Asymptotic behaviour of constant rate random codes in rank metric

Pierre Loidreau Pierre.Loidreau@m4x.org
DGA MI and IRMAR, Université de Rennes 1

Abstract. We study the asymptotic behaviour of the minimum rank distance of constant rate random codes and random linear codes. In the case of linear codes, we show that the codes reach GV-bound.

1 Introduction

In [4] was proved an asymptotic equivalent for the minimum rank distance of codes reaching rank metric GV-bound Following the work initiated by Pierce in [5] and Barg and Forney [1] for Hamming metric, we show in this paper that random codes are asymptotically far from reaching GV-bound whereas random linear codes asymptotically reach GV-bound.

In the first part of the paper, we recall some rank metric background. In the second part we establish the asymptotic equivalent of the minimum rank distance of constant rate codes and constant rate linear codes.

2 Background in rank metric

Let q be a power of a prime and let $\mathbf{b} = (\beta_1, \ldots, \beta_n)$ be a basis of $GF(q^m)$ over $GF(q)$. The integer n will denote the length of the code. Rank norm over $GF(q)$ of a an element of $GF(q^m)^n$ is defined by

Definition 1 ([2]). *Let* $\mathbf{x} = (x_1, \ldots, x_n) \in GF(q^m)^n$. *The rank of* $\mathbf{x}$ *on* $GF(q)$, *is the rank of matrix*

$$\mathbf{X} = \begin{pmatrix} x_{11} & \cdots & x_{1n} \\ \vdots & \ddots & \vdots \\ x_{m1} & \cdots & x_{mn} \end{pmatrix},$$

where $x_j = \sum_{i=1}^{n} x_{ij}\beta_i$. *It is denoted by* $Rk(\mathbf{x})$

Rank metric is the metric over $GF(q^m)^n$ induced by the rank norm. spheres and balls in rank metric have the following expression:

- Sphere of radius $t \geq 0$: $\mathcal{S}_t \overset{def}{=} \{\mathbf{y} \in GF(q^m)^n \mid \mathrm{Rk}(\mathbf{y}) = t\}$.
- Ball of radius $t \geq 0$: $\mathcal{B}_t \overset{def}{=} \cup_{i=0}^{t} \mathcal{S}_i$.

We have the following bounds:

$$\left\{ \begin{array}{lcl} q^{(m+n-1)t-t^2} & \leq \mathcal{S}_t \leq & q^{(m+n+1)t-t^2+\sigma(q)} \\ q^{(m+n)t-t^2} & \leq \mathcal{B}_t \leq & q^{(m+n+1)t-t^2+\sigma(q)} \end{array} \right. \tag{2.1}$$

where $\sigma(q) = -\frac{1}{\ln(q)} \sum_{i=1}^{\infty} \ln(1-q^{-i}) \leq 1$.

Let $\mathcal{C} \subset GF(q^m)^n$ for m and n non-zero integers. If M denotes the cardinality of $\mathcal{C}$ and $d \overset{def}{=} \min_{\mathbf{c}_1 \neq \mathbf{c}_2 \in \mathcal{C}}(\mathrm{Rk}(\mathbf{c}_1 - \mathbf{c}_2))$ we say that $\mathcal{C}$ is a $(n, M, d)_r$ code over $GF(q^m)$. The integer d is called the *minimum rank distance* of $\mathcal{C}$.

From [4], we have

Definition 2. *A $(n, M, d)_r$-code reaches GV-bound if*

$$(M-1) \times \mathcal{B}_{d-1} < q^{mn} \leq M \times \mathcal{B}_{d-1}. \tag{2.2}$$

and also the proposition

Proposition 1 (GV-Bound)**.** *Let $\mathcal{F}$ be a family of $(n, M_n = q^{\alpha n^2 R}, d_n)_r$ codes over $GF(q^{\alpha n})$ reaching GV-bound. Then*

$$\lim_{n \to \infty} d_n/n = \frac{\alpha+1}{2} - \sqrt{(\alpha-1)^2/4 + \alpha R}. \tag{2.3}$$

3 Asymptotic behaviour of random codes

The goal of this section is to establish both parts in rank metric for non-linear and linear constant rate random codes. We define the sampling spaces over which we will take the probabilities. We prove that the relative minimum rank distance of general constant rate random linear codes depends on the rate of the codes, the exponent of the extension and is strictly less than GV-bound. For linear codes we show that the relative minimum distance asymptotically corresponds to GV-bound.

