On subcodes of codes in rank metric

Ernst M. Gabidulin
Moscow Institute of Physics and Technology
Institutskii per., 9 141700 Dolgoprudny
Moscow Region, Russia
Email: gab@pop3.mipt.ru

Pierre Loidreau
Ecole Nationale Supérieure de Techniques Avancées
32, bd Victor, 75015 Paris, France
Email: Pierre.Loidreau@ensta.fr

***Abstract*— Maximum rank distance codes are the equivalent in rank-metric of Reed-Solomon codes whose subcodes have been widely studied. In this paper we characterize subspace subcodes of MRD codes and we show that it is possible to construct efficient polynomial-time encoding-decoding procedures for these subcodes. In a second part we show that subfield subcodes of Maximum rank distance codes can be represented in some sense by the direct sum of Maximum rank distance codes of smaller length and same minimum distance. We then derive an algorithm correcting some error-patterns beyond the error-correcting capability of the codes.**

I. Introduction

Many publications concern specific subcodes of the optimal family of Reed-Solomon. There have been significant work on their subspace (or subgroup) subcodes, as well as subfield subcodes, since many of the interesting families of codes can be derived from this family of polynomial codes [5], [8], [1].

Maximum rank distance codes (MRD codes) are equivalent in rank metric to RS codes [2], [7]. They have fast decoding algorithms up to their error-correcting capability [3], [2], [7], [6]. Therefore, studying subcodes of rank codes is of interest in designing new codes for which there exist decoding algorithms up to some rank distance.

In this paper we classify subcodes of rank codes that are constructed by taking the words of the codes whose coordinates lie in subspaces or in subfield of the field alphabet. In particular, we design a systematic encoding procedure for subspace subcodes, and we design specific decoders, of lower complexity than using the decoder for the initial code. A particular subclass of subspace subcodes of great interest is the class of subfield subcodes. We show that, in some sense, they are similar to the direct sum of maximum rank distance codes over a smaller field. For these codes we show how to correct some error-patterns beyond the error correcting capability, by decoding several times in maximum rank-distance codes of smaller size.

II. Maximum Rank Distance codