# Asymptotic behaviour of codes in rank metric over finite fields

P Loidreau

# Asymptotic behaviour of codes in rank metric over finite fields

P. Loidreau*
DGA MI et Université de Rennes 1

**Abstract**

In this paper, we first recall some basic facts about rank metric. We then derive an asymptotic equivalent of the minimum rank distance of codes that reach the rank metric Gilbert–Varshamov bound. We then derive an asymptotic equivalent of the average minimum rank distance of random codes. We show that random codes reach GV bound. Finally, we show that optimal codes in rank metric have a packing density which is bounded by functions depending only on the base field and the minimum distance and show the potential interest in cryptographic applications.

## 1 Introduction

### 1.1 Goal of the paper

Rank metric in the field of combinatorial coding theory appeared in the 70's in an article by P. Delsarte [8], and in the field of algebraic coding in papers by E. M. Gabidulin available in Russian, later summarized in English in [11].

In this seminal paper, E. M. Gabidulin designed a family of optimal codes (reaching the Singleton bound for rank metric), as well as a polynomial-time algorithm decoding up to their error-correcting capability. Later, R. M. Roth showed in an article that these so-called Gabidulin codes were also optimal, as generalizations of the Patel-Hong codes, [4] in the field of criss-cross errors or erasures correction. In this model, errors or erasures occurred along lines or columns of arrays. This model was suitable for modelizing the storage of information on magnetic tapes or on chipsets, [31].

Since then, rank metric codes and especially codes derived from Gabidulin codes have found numerous applications in the field of coding theory: they form the heart of the design of almost optimal codes with efficient decoding algorithms in the field of random network coding, [20, 32], as well as in the design of space-time codes with optimal rate/diversity trade-off [23, 19].

The research domain where properties of rank metric have to be investigated at length is without doubt the field of cryptology. The idea of using rank metric in the design of code-based public key cryptosystems was first introduced by E. M. Gabidulin, A. V. Paramonov and O. V. Tretjakov in 1991 [13]. Its efficiency was based on the fact that the state of the art decoding algorithm for random codes have a much higher complexity in rank metric than in Hamming metric for the same sets of parameters, [25, 5, 6, 27]. Therefore, since the strength of the system relies on the complexity of the decoding in the public code without any further

*Pierre.Loidreau@univ-rennes1.fr

information, it enables to design cryptosystems with a much smaller public-key size. Hence one of the major drawbacks of McEliece type systems vanishes [25].

Whereas very little improvement has been made concerning the decoding of random codes in rank metric, many successful attacks were operated on the structure of the public code itself which was not sufficiently masked, [17, 18, 28]. Many modifications of the cryptosystems were made to prevent these attacks, but they all require a significant increase of the public-key size to prevent the most powerful attacks, as well as the construction of a new non-optimal rank metric codes, [12, 26, 21].

Since, in rank metric there are already at hand optimal codes for Singleton equality, one can wonder what is the interest in considering other possible families of codes, and in studying the behaviour of random codes in rank metric. We can find good reasons both from a coding theory point of view as well as from a cryptographic point of view:

- From a coding theory point of view, one might wish to use not necessarily optimal codes in rank metric. Namely, it might happen that what effectively counts is the complexity of decoding. We cannot exclude to find a family of non-optimal codes with a better complexity decoder as the family of Gabidulin codes, even find codes with efficient iterative decoding algorithms. Moreover, in the field of space-time coding, maximizing the rank is only one criterium to evaluate the performance of such codes [33]. Therefore, considering also non-optimal codes in the design of space-time codes might also be of interest, for an efficiency trade-off between the two criteria.

- From a cryptographic point of view it is clear that no optimal code can be used in the design of public-key primitives. These code have to be distorted, that is modified so that they look like random, [26, 30, 21].

Then there is a natural question that arises when one construct new families of code. Are they good ? One tool of measurement is to compare their behaviour to the behaviour of random codes.

The goal of the paper is dual. In the second and third section, we gather some already known results about rank metric which are scattered in the different papers cited in the references. We recall the upper and lower bounds on the sizes of spheres and balls in rank metric which can be found in many papers, as well as some classical bound in coding theory (Hamming bound, GV-like bound). We also provide a simple alternate proof to Babu's result that no perfect codes exist in rank metric, [1].

The main goal of this paper is to study the asymptotic behaviour of random codes, and to show that they

In the second and third section we establish some basic facts concerning rank metric and codes in rank metric. We reestablish upper and lower bounds on the sizes of spheres and balls, and define the main bounds. Then, we give a simple alternate proof that no perfect codes exist in rank metric. The original proof can be found in [1].

In the fourth section, we are interested by an asymptotic equivalent of the relative minimum rank distance of constant rate codes, which are closest to GV-bound. Note that in [14], the authors gave an asymptotic equivalent on the lower bound on the rate of codes having a given relative minimum rank distance. Although both results have similarities, they cannot be derived directly from one another since we are dealing with asymptotics. Therefore the purpose of the section is to properly establish the proof of the result.

The fifth section is dedicated to establish the behaviour of so-called random codes. We establish for random constant rate codes and random constant rate additive codes an asymtotic equivalent of the minimum rank distance.

One could argue that it suffices to directly use the results in [3] paper about Hamming metric. This is partly true but their paper provides only a lower bound for the minimum rank distance. Therefore, we also have to establish an upper bound. For Hamming metric, this was done by Pierce for linear codes in [29], although the proofs suppose in some sense that the choice of codewords is independent, which is not the case in Pierce's sampling space. For the definition of the sampling space we prefer to refer to Richardson and Urbanke's [**?**]

Our results show similar results to the case of Hamming metric.

additive codes have a much better minimum rank distance than random codes. Comparatively to Barg and Forney's paper, our results are more accurrate, since the result that they obtaine is . We prefered to follow the approach of Pierce's paper [29], by correcting the

This theorem shows that random constant rate $GF(q)$-ary codes reach asymptotically GV-bound.

Some of the proofs which are very technical are given in appendix

The fourth section is dedicated to establishing the asymptotic behaviour of constant rate codes reaching GV-bound. The fifth section establishes the proof of theorem **??**. This theorem shows that random constant rate $GF(q)$-ary codes reach asymptotically GV-bound. In the sixth section, we study the packing density of optimal codes in rank metric and show they could be interesting in the design of rank-metric based signature schemes.