3.1 General case

Let $0 < R < 1$, and $\alpha > 0$. A rate R random code $\mathcal{C}$ over $GF(q^{\alpha n})$ is constructed as such:

- pick up randomly $\mathbf{c}_1, \ldots, \mathbf{c}_M$ codewords uniformly and independently in the space of vectors of length n over $GF(q^{\alpha n})$, where $M = q^{\alpha n^2 R}$. Without loss of generalities we suppose that M is an integer ;
- the code $\mathcal{C}$ is $\mathcal{C} = \{\mathbf{c}_1, \ldots, \mathbf{c}_M\}$.

The codewords are not necessarily distinct. Thanks to this construction, the probability that the codeword $\mathbf{c}_j \in \mathcal{C}$ is at rank distance less than i from a vector $\mathbf{y} \in GF(q^{\alpha n})^n$ depends on i only and is equal to:

$$\Pr(\mathrm{Rk}(\mathbf{c}_j - \mathbf{y}) \leq i) = \frac{\mathcal{B}_i}{q^{\alpha n^2}} \leq q^{(m+n)i-i^2-\alpha n^2+\sigma(q)},$$

Now we define the following random variable on $\mathcal{C}$ by:

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

where $\mathbf{1}_{\mathrm{Rk}(\mathbf{c}_u-\mathbf{c}_v)\leq i}$ is this indicator function, that is equal to 1 if $\mathrm{Rk}(\mathbf{c}_u-\mathbf{c}_v) \leq i$ and equal to 0 if $\mathrm{Rk}(\mathbf{c}_u - \mathbf{c}_v) > i$. Thus $\mathcal{D}_i$ counts the number of unordered pairs of codewords at rank distance less or equal to i from each other. Let d be the minimum rank distance of $\mathcal{C}$.

It is clear that

- $d \leq i$ implies $\mathcal{D}_i \geq 1$, that is: there is at least one pair of codewords at rank distance less than i;
- $d \geq i$ implies:
  1. either $\mathcal{D}_{i-1} = 0$: that is, there are no pairs of codewords at distance less than $i - 1$;
  2. or $\mathcal{D}_{i-1} \geq 1$. In that case there is at least one vector appearing twice in the M codewords randomly chosen, that is: there are u and v with $1 \leq u < v \leq M$ such that $\mathbf{c}_u = \mathbf{c}_v$;

Hence, for all $i \geq 1$,

- $\Pr(d \leq i) \leq \Pr(\mathcal{D}_i \geq 1)$,
- $\Pr(d \geq i) \leq \Pr(\mathcal{D}_{i-1} = 0) + \Pr(\exists 1 \leq u < v \leq M \mid \mathbf{c}_u = \mathbf{c}_v)$. From the birthday paradox, we have

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

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

Let $\Delta = \frac{\alpha+1}{2} - \sqrt{(\alpha-1)^2/4 + 2\alpha R}$ we show the following proposition

Proposition 2. *For $0 \leq R < 1$, and for all ϵ such that ϵn grows to $+\infty$ with n, we have $\Pr(d/n \leq \Delta - \epsilon) \overset{n\to\infty}{\to} 0$. Moreover, if ϵ is a constant, the probability decreases exponentially.*

