*Eleventh International Workshop on Algebraic and Combinatorial Coding Theory*
*June 16-22, 2008, Pamporovo, Bulgaria* *pp. 192-198*

# Properties of codes in rank metric

Pierre Loidreau Pierre.Loidreau@m4x.org
CELAR and IRMAR, Université de Rennes

**Abstract.** We study properties of rank metric and codes in rank metric over finite fields. We show that perfect codes do not exist. We derive an equivalent of the Varshamov-Gilbert bound in Hamming metric. We study the asymptotic behavior of the minimum rank distance of codes that are on GV. We show that the packing density of maximum rank distance codes is lower bounded by a function depending on the error-correcting capability. We show that there are asymptotically perfect codes correcting errors of rank 1 over fields of characteristic 2.

## 1 Introduction

Apart from cryptographic applications and applications in tape recording, rank metric found recently many more applications in the field of random network coding and construction of optimal rate-diversity tradeoff space-time codes.

In this paper, we first recall properties of rank metric and existing bounds. We show that perfect codes cannot exist in rank metric. Then we exhibit an asymptotic relation between parameters of a code which is said to be on GV, that is, which satisfies the Varshamov-Gilbert bound in rank metric.

We also study codes which reach the Singleton bound. These codes are called MRD-codes for *Maximum Rank Distance* codes. After recalling the formula given by Gabidulin on the rank distribution of linear MRD-codes, we present some simulations showing that rank distribution of random codes and of MRD-codes is very similar. In addition, we prove that the density of *correctable* errors for MRD-codes corresponding to codes formed with square matrices is lower bounded by a function depending only on the error-correcting capability of the code. In the special case of fields of characteristic 2, we show that we can construct a family of codes over fields of characteristic 2 that is asymptotically perfect.

## 2 Properties of 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 $n$ denotes the length of the code. The rank norm over $GF(q)$ of an element of $GF(q^m)^n$ is defined by

**Definition 1 ([1])** *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 $t \geq 0$: $\mathcal{S}_t \stackrel{def}{=} \{\mathbf{y} \in GF(q^m)^n \mid \mathrm{Rk}(\mathbf{y}) = t\}$
- Ball of radius $t \geq 0$: $\mathcal{B}_t \stackrel{def}{=} \cup_{i=0}^{t} \mathcal{S}_i$

We have the following bounds:

$$\begin{cases} q^{(m+n-2)t-t^2} & \leq \mathcal{S}_t \leq & q^{(m+n+1)t-t^2} \\ q^{(m+n-2)t-t^2} & \leq \mathcal{B}_t \leq & q^{(m+n+1)t-t^2+1} \end{cases} \tag{2.1}$$

Let $\mathcal{C} \subset GF(q^m)^n$ for $m$ and $n$ non-zero integers. If $M$ denotes the cardinality of $\mathcal{C}$ and $d \stackrel{def}{=} \min_{\mathbf{c}_1 \neq \mathbf{c}_2 \in \mathcal{C}}(\mathrm{Rk}(\mathbf{c}_1 - \mathbf{c}_2))$ 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 $\mathcal{C}$.

## 3 Upper bounds and perfect codes

In this section we recall a Singleton-like bound for rank metric codes and state an equivalent to the sphere-packing bound. We show that there are no perfect codes in rank metric.

**Proposition 1** *Let* $\mathcal{C}$ *be a* $(n, M, d)_r$ *code over* $GF(q^m)$. *We have*

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

$$M \times \mathcal{B}_t \leq q^{mn}, \tag{3.2}$$

For the proof of Singleton-like bound see [1, 6]. The proof of the *sphere-packing* 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. The proof is similar to that of Hamming metric.

If we define perfect codes as usual, that is: an $(n, M, d)_r$-code over $GF(q^m)$ is perfect if and only if $M \times \mathcal{B}_t = q^{mn}$, we can investigate the existence of perfect codes. The following proposition answers the question

**Proposition 2** *There are no perfect codes in rank metric.*

*Proof.* The proof can be derived from the bounds (2.1)

## 4 A Varshamov–Gilbert like bound

In rank metric the equivalent of Varshamov–Gilbert (GV) bound is given by the following result:

**Proposition 3** *Let $m, n, M, d$ be positive integers. If*

$$M \times \mathcal{B}_{d-1} < q^{mn}, \tag{4.3}$$

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

From this result we define the property for some code to be on GV:

**Definition 2** *An $(n, M, d)_r$-code is said to be on GV if*

$$(M-1) \times \mathcal{B}_{d-1} < q^{mn} \leq M \times \mathcal{B}_{d-1}, \tag{4.4}$$

Now we proove the following result given the relations between the parameters of a $(n, M, d)_r$, which is on $GV$ and whose cardinality is not *too small*.