## 2 Background in rank metric

In the rest of the paper the code alphabet is the finite field $GF(q^m)$ with $q^m$ elements where $q$ is the power of some prime. Let $\mathbf{b} = (\beta_1, \ldots, \beta_m)$ be a basis of $GF(q^m)$ over $GF(q)$. The integer $n$ is as usual the length of the code. Thus vectors of the ambient space $GF(q^m)^n$ are indifferently considered as vectors with components in $GF(q^m)$ or as $m \times n$ $q$-ary matrices obtained by projecting the elements of $GF(q^m)$ on $GF(q)$ with respect to the basis $\mathbf{b}$.

The rank norm of a vector $\mathbf{x}$ in $GF(q^m)^n$ is defined by

**Definition 1 ([11])**
*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 $Rk(\mathbf{x}|GF(q))$, or by $Rk(\mathbf{x})$ when there is no ambiguity on the base field.*

Rank metric is the metric over $GF(q^m)^n$ induced by the rank norm. Given a vector $\mathbf{x} \in GF(q^m)^n$ spheres and balls in rank metric have the following expression:

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

Since rank metric is invariant by translation of vectors, the volumes of spheres and balls do not depend on the chosen center. Therefore to simplify notations, we define:

- $\mathcal{S}_t \stackrel{def}{=}$ volume of sphere of radius $t$ in $GF(q^m)$. It is equal to the number of $m \times n$ $q$-ary matrices of rank $= t$. If $t = 0$ then $\mathcal{S}_0 = 1$ and for $t = 1, \ldots, \min(n, m)$ it is equal (see for example [2]) to
$$\mathcal{S}_t = \prod_{j=0}^{t-1} \frac{(q^n - q^j)(q^m - q^j)}{q^t - q^j}. \tag{2.1}$$

- $\mathcal{B}_t \stackrel{def}{=}$ volume of ball of radius $t$ in $GF(q^m)$. It is equal to the number of $m \times n$ matrices of rank $\leq t$ in $GF(q)$. Therefore
$$\forall t = 0, \ldots, \min(n, m), \quad \mathcal{B}_t = \sum_{i=0}^{t} \mathcal{S}_i. \tag{2.2}$$

A code $\mathcal{C}$ of length $n$ and of size $M$ over $GF(q^m)$ is a set of $M$ vectors of length $n$ over $GF(q^m)$. Its minimum rank distance is defined by

**Definition 2**
*Let $\mathcal{C}$ be a code over $GF(q^m)$, then $d \stackrel{def}{=} \min_{\mathbf{c}_1 \neq \mathbf{c}_2 \in \mathcal{C}}(Rk(\mathbf{c}_1 - \mathbf{c}_2))$ is called* minimum rank distance *of $\mathcal{C}$.*

If the code is $GF(q)$-linear (it is most often the case when considered as a matricial code) or even linear and since rank metric is invariant by translation, the *minimum rank distance* of the code is
$$d = \min_{\mathbf{c} \neq \mathbf{0} \in \mathcal{C}} (\mathrm{Rk}(\mathbf{c})). \tag{2.3}$$
If $d$ is the minimum rank distance of $\mathcal{C}$ we will say that $\mathcal{C}$ is a $(n, M, d)_r$-code. Moreover if the code is linear of dimension $k$ we will say that it is a $[n, k, d]_r$-code. The value $R = \log_{q^m}(M)/n$ is as usual the rate of the code, and corresponds to $k/n$ in the linear case.

The quantities (2.1) and (2.2) are not very easy to handle in computation. We derive bounds sufficiently accurate enough for our needs.

**Proposition 1**
*For all $t = 0, \ldots, \min(n, m)$, we have*
$$\begin{cases} q^{(m+n-1)t-t^2} & \leq \mathcal{S}_t \leq \quad q^{(m+n)t-t^2+\sigma(q)}, \\ q^{(m+n)t-t^2} & \leq \mathcal{B}_t \leq \quad q^{(m+n)t-t^2+\sigma(q)}, \end{cases} \tag{2.4}$$
*where $\sigma(q) = -\frac{1}{\ln(q)} \sum_{i=1}^{\infty} \ln(1 - q^{-i})$.*

Proof.
The proof for the upper bound on $\mathcal{B}_t$ can be found in in [15], Lemma 9. It gives also the upper bound for $\mathcal{S}_t$. The proof for the lower bound on $\mathcal{B}_t$ can be found in [16], Lemma 5. It remains to proove the lower bound on $\mathcal{S}_t$. Formula (2.1) can be rewritten under the form
$$\mathcal{S}_t = q^{(m+n)t-t^2} \prod_{j=0}^{t-1} \frac{(1 - q^{j-n})(1 - q^{j-m})}{1 - q^{j-t}}.$$

Since $t \leq m$, then for all $j = 0, \ldots, t-1$ we have $1 - q^{j-m} \geq 1 - q^{j-t}$. Therefore $(1 - q^{j-m})/(1-q^{j-t}) \geq 1$, and since $1-q^{j-n}$ is a decreasing function of $j$ and positive if $j-n \geq 1$, which is the case by hypothesis, we have $1 - q^{j-n} \geq 1 - 1/q = (q-1)/q$. Since $q \geq 2$ we deduce that $1 - q^{j-n} \geq q^{-1}$. Therefore, for all $j = 0, \ldots, t-1$

$$\frac{(1-q^{j-n})(1-q^{j-m})}{1-q^{j-t}} \geq q^{-1}.$$

Thus

$$\prod_{j=0}^{t-1} \frac{(1-q^{j-n})(1-q^{j-m})}{1-q^{j-t}} \geq q^{-t}.$$

This gives the lower bound on $\mathcal{S}_t$.

■

# 3 Upper bounds and perfect codes

In this section, we make a summary of known results on bounds for codes in rank metric, like Singleton-like bound and Hamming-like bound. Moreover a straightforward corollary of previous section is a new very simple proof of a known result given in [1]: there are no perfect codes in rank metric.

**Theorem 1**

*Let $\mathcal{C}$ be a $(n, M, d)_r$ code over $GF(q^m)$. We have*

- Singleton-like bound: $M \leq q^{\min(m(n-d+1), n(m-d+1))}$.
- Hamming-like bound: *If $t = \lfloor (d-1)/2 \rfloor$, then*

$$M\mathcal{B}_t \leq q^{mn}. \tag{3.5}$$

For the proof of Singleton-like bound, see for instance [11, 26]. The proof of the Hamming-like bound comes from the fact that, for rank metric, two balls of radius $t = \lfloor (d-1)/2 \rfloor$ centered on codewords do not intersect. Thus, the full packing has size less than the whole space, see [14].

The so-called perfect codes are codes reaching the Hamming-liked bound. It is well known that in Hamming metric the only perfect linear codes are repetition codes, Hamming codes over any finite fields and the binary and ternary Golay codes [24], page 179-180. What then of the existence of perfect codes in rank metric ? The following proposition answers the question

**Proposition 2 ([1])** *There are no perfect codes in rank metric.*

PROOF. Suppose on the contrary that a perfect code does exist with parameters $(n, M, d)_r$ over $GF(q^m)$, that is suppose that

$$M\mathcal{B}_t = q^{mn}.$$

Without loss of generality we can assume that $n \leq m$ (Else consider the transposed code). The right part of the inequality (2.4) on the volume of balls implies that

$$Mq^{(m+n+1)t-t^2+1} \geq q^{mn}.$$

Moreover, from Singleton bound we have $M \leq q^{m(n-d+1)}$. Since $t = \lfloor (d-1)/2 \rfloor$ this implies that $M \leq q^{m(n-2t)}$. Therefore

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

By taking the base $q$ logarithm of the inequality and by reordering the terms, we obtain

$$(n-m)t \geq t^2 - t + 1.$$

By hypothesis $n - m \leq 0$ and $t > 0$. Therefore we must have $t^2 - t - 1 \leq 0$. Since $t$ is integer the only possibility is $t = 1$ and accordingly $n = m$. In that case however the formula that parameters have to satisfy is $M \times \mathcal{B}_1 = q^{n^2}$. Hence

$$\underbrace{q^{n(n-2)}}_{\text{Singleton}} \frac{q^{2n} - 2q^n + q}{q-1} \geq M \underbrace{\frac{q^{2n} - 2q^n + 1}{q-1} + 1}_{\mathcal{B}_1} = q^{n^2},$$

which implies

$$1 - \frac{2}{q^n} + \frac{1}{q^{2n-1}} \geq q - 1. \tag{3.6}$$

This inequality cannot be satisfied for $q \geq 2$.
■

# 4 A Varshamov–Gilbert like bound

Until now we have obtained bounds and results on the non-existence of codes in rank metric with given parameters. What then of the existence of codes ? In Hamming metric there is the so-called Varshamov-Gilbert (GV) bound which gives information on the existence of codes with parameters $(n, M, d)$. In rank metric we have the exact equivalent.

**Proposition 3 ([14])**
*Let $m, n, M, d$ be positive integers. If*

$$M \times \mathcal{B}_{d-1} < q^{mn}, \tag{4.7}$$

*then there exists a $(n, M+1, d)_r$-code over $GF(q^m)$.*

In Hamming metric, an asymptotic version of GV bound provides a lower bound on the maximum rate of codes with relative minimum Hamming distance $\delta$, [24, 22]. This lower bound is given by

$$1 - H_q(\delta),$$

for $0 \leq \delta \leq (q-1)/q$.

An analogous of this bound asymptotic version for rank metric was given in [14]. The authors showed a lower bound

$$(1-\delta)(1-\alpha), \tag{4.8}$$

provided $\alpha \stackrel{def}{=} m/n$ is constant.

However for cryptographic motivation and benchmarking, we are more interested in the inverse function, that is the behaviour of the relative minimum distance as a function of the

rate of the code. This enables to show that randomly chosen codes are with high probability on GV-bound in the same manner as it was proven in J. Pierce's paper [29] for randomly chosen codes in Hamming metric.

Before doing some asymptotic, we need to define what does it mean for a code to reach GV-bound given a minimum rank distance $d$. Roughly speaking, it is a code optimal in the sense that you cannot pack the space with balls of radius $d-1$ around the codewords if you remove only one codeword.

**Definition 3**

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

$$(M-1) \times \mathcal{B}_{d-1} < q^{mn} \leq M \times \mathcal{B}_{d-1}. \tag{4.9}$$

Now we are interested in the following problem : suppose that we have an infinite family of codes of parameters $(n, M_n, d_n)$ over $GF(q^{m_n})$ reaching GV-bound. The following proposition gives relations between the fundamental parameters of the codes for the so-called constant rate codes over a field extension $GF(q^{m_n=\alpha n})$ :

**Proposition 4**

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

$$\lim_{n\to\infty} d_n/n = \frac{\alpha+1}{2} - \sqrt{(\alpha-1)^2/4 + \alpha R}. \tag{4.10}$$

In particular, if $\alpha = 1$, then the limit of the ratio is $1-\sqrt{R}$ which is similar to the Johnson bound for Gabidulin codes, which gives the maximum radius for which a ball centered on some vector of the ambient space contains on average a number of codewords that is polynomial in the length of the code, see [10].

PROOF.

By taking the base $q$ logarithm of (4.9) and by using the inequalities (2.4), for any $(n, M_n = q^{\alpha n^2 R}, d_n)$-code over $q^{\alpha n}$ reaching GV-bound, we have:

$$\begin{cases} \alpha n^2 \leq (\alpha+1)n(d_n-1) - (d_n-1)^2 + \sigma(q) + \log_q M_n, \\ \log_q(M_n-1) + ((\alpha+1)n)(d_n-1) - (d_n-1)^2 < \alpha n^2. \end{cases}$$

Since $M_n \geq 2$ we have further that $\log_q(M_n-1) \geq \log_q M_n - \log_q(2) \geq \log_q M_n - 1$. Hence by replacing $\log_q M_n$ by $\alpha n^2 R$ we have

$$\begin{cases} 0 \leq -d_n^2 + ((\alpha+1)n+2)d_n + \alpha n^2 R - \alpha n^2 - ((\alpha+1)n - \sigma(q) - 1), \\ 0 \geq -d_n^2 + ((\alpha+1)n+2)d_n + \alpha n^2 R - \alpha n^2 - ((\alpha_n+1)n + 1). \end{cases}$$