Proof. We have $\Pr(d/n \leq \Delta - \epsilon) = \Pr(d \leq n(\Delta - \epsilon)) \leq \Pr(\mathcal{D}_{n(\Delta-\epsilon)} \geq 1)$. For simplicity let us write $i \overset{def}{=} n(\Delta - \epsilon)$. Since all the codewords in $\mathcal{C}$ are chosen independently, we have

$$\Pr(\mathcal{D}_i \geq 1) = \binom{M}{2} \Pr(\mathrm{Rk}(\mathbf{c}_u - \mathbf{c}_v) \leq i) \leq 0.5 q^{f(i)+\sigma(q)},$$

where $f(x) = -x^2 + (\alpha+1)nx - (1-2R)\alpha n^2$. Then the discriminant of f is equal to $(\alpha-1)^2 n^2 + 8\alpha n^2 R$. That is $n\Delta$ is the smallest root of f. Then for all ϵ, by Taylor formula we have that:

$$f(n(\Delta - \epsilon)) = -((\alpha+1)n - 2n\Delta)n\epsilon - \epsilon^2 n^2.$$

By construction we have $\Delta \leq \frac{\alpha+1}{2}$, therefore

$$f(n(\Delta - \epsilon)) \leq -\epsilon^2 n^2$$

Hence ϵn grows to infinity with n, the quantity $0.5 q^{\sigma(q)} q^{f(n(\Delta-\epsilon))} \leq 0.5 q^{\sigma(q)} q^{-\epsilon^2 n^2}$ vanishes with n. Moreover, if ϵ is constant, then it decreases exponentially towards 0. □

We now prove the converse statement.

Proposition 3. *For $0 \leq R < 1/2$, and for all ϵ constant sufficiently small, we have $\Pr(d/n \geq \Delta + \epsilon) \overset{n\to\infty}{\to} 0$, exponentially fast.*

Proof. We have $\Pr(d/n \geq \Delta + \epsilon) = \Pr(d \geq n(\Delta + \epsilon)) \leq \Pr(\mathcal{D}_{n(\Delta+\epsilon)-1} = 0) + \frac{M^2}{2q^{\alpha n^2}}$. Since $R < 1/2$, and since $M = q^{\alpha R n^2}$ the quantity $\frac{M^2}{2q^{\alpha n^2}}$ decreases exponentially fast when $n \to +\infty$. Therefore it remains to proove that $\Pr(\mathcal{D}_{n(\Delta+\epsilon)-1} = 0)$ also decreases exponentially fast. Let $i \overset{def}{=} n(\Delta + \epsilon)$, then $\mathcal{D}_{i-1} = 0$ if and only if all the codewords in $\mathcal{C}$ are at distance greater than $i - 1$ from each other. Therefore since

$$\Pr(\mathrm{Rk}(\mathbf{c}_u - \mathbf{c}_v) > i - 1) = 1 - \frac{\mathcal{B}_{i-1}}{q^{\alpha n^2}},$$

we have

$$\Pr(\mathcal{D}_{i-1} = 0) = \left(1 - \frac{\mathcal{B}_{i-1}}{q^{\alpha n^2}}\right)^{\binom{M}{2}} = e^{\binom{M}{2}\ln(1 - \frac{\mathcal{B}_{i-1}}{q^{\alpha n^2}})} \tag{3.4}$$

Now since $\forall 0 \leq x \leq 1 \ \ln(1-x) \leq -x$, we have

$$\Pr(\mathcal{D}_{i-1} = 0) \leq \lambda e^{-M^2 \frac{\mathcal{B}_{i-1}}{q^{\alpha n^2}}} \leq \lambda e^{-q^{f(i-1)}},$$

where λ is the constant $e^{-0.5}$, and $f(x) = -x^2 + (\alpha+1)nx - (1-2R)\alpha n^2$. The function f is the same function as in the proof of proposition 2. Therefore the smallest root of f is equal to $n\Delta$ and by Taylor formula

$$f(i-1) = f(n(\Delta+\epsilon)-1) = ((\alpha+1)-2\Delta)(n^2\epsilon - n) - (n\epsilon - 1)^2.$$

Since $(\alpha+1) - 2\Delta > 0$, by construction, for ϵ constant sufficiently small ($< (\alpha+1) - 2\Delta$) the quantity $f(i-1)$ increases quadratically in n. Therefore $\Pr(\mathcal{D}_{i-1} = 0)$ decreases exponentially fast. □