**Proposition 4** *Consider an $(n, M, d)_r$-code $\mathcal{C}$ over $GF(q^m)$ where $m = m(n) \geq n$. Then, if $\mathcal{C}$ is on GV we have*

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

*provided $\log_q M = \lambda(n) m$, where $\lambda(n) = o(n)$ tends to $+\infty$ with $n$.*

*Proof.* By taking the base $q$ logarithm of the inequalities (2.1), we obtain from property (4.4) that

$$\begin{cases} mn \leq (m+n+1)(d-1) - (d-1)^2 + 1 + \log_q M, \\ \log_q(M-1) + (m+n-2)(d-1) - (d-1)^2 < mn. \end{cases}$$

Since $M \geq 2$ we have further that $\log_q(M-1) \geq \log_q(M) - \log_q(2) \geq \log_q(M) - 1$. Hence the minimum distance of the code must satisfy

$$\begin{cases} 0 \leq -d^2 + (m+n+3)d + \log_q M - mn - (m+n+1), \\ 0 \geq -d^2 + (m+n)d + \log_q M - mn - (m+n). \end{cases}$$

The inequalities are given by second order equations whose discriminant are respectively

$$\Delta_1 = (m-n)^2 + 4\log_q(M) + 2(m+n) + 5,$$
$$\Delta_2 = (m-n)^2 + 4\log_q(M) - 4(m+n).$$

Therefore the minimum distance of a code on GV satisfies the inequalities

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

Under the conditions of the theorem ($\log_q M = \lambda(n)(m+n)$, where $\lambda(n) = o(n)$ and tends to infinity with $n$), it is not very difficult to complete the proof of the proposition. ■

**Example 1** *A special case is when $m = n$ and for a family of constant rate codes $0 < R < 1$ that is*

$$\log_q M = n^2 R.$$

*In that case we have*

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

*This result implies that the ratio of the minimum rank distance on the length of the code is asymptotically constant.*

## 5 Maximum rank distance codes

Singleton inequality gives an upper bound on the cardinality of codes with given parameters. We call optimal codes or MRD (*Maximum Rank Distance*) codes, codes attaining the Singleton bound

**Definition 3 (MRD-codes – [1])** *A $(n, M, d)_r$-code over $GF(q^m)$ is called MRD if*

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

We study properties of MRD codes such as the distribution of the rank of codewords as well as bounds on their packing density.

### 5.1 Rank weight distribution of MRD-codes

In Hamming metric, the weight distribution of MDS-codes is well-known [5]. Gabidulin showed the rank distribution of codes in rank metric can be expressed by

**Proposition 5 ([1])** *Let $A_s(n,d)$ be the number of rank $s$ codewords of an MRD-code over $GF(q^m)$. Then*

$$A_{d+\ell}(n,d) = \left[ \begin{array}{c} n \\ d+\ell \end{array} \right]_q \sum_{t=0}^{\ell} (-1)^{t+\ell} \left[ \begin{array}{c} d+\ell \\ \ell+t \end{array} \right]_q q^{\binom{\ell-t}{2}} \left( q^{m(t+1)} - 1 \right), \qquad (5.5)$$

*where* $\left[ \begin{array}{c} n \\ i \end{array} \right]_q$ *is the Gaussian binomial.*

Our contribution to this section comes from the simulations we made to evaluate the *randomness degree* of MRD-codes. By using these simulations we obtained that the rank distribution of random $GF(q)$-linear codes in rank metric was almost identical to the weight distribution of linear MRD-codes. Results are presented in table 5.1. The table gives the base 2 logarithm of the proportion $A_i(n,d)/2^{mn}$ for $n = 32,\ m \geq 32$. The left-most curve corresponds to $m = 32$, the right-most to $m = 40$. We made simulations for random $GF(q)$-linear codes as well as for MRD-codes *sufficiently* large with the same parameters. For ranks significantly greater than the minimum rank distance both curves coincide very accurately.

### 5.2 Packing density of MRD codes

In section 3 we proved that no perfect codes existed in rank metric. However a natural question can be: what is the *defect* of *perfectitude* of MRD-codes, that is, given an $(n, M, d)_r$ MRD-code what is the volume of the space covered by balls of radius $\lfloor (d-1)/2 \rfloor$ compared to the volume of the whole space. The *packing density* of the code is thus defined by

$$D = \frac{M\mathcal{B}_t}{q^{mn}},$$

where $t = \lfloor (d-1)/2 \rfloor$ is the rank error-correcting capability of the code. By using the bounds (2.1), we prove

**Proposition 6 (Packing 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*

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

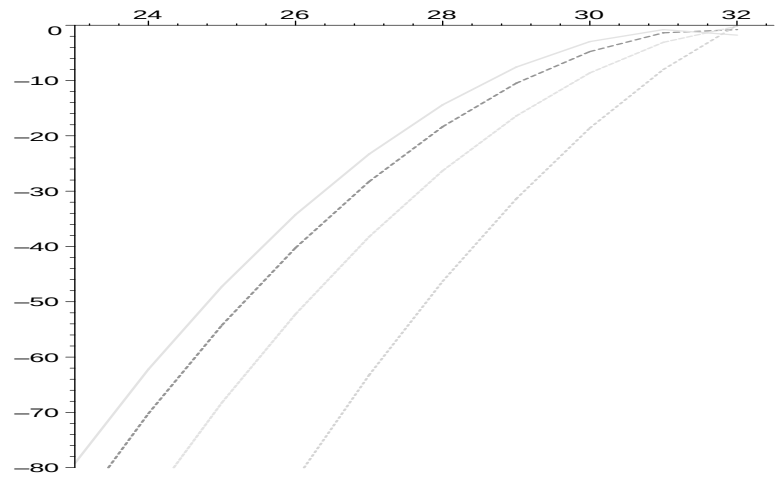


Table 1: Base 2 logarithm of proportion of words of given rank in an MRD-codes of length $n = 32$ over $GF(2^m)$, where $m = 32,\ 33,\ 35,\ 40$.

This proposition shows that, whenever the length of the code equals the extension degree, *i.e.* $n = m$, and if $n$ tends to $\infty$, then the packing density is lower bounded by $q^{-t^2-2t}$, which depends only on the rank error-correcting capability of the code.

**Particular case of rank 1 correcting MRD codes** For rank 1 MRD codes where $m = n$, we can express the exact formulas and obtain

**Proposition 7** *An $(n, q^{n-2}, 3)_r$ MRD-code over $GF(q^n)$ has a packing density equal to*

$$D = \frac{1 - 2q^{-n} + q^{-2n+1}}{q - 1}. \tag{5.6}$$

There is a special interest in the binary case. In section 3, we showed that there are no perfect codes in rank metric. However from previous proposition wd have

**Corollary 1** *Let $\mathcal{F} = \{\mathcal{C}_i\}_{i\geq 2}$ be a family of $(i, 2^{i-2}, 3)_r$ MRD-codes over $GF(2^i)$. If $D_i$ is the packing density of code $\mathcal{C}_i$ then*

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

This means that $\mathcal{F}$ is a sequence of codes with increasing length and alphabet that are asymptotically perfect. Since Gabidulin codes are MRD codes we can construct such families of codes.

## References

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

[2] E. M. Gabidulin, A fast matrix decoding algorithm for rank-error correcting codes, *Algebr. Coding, Lect. Notes Comp. Sci.* 573, G. Cohen, S. Litsyn, A. Lobstein, G. Zémor, editors, Springer-Verlag, 1991, 126-133.

[3] E .M. Gabidulin, A. V. Paramonov, and O. V. Tretjakov, Ideals over a non-commutative ring and their application in cryptology, *Adv. Cryptol. – EUROCRYPT'91, Lect. Notes Comp. Sci.* 547, D. W. Davies, editor, Springer-Verlag, 1991, 482-489.

[4] P. Loidreau, A Welch-Berlekamp like algorithm for decoding Gabidulin codes, *Proc. Fourth Intern. Workshop Cod. Crypt., Lect. Notes Comp. Sci.* 3969, Ø. Ytrehus, editor, 2006, 36-45.

[5] F. J. MacWilliams, N. J. A. Sloane, *The theory of error-correcting codes*, North Holland, 1977.

[6] A. V. Ourivski, E. M. Gabidulin, B. Honary, B. Ammar, Reducible rank codes and their applications to cryptography, *IEEE Trans. Inform. Theory* 49, 2003, 3289-3293.

[7] G. Richter, S. Plass, Fast decoding of rank-codes with rank errors and column erasures, *IEEE Intern. Symp. Inform. Theory*, 2004.

[8] R. M. Roth, Maximum-rank array codes and their application to crisscross error correction, *IEEE Trans. Inform. Theory* 37, 1991, 328-336.