Both inequations imply that $d_n$ lies in two

In particular by the basic properties of second order inequalities, $d_n$ has to be greater than the smallest root of the first polynomial in $d_n$ and smaller than the smallest root of the second polynomial in $d_n$. This formally leads to

$$\frac{\alpha+1}{2} - \frac{\sqrt{\Delta_1}}{2n} + \frac{1}{n} \leq \frac{d_n}{n} \leq \frac{\alpha+1}{2} - \frac{\sqrt{\Delta_2}}{2n} + \frac{1}{n}, \tag{4.11}$$

where the discriminants $\Delta_1$ and $\Delta_2$ satisfy:

$$\Delta_1 = (\alpha-1)^2 n^2 + 4\alpha n^2 R + O(n),$$
$$\Delta_2 = (\alpha-1)^2 n^2 + 4\alpha n^2 R + O(n).$$

By considering the square root of the discriminants and by dividing by $2n$, we obtain:

$$\frac{\sqrt{\Delta_1}}{2n} = \sqrt{(\alpha-1)^2/4 + \alpha R + O(1/n)} = \sqrt{(\alpha-1)^2/4 + \alpha R} + O(1/n),$$
$$\frac{\sqrt{\Delta_2}}{2n} = \sqrt{(\alpha-1)^2/4 + \alpha R + O(1/n)} = \sqrt{(\alpha-1)^2/4 + \alpha R} + O(1/n).$$

By replacing the value of the discriminants in (4.11), and since we obtain

$$\frac{\alpha+1}{2} - \sqrt{(\alpha-1)^2/4 + \alpha R} + O(1/n) \leq \frac{d_n}{n} \leq \frac{\alpha+1}{2} - \sqrt{(\alpha-1)^2/4 + \alpha R} + O(1/n).$$

Therefore

$$\frac{d_n}{n} = \frac{\alpha+1}{2} - \sqrt{(\alpha-1)^2/4 + \alpha R} + O(1/n),$$

which gives the result (4.10).
■

**Definition 4** *A family of constant rate codes satisfying proposition* 4 *is said to reach GV-bound.*

# 5 Random codes

In cryptography, random codes provide benchmarks for cryptosystems. Namely, in McEliece type cryptosystems, security proofs imply that the family of codes that is used is indistinguishable of random codes [7]. In rank metric based cryptography, the fact that many variant using Gabidulin codes are weak could be interpreted in the sense that all these families can be easily distinguished from random codes. Therefore investigating the behaviour of random codes could provide arguments to evaluate the security of rank-metric based cryptosystem.

In Hamming metric the paper [29] shows that random codes in Hamming metric reach GV-bound. In this section we proove an analoguous proposition for rank metric.

## 5.1 General case

We will consider a code with cardinality $M = q^{\alpha n^2 R}$ over the finite field $GF(q^{\alpha n})$. We construct a code $\mathcal{C}$ of cardinality $M$ from the random code ensemble as defined in [**?**], that is, we choose randomly $\mathbf{c}_1, \ldots, \mathbf{c}_M$ codewords by sampling uniformly and independently in the space of vectors of length $n$ over $GF(q^{\alpha n})$. Note that the codewords are not necessarily distinct. Thanks to this construction, the probability that a codeword is at rank distance from any vector of $\mathbf{y} \in GF(q^{\alpha n})^n$ depends on $i$ only and is equal to:

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

Now we define the following indicator function:

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

This function counts the number of unordered pairs of codewords at rank distance less than $i$ from each other. Let $d$ be the minimum rank distance of the code $\mathcal{C}$. 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 $\mathcal{D}_{i-1} = 0$, that is, there are no pairs of codewords at distance less than $i-1$

Hence we obtain for all $i \geq 1$,

- $\Pr(d \leq i) \leq \Pr(\mathcal{D}_i \geq 1)$,
- $\Pr(d \geq i) \leq \Pr(\mathcal{D}_{i-1} = 0)$,

Now since $\mathcal{D}_i$ is a sum of indicator function, since $E(\mathbb{1}_{\mathrm{Rk}(\mathbf{c}_u - \mathbf{c}_v)}) = \Pr(\mathrm{Rk}(\mathbf{c}_u - \mathbf{c}_\mathbf{v}) \leq i)$ and since all the codewords are chosen inependently from one another, we have that

$$E(\mathcal{D}_i) = \binom{M}{2} \frac{\mathcal{B}_i}{q^{\alpha n^2}} \leq 0.5 q^{-i^2 + (\alpha+1)ni - (1-2R)\alpha n^2 \alpha \sigma(q)}$$

Hence we have

$$\Pr(d \leq i) \leq \Pr(\mathcal{D}_i \geq 1) = E(\mathcal{D}_i) \leq 0.5 q^{-i^2 + (\alpha+1)ni - (1-2R)\alpha n^2 + \sigma(q)} \tag{5.12}$$

Now let $\Delta_{GV} = \frac{\alpha+1}{2} - \sqrt{(\alpha-1)^2/4 + 2\alpha R}$ we show the following proposition

**Proposition 5** *For $0 \leq R < 1/2$, and for all $\epsilon$ such that $\epsilon n$ tends to $\infty$ with $n$, we have $Pr(d/n \leq \Delta_{GV} - \epsilon) \overset{n \to \infty}{\to} 0$. Moreover, if $\epsilon$ is a constant, this quantity decreases exponentially.*

Proof. Let $f(i) = -i^2 + (\alpha+1)ni - (1-2R)\alpha n^2$. Then the discriminant of $f$ is equal to $(\alpha-1)^2 n^2 + 8\alpha n^2 R$. That is $n\Delta_{GV}$ is the smallest root of $f$. Then for all $\epsilon$, by Taylor formula we have that:

$$f(n(\Delta_{GV} - \epsilon)) = ((\alpha+1)n - 2n\Delta_{GV})n\epsilon - \epsilon^2 n^2$$

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

$$f(n(\Delta_{GV} - \epsilon)) \leq -\epsilon^2 n^2$$

Therefore if $\epsilon n$ tends to infinity with $n$, the quantity $0.5 q^{\sigma(q)} q^{f(n(\Delta_{GV} - \epsilon))}$ tends to 0 with $n$. Moreover, if $\epsilon$ is constant, then it decreases exponentially towards 0.