3.2 Linear codes

Let $0 < R < 1$, and $\alpha > 0$. A rate R random code $\mathcal{C}$ over $GF(q^{\alpha n})$ is:

- label the vector space $\{\mathbf{x}_1, \ldots, \mathbf{x}_{q^{\alpha n^2 R}}\} = GF(q^{\alpha n})^{nR}$, and where $\mathbf{x}_1 = \mathbf{0}$. We suppose without loss of generalities that nR is an integer ;
- choose randomly and uniformly a matrix $nR \times R$ with coefficients in $GF(q^{\alpha n})$ denoted by $\mathbf{G}$;
- set $\mathcal{C} = \{\mathbf{x}_1\mathbf{G}, \ldots, \mathbf{x}_{q^{\alpha n^2 R}}\mathbf{G}\}$.

Let $j > 1$. The probability that the codeword $\mathbf{x}_j \in \mathcal{C}$ has rank less than i is

$$\Pr(\mathrm{Rk}(\mathbf{x}_j\mathbf{G}) \leq i) = \frac{\mathcal{B}_{i-1}}{q^{\alpha n^2}}.$$

Now we define the following random variable on $\mathcal{C}$:

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

Let d be the random variable giving the minimum rank distance of $\mathcal{C}$. We have:

- $d \leq i$ implies $\mathcal{D}_i \geq 1$, that is there is at least one $j > 2$ such that $\mathbf{x}_j\mathbf{G}$ has rank less or equal to i ;
- $d \geq i$ implies:
  1. either $\mathcal{D}_{i-1} = 0$. In our case this is equivalent to the fact that $\mathbf{G}$ has rank nR ;
  2. or $\mathcal{D}_{i-1} \geq 1$. But this implies that there is at least one $j > 2$ such that $\mathbf{x}_j\mathbf{G} = \mathbf{0}$. Since $\mathbf{x}_j \neq 0$, this implies that $\mathbf{G}$ has rank $< nR$.

Therefore, for all $i \geq 1$,

- $\Pr(d \leq i) \leq \Pr(\mathcal{D}_i \geq 1)$,
- $\Pr(d \geq i) \leq \Pr(\mathcal{D}_{i-1} = 0) + \Pr(\mathrm{Rk}(\mathbf{G}) < nR)$.

Recall that GV-bound satisfies $\Delta_{GV} = \frac{\alpha+1}{2} - \sqrt{(\alpha-1)^2/4 + \alpha R}$. With these properties and by using similar arguments as in previous section, we can show the following two propositions.

Proposition 4. *For $0 \leq R < 1$, and for all ϵ such that ϵn grows to ∞ with n, we have $\Pr(d/n \leq \Delta_{GV} - \epsilon) \overset{n\to\infty}{\to} 0$. Moreover, if ϵ is a constant, the probability decreases exponentially.*

For the other bound, we have a similar result.

Proposition 5. *For $0 \leq R < 1$, and for all ϵ constant sufficiently small, we have $\Pr(d/n \geq \Delta_{GV} + \epsilon) \overset{n\to\infty}{\to} 0$, exponentially fast.*

References

[1] A. Barg and G. . Forney, Jr Random codes: minimum distances and error exponents *IEEE Transactions on Information Theory*, 48(9):2568-2573, November 2002.

[2] E. M. Gabidulin. Theory of codes with maximal rank distance. *Problems of Information Transmission*, 21:1–12, July 1985.

[3] E. M. Gabidulin. A fast matrix decoding algorithm for rank-error correcting codes. In G. Cohen, S. Litsyn, A. Lobstein, and G. Zémor, editors, *Algebraic coding*, volume 573 of *LNCS*, pages 126–133. Springer-Verlag, 1991.

[4] P. Loidreau. Properties of codes in rank metric. In *Eleventh International Workshop on Algebraic and Combinatorial Coding Theory - ACCT 2008*, Pamporovo, 2008.

[5] J. N. Pierce. Limit distribution of the minimum distance of random linear codes. *IEEE Transactions on Information Theory*, 13(4):595–599, October 1967.