Now we have proven that the minimum rank distance of code extracted from a random code ensemble cannot be much smaller than $\Delta_{GV}$. We followed a similar approach as in the paper by Barg and Forney. What remains to proove and which is absent from this paper is the fact that the minimum rank distance cannot be much greater than

Now we want to have an upper bound on $\Pr(\mathcal{D}_{i-1} = 0)$. Since $\mathcal{D}_{i-1}$ is the sum of indicator functions of independent events, it is not difficult to see that the event $\mathcal{D}_{i-1}$ corresponds to the intersection of all events $\mathrm{Rk}(\mathbf{c}_u - \mathbf{c}_\mathbf{v}) \geq i$, for all $1 \leq u \leq v \leq M$. Therefore,

$$\Pr(\mathcal{D}_{i-1} = 0) = \left(1 - \frac{\mathcal{B}_{i-1}}{q^{\alpha n^2}}\right)^{\binom{M}{2}}, \tag{5.13}$$

### 5.2 Additive code case

Now our random model is different.

Before prooving the theorem, we first need to have an expression for the probability distribution of the minimum distance for a random $GF(q)$-linear code $\mathcal{C}$ of length $n$ with cardinality $M$ over $GF(q^m)$. Let us define

$$\forall i = 1, \ldots, n, \quad \left\{ \begin{array}{l} \mathcal{A}_i = |\{\mathbf{c} \in \mathcal{C} \mid \mathrm{Rk}(\mathbf{c}) = i\}|, \\ \mathcal{D}_i = |\cup_{t=1}^{i} \mathcal{A}_i| = |\{\mathbf{c} \in \mathcal{C} \setminus \{\mathbf{0}\}, \mid \mathrm{Rk}(\mathbf{c}) \leq i\}|. \end{array} \right.$$

If $d$ is the minimum rank distance of $\mathcal{C}$ we have

$$\forall i = 1, \ldots, n, \quad p_i \stackrel{def}{=} \Pr(d = i) = \Pr(\mathcal{D}_{i-1} = 0, \ \mathcal{D}_i \geq 1).$$

Since

$$\mathcal{D}_i = \sum_{\mathbf{c} \in \mathcal{C} \setminus \{\mathbf{0}\}} \mathbf{1}_{\mathrm{Rk}(\mathbf{c}) \leq i},$$

and $\mathcal{C}$ is a uniformly chosen vector-space over $GF(q)$, we have

$$\Pr(\mathrm{Rk}(\mathbf{c}) = i \mid \mathbf{c} \in \mathcal{C}) = \Pr(\mathrm{Rk}(\mathbf{c}) = i) = \mathcal{B}_i / q^{mn}.$$

Therefore

$$\Pr(\mathcal{D}_{i-1} = 0) = \Pr(\forall \mathbf{c} \in \mathcal{C} \setminus \{\mathbf{0}\}, \mathrm{Rk}(\mathbf{c}) \geq i) = \left(1 - \frac{\mathcal{B}_{i-1}}{q^{mn}}\right)^{M-1}, \tag{5.14}$$

and

$$\Pr(\mathcal{D}_i \geq 1 \mid \mathcal{D}_{i-1} = 0) = 1 - \left(1 - \frac{\mathcal{S}_i}{q^{mn} - \mathcal{B}_{i-1}}\right)^{M-1}. \tag{5.15}$$

From the previous paragraphs, by multiplying (5.14) by (5.15) and since $\mathcal{B}_i = \mathcal{B}_{i-1} + \mathcal{S}_i$, we have prooved

**Proposition 6**

*Let $\mathcal{C}$ be a $(n, M, d)_r$ random $GF(q)$-linear code over $GF(q^m)$. Let*

$$\forall i = 1, \ldots, n, \ p_i \stackrel{def}{=} \Pr(d = i).$$

*Then we have*

$$\forall i = 1, \ldots, n, \quad p_i = \left(1 - \frac{\mathcal{B}_{i-1}}{q^{mn}}\right)^{M-1} - \left(1 - \frac{\mathcal{B}_i}{q^{mn}}\right)^{M-1}, \tag{5.16}$$

*where $\mathcal{B}_i$ is the volume of the ball of rank radius $i$ in $GF(q^m)^n$.*

We use (5.16) and the fact that for any positive integer $N$,

$$\forall a \geq b \geq 0, \ a^N - b^N = (a-b) \sum_{j=0}^{N-1} a^j b^{N-1-j} \leq N(a-b) \left(\max(a,b)\right)^{N-1}.$$

By taking $a$ and $b$ such that $a = \left(1 - \frac{\mathcal{B}_{i-1}}{q^{mn}}\right) > b = \left(1 - \frac{\mathcal{B}_i}{q^{mn}}\right)$, we deduce

$$p_i \leq \frac{(M-1)\mathcal{S}_i}{q^{mn}} \left(1 - \frac{\mathcal{B}_{i-1}}{q^{mn}}\right)^{M-2}. \tag{5.17}$$

The following lemma is a ground stone for prooving theorem **??**. It shows that all the contribution to the minimum rank distance of a random $GF(q)$-linear reaches GV-bound.

**Lemma 1**

*Let $\mathcal{F}$ be a family of $(n, q^{\alpha n^2 R}, d_n)_r$ random $GF(q)$-linear codes over $GF(q^{\alpha n})$. Let*

$$\forall i = 1, \ldots, n,\ p_i^{(n)} \stackrel{def}{=} \Pr(d_n = i),$$

- *If $1 \leq i/n \leq \frac{\alpha+1}{2} - \sqrt{\frac{(\alpha-1)^2}{4} + \alpha R + \frac{1}{n}}$, then on can find a positive constant $C_1$ such that*
$$p_i^{(n)} \leq C_1 q^{-n}. \tag{5.18}$$
- *If $n \geq i/n \geq \frac{\alpha+1}{2} - \sqrt{\frac{(\alpha-1)^2}{4} + \alpha R - \frac{1}{n}}$, and if $n$ is large enough, then there is a positive constant $C_1'$ such that*
$$p_i^{(n)} \leq q^{-C_1' n}. \tag{5.19}$$

Proof.

Since $M = q^{\alpha n^2 R}$, and since $q \geq 2$ we have that

$$\alpha n^2 R > \log_q(M-1) \geq \alpha n^2 R - 1. \tag{5.20}$$

To prove the lemma, we upper-bound $p_i^{(n)}$ by upper-bounding the inequality (5.17).

- From (2.4) and (5.20) we have
$$p_i^{(n)} \leq \frac{(M-1)\mathcal{S}_i}{q^{\alpha^2}} \underbrace{\left(1 - \frac{\mathcal{B}_{i-1}}{q^{\alpha n^2}}\right)^{M-2}}_{<1} \leq \frac{(M-1)\mathcal{S}_i}{q^{\alpha n^2}} \leq q^{(\alpha+1)ni - i^2 - \alpha n^2(1-R) + \sigma(q)}.$$

  The right part of the inequality is smaller than $q^{-\lambda(n)}$ for some function $\lambda(n)$ if and only if $-i^2 + (\alpha+1)ni - \alpha n^2(1-R) + \sigma(q) + \lambda(n) \leq 0$. The discriminant of this second order inequality is equal to

$$\Delta = (\alpha-1)n^2 + 4\alpha n^2 R + 4\lambda(n) + 4\sigma(q).$$

  The smallest root of the second order equation is thus given by

$$\frac{(\alpha+1)n}{2} - \sqrt{\frac{(\alpha-1)n^2}{4} + \alpha n^2 R + \lambda(n) + \sigma(q)},$$

  Therefore, by taking $\lambda(n) = n - \sigma(q)$ we obtain: if

$$i/n \leq \frac{\alpha+1}{2} - \sqrt{\frac{(\alpha+1)^2}{4} + \alpha R + \frac{1}{n}},$$

  Then

$$p_i^{(n)} \leq C_1 q^{-n},$$

  where $C_1 = q^{\sigma(q)}$.

- For the second bound we still use the upper bound (5.17), by upper bounding the other multiplicative term. We have

$$p_i^{(n)} \leq \underbrace{\frac{\mathcal{S}_i}{q^{\alpha n^2}}}_{<1}(M-1)\left(1-\frac{\mathcal{B}_{i-1}}{q^{\alpha n^2}}\right)^{M-2} < Me^{(M-2)\ln\left(1-\frac{\mathcal{B}_{i-1}}{q^{\alpha n^2}}\right)}.$$

  By properties of the logarithm, we have $\forall 0 \leq x < 1,\ \ln(1-x) \leq -x$. Thus

$$(M-2)\ln\left(1-\frac{\mathcal{B}_{i-1}}{q^{\alpha n^2}}\right) \leq -(M-2)\frac{\mathcal{B}_{i-1}}{q^{\alpha n^2}}.$$

  If we use the lower bound given in (2.4), and the fact that $\log_q(M-2) > \log_q(M) - 1 = \alpha n^2 R - 1$ as soon as $M \geq 4$ we have

$$-(M-2)\frac{\mathcal{B}_{i-1}}{q^{\alpha n^2}} \leq -q^{(\alpha+1)n(i-1)-(i-1)^2-\alpha n^2(1-R)+1}.$$

  This inequality implies that the quantity $-(M-2)\frac{\mathcal{B}_{i-1}}{q^{\alpha n^2}}$ is less than $-n$ as soon as

$$(\alpha+1)n(i-1)-(i-1)^2-\alpha n^2(1-R)+1-\log_q(n) \geq 0.$$

  The discriminant of the inequality is

$$\Delta = (\alpha-1)^2n^2 + \alpha n^2 R + 4 - 4\log_q(n).$$

  Therefore as soon as $n \geq 4\log_q(n) - 2$ we have that $\Delta \leq (\alpha-1)^2n^2 + \alpha n^2 R - n$, and provided that

$$i/n \geq \frac{\alpha+1}{2} - \sqrt{\frac{(\alpha-1)^2}{4} + \alpha R - \frac{1}{n}},$$

  the quantity $-(M-2)\frac{\mathcal{B}_{i-1}}{q^{\alpha n^2}}$ is less than $-n$. Therefore $p_i^{(n)} \leq e^{-n}$, and we obtain the result by taking $C_1' = \log_q(e)$.

■

## 5.3 Proof of the theorem

In this section we proove theorem **??**.

**Proof of theorem ??**

The proof is divided into two parts. The first part derives an equivalent for the expectation of the minimum rank distance, while second part gives an equivalent for the variance of the minimum rank distance

- By definition the expectation of the minimum rank distance is given by

$$E(d_n) = \sum_{i=1}^{n} i\Pr(d_n = i) = \sum_{i=1}^{n} ip_i^{(n)}.$$

Let us define

$$\left\{ \begin{array}{l} a_n = n\left(\frac{\alpha+1}{2} - \sqrt{\frac{(\alpha-1)^2}{4} + \alpha R + \frac{1}{n}}\right), \\ b_n = n\left(\frac{\alpha+1}{2} - \sqrt{\frac{(\alpha-1)^2}{4} + \alpha R - \frac{1}{n}}\right). \end{array} \right.$$

The upper bounds for $p_i^{(n)}$ of Lemma 1 directly implies that for sufficiently large $n$

$$\left\{ \begin{array}{rcl} \sum_{i=1}^{\lfloor a_n \rfloor} i p_i^{(n)} & \leq & C_1 q^{-n} \sum_{i=1}^{n} i \quad = \quad O\left(n^2 q^{-n}\right), \\ \sum_{i=\lceil b_n \rceil}^{n} i p_i^{(n)} & \leq & q^{-C_1' n} \sum_{i=1}^{n} i \quad = \quad O\left(n^2 q^{-C_1' n}\right). \end{array} \right.$$

Now we want to evaluate the contribution of the terms labeled by $\lfloor a_n \rfloor + 1 \leq i \leq \lceil b_n \rceil - 1$. We have

$$a_n \sum_{i=\lfloor a_n \rfloor+1}^{\lceil b_n \rceil-1} p_i^{(n)} \leq \sum_{i=\lfloor a_n \rfloor+1}^{\lceil b_n \rceil-1} i p_i^{(n)} \leq b_n \sum_{i=\lfloor a_n \rfloor+1}^{\lceil b_n \rceil-1} p_i^{(n)}. \tag{5.21}$$

Now since

$$1 = \sum_{i=1}^{n} p_i^{(n)} = \sum_{i=\lfloor a_n \rfloor+1}^{\lceil b_n \rceil-1} p_i^{(n)} + \underbrace{\sum_{i=1}^{\lfloor a_n \rfloor} p_i^{(n)}}_{O(n^2 q^{-n})} + \underbrace{\sum_{i=\lceil b_n \rceil+1}^{n} p_i^{(n)}}_{O(n^2 q^{-C_1' n})},$$

we obtain

$$1 + O(n^2 q^{-Cn}) \leq \sum_{i=\lfloor a_n \rfloor+1}^{\lceil b_n \rceil-1} p_i^{(n)} \leq 1,$$

where $C = \min(1, C_1')$. From the definition, it is obvious that $a_n = O(n)$. Therefore, by replacing the inequalities in equation (5.21), we obtain that

$$a_n + O(n^3 q^{-Cn}) \leq \sum_{i=\lfloor a_n \rfloor+1}^{\lceil b_n \rceil-1} i p_i^{(n)} \leq b_n.$$

By using all the previous inequalities, we obtain

$$a_n + O(n^3 q^{-Cn}) \leq E(d_n) \leq b_n + O(n^2 q^{-C_1' n}).$$

Now to finish the proof we have to show that $a_n$ and $b_n$ are close enough. Let us denote $A = \sqrt{(\alpha-1)^2/4 + \alpha R}$. From the definitions of $a_n$ and $b_n$ we have

$$\begin{array}{rcl} b_n - a_n & = & nA\left(\sqrt{1 + 1/(An)} - \sqrt{1 - 1/(An)}\right), \\ & = & nA(1/(An) + O(1/n^2)), \\ & = & O(1). \end{array}$$

Therefore we deduce the result

$$E(d_n) = d_{GV} + O(1), \tag{5.22}$$

where

$$d_{GV} \stackrel{def}{=} n\Delta_{GV}.$$

Therefore

$$\frac{E(d_n)}{n} = \Delta_{GV} + O(1/n).$$

- The variance is by definition $Var(d_n) = E(d_n^2) - E(d_n)^2$. From (5.22) and since $d_{GV} = O(n)$, we have
$$E(d_n)^2 = d_{GV}^2 + O(n).$$
To deal with $E(d_n^2)$ we recall its definition:
$$E(d_n^2) = \underbrace{\sum_{i=1}^{\lfloor a_n \rfloor} i^2 p_i}_{=O(n^3 q^{-C_2})} + \underbrace{\sum_{i=\lceil b_n \rceil + 1}^{n} i^2 p_i}_{=O(n^3 q^{-C_1' n})} + \sum_{i=\lfloor a_n \rfloor + 1}^{\lceil b_n \rceil - 1} i^2 p_i.$$
Using the same approach as for the expectation, and the approximations of equation (5.21), we show that
$$a_n^2 + O(n^4 q^{-Cn}) \leq E(d_n^2) \leq b_n^2 + O(n^3 q^{-C_1' n}).$$
Since $a_n^2 - b_n^2 = O(n)$, we obtain finally that $E(d_n^2) = d_{GV}^2 + O(n)$ and that
$$Var(d_n) = O(n).$$
Hence,
$$\frac{Var(d_n)}{n^2} = O(1/n).$$

■

# 6 Packing density of optimal codes

In section 3, we showed that there are no perfect codes in rank metric. From a cryptographic point of view it is a disappointing result since the existence of perfect codes would provide a manner to design signature schemes. Namely, the procedure is the following:

- Given a vector $\mathbf{y}$ in some space $GF(q^m)^n$,
- given a code $\mathcal{C}$,

if the vector $\mathbf{y}$ lies within a ball centered on a codeword of $\mathcal{C}$ and of radius less than the error correcting capability of $\mathcal{C}$ then return the center of the ball. Else the vector $\mathbf{y}$ cannot be signed.

Under this framework, if the code $\mathcal{C}$ was perfect, every vector of $GF(q^m)^n$ would be uniquely signed. Since it is not the case, there are residual vectors $\mathbf{y}$ that cannot be signed.

Although it is almost the same problem in Hamming metric, a signature scheme was designed in 2001, based on this principle, [7]. In this construction, the authors used binary Goppa codes with a very high rate so that the packing density of the code in the ambiant space is pretty high. Hence, with slight and controlled modifications of the message which has to be signed, they manage to transformed it into a signable message. In this precise case, the system is faster if the packing density is higher.

This is one of the main reasons which motivates the study of the packing density of codes in rank metric and in particular of the MRD codes. By definition, the packing density of a $(n, M, d)_r$ code is
$$D = \frac{M\mathcal{B}_t}{q^{mn}},$$

where $t = \lfloor (d-1)/2 \rfloor$.

Singleton inequality provides an upper bound on the cardinality of codes with given parameters. We call optimal codes or MRD (*Maximal Rank Distance*) codes, codes satisfying the Singleton equality

**Definition 5 (MRD-codes – [11])**
*A $(n, M, d)_r$-code over $GF(q^m)$ is called MRD if*

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

From this definition it follows that, whenever a code is MRD, the corresponding transposed code is also MRD. In this context we proove the following proposition:

**Proposition 7 (Density of MRD-codes)**
*Let $\mathcal{C}$ be a MRD-code, $(n, q^{m(n-2t)}, 2t+1)_r$ over $GF(q^m)$. The packing density of $\mathcal{C}$ satisfies*

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

The proposition shows that whenever the length of the code is equal to the extension degree, *i.e.* $n = m$ and if $n$ tends to $\infty$, then its packing density is lower bounded by the quantity $q^{-t^2-t}$. This lower bound depends only on the rank error-correcting capability of the code. Although MRD codes without distortion are not suitable for cryptograpic applications, it is worth remarking that there are families of codes whose packing density can be asymptotically bounded by a function of their minimum rank distance alone.

Therefore constructing such families would be of cryptographic interest. Namely, the complexity of the decoding algorithms is such that $t$ could remain very small, because they are exponential in the length or the dimension of the code, [27, 6].

# 7 Conclusion

In this paper we presented showed that asymptotically random codes reach GV-bounds in rank metric also. This behaviour can provide a benchmark for the construction of cryptosystems whose public-key could be secure, since it appears important that the public-code can not be distinguished from a random codes, as seems to be the case for medium rate Goppa codes (it is no more the case for high rate Goppa codes,[9]. One of the key arguments for saying that binary Goppa codes are good candidates for cryptographic applications is that their family reaches GV whereas for instance the family of BCH codes does not, [22]. So these benchmarks, from a cryptographic point of view could guarantee some randomness behaviour of a family of codes in rank metric.

We can mention also some open problems in rank metric that are worth investigating :

- We mentioned in section 4 that the asymptotic relative minimum distance of codes reaching GV is similar to the Johnson bound for Gabidulin codes. It could be of interest to understand the link between both bounds.
- Constructing also families of non MRD codes whose packing density depend on the minimum distance only is a challenging problem.

## References


[1] N. Suresh Babu *Studies on rank distance codes*, PhD Dissertation, IITP Madras, Feb. 1995.

[2] A. Barg. *Handbook of Coding Theory, Vol. 1*, chapter 7, pages 649–754. North–Holland, 1998.

[3] A. Barg and G. D. Forney. Random Codes: Minimum Distances and Error Exponents *IEEE Transactions on Information Theory*, 48(9):2568–2573, September 2002.

[4] M. Blaum and R. J. McEliece. Coding protection for magnetic tapes: A generalization of the Patel-Hong code. *IEEE Transactions on Information Theory*, 31(5):690–693, September 1985.

[5] A. Canteaut and F. Chabaud. A new algorithm for finding minimum-weight words in a linear code: Application to McEliece's cryptosystem and to narrow-sense BCH codes of length 511. *IEEE Transactions on Information Theory*, 44(1):367–378, January 1998.

[6] F. Chabaud and J. Stern. The cryptographic security of the syndrome decoding problem for rank distance codes. In K. Kim and T. Matsumoto, editors, *Advances in Cryptology - ASIACRYPT '96*, volume 1163 of *LNCS*. Springer, November 1996.

[7] N. Courtois, M. Finiasz and N. Sendrier How to achieve a McEliece-based signature scheme. In C. Boyd, editor, *Advances in Cryptology - ASIACRYPT'2001*, volume 2248 of *LNCS*, pp 151–174, Springer, 2001.

[8] P. Delsarte. Bilinear forms over a finite field, with applications to coding theory. *Journal of Combinatorial Theory, Series A*, 25:226–241, 1978.

[9] J.-C. Faugère, A. Otmani, L. Perret and J.-C. Faugère Algebraic cryptanalysis of McEliece variants with compact keys In H. Gilbert, editor, *Advances in Cryptology - EUROCRYPT 2010*, volume 6110 of *LNCS*, pp 279–294, Springer 2010.

[10] C. Faure. Average number of Gabidulin codewords within a sphere. *Proceedings of the 10th International Workshop on Algebraic and Combinatorial Theory - ACCT-10*, pages 86–90, 2006.

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

[12] E. M. Gabidulin and A. V. Ourivski. Modified GPT PKC with right scrambler. In D. Augot and C. Carlet, editors, *Proceedings of the 2nd International workshop on Coding and Cryptography, WCC 2001*, pages 233–242, 2001. ISBN Number : 2-761-1179-3.

[13] E .M. Gabidulin, A. V. Paramonov, and O. V. Tretjakov. Ideals over a non-commutative ring and their application in cryptology. *INDOCRYPT 2004*, volume 2656 of *LNCS*, pages 360–373. Springer-Verlag, 2004. [21]

[14] M. Gadouleau and Z. Yan. Properties of codes with the rank metric. In *Proceedings of Globecom 2006*.

[15] M. Gadouleau and Z. Yan. On the decoder error probability of bounded rank distance decoders for maximum-rank distance codes. In *IEEE Transactions on Information Theory*, 54(7):3202–3206.

[16] M. Gadouleau and Z. Yan. Packing and Covering properties of rank metric codes. In *IEEE Transactions on Information Theory*, 54(9):3873–3883.

[17] J. K. Gibson. Severely denting the Gabidulin version of the McEliece public-key cryptosystem. *Designs, Codes and Cryptography*, vol. 6, 1995, pp. 37–45.

[18] J. K. Gibson. The security of the Gabidulin public-key cryptosystem. In U. Maurer, editor, *Advances in Cryptology – EUROCRYPT'96*, volume 1070 of *LNCS*, pages 212–223. 1996.

[19] A. R. Hammons. Space-time code designs based on the generalized binary rank criterion with applications cooperative diversity. In Ø. Ytrehus, editor, *Proceedings of the 4th International Workshop on Coding and Cryptography, WCC 2005*, volume 3969 of *LNCS*, pages 69–84. Springer, 2006.

[20] R. Kötter and F. R. Kschischang. Coding for errors and erasures in the field of random network coding *IEEE Transactions on Information Theory*, 54(8):3579–3591, August 2008.

[21] P. Loidreau. Designing a rank metric based McEliece cryptosystem. In N. Sendrier editor, *Proceedings of the 3rd International Workshop on Post Quantum Cryptography, PQCrypto 2010*, number 6061 in LNCS, pages 142–152, 2010.

[22] J. van Lint *Introduction to Coding Theory*, chapter 5. volume 84 or *Graduate Texts in Mathematics*, Springer-Verlag, 1982.

[23] H. F. Lu and P. V. Kumar. A unified construction of space-time codes with optimal rate-diversity tradeoff. *IEEE Transactions on Information Theory*, 51(5):1709–1730, May 2005.

[24] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error–Correcting Codes.* North Holland, 1977.

[25] R. J. McEliece. *A public-key cryptosystem based on algebraic coding theory.* Jet Propulsion Lab. DSN Progress Report, 1978.

[26] A. V. Ourivski, E. M. Gabidulin, B. Honary, and B. Ammar. Reducible rank codes and their applications to cryptography. *IEEE Transactions on Information Theory*, 49(12):3289–3293, December 2003.

[27] A. V. Ourivski and T. Johannson. New technique for decoding codes in the rank metric and its cryptography applications. *Problems of Information Transmission*, 38(3):237–246, September 2002.

[28] R. Overbeck. Structural attacks for public-key cryptosystems based on Gabidulin codes *Journal Of Cryptology*, 21(2):280–301, 2008.

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

[30] H. Rashwan, E. M. Gabidulin and B. Honary. A smart approach for GPT cryptosystems based on rank codes. In *2010 IEEE International Symposium on Information Theory, ISIT 2010*, 2010.

[31] R. M. Roth. Maximum-Rank array codes and their application to crisscross error correction. *IEEE Transactions on Information Theory*, 37(2):328–336, March 1991.

[32] D. Silva, F. R. Kschischang and R. Kötter. A rank-metric approach to error control in random netword coding *IEEE Transactions on Information Theory*, 55(12):3951–3967, September 2009.

[33] V. Tarokh, N. Seshadri, and R. Calderbank. Space-time codes for high data rate wireless communication: Performance criterion and code construction. *IEEE Transactions on Information Theory*, 44(2):744–765, March 1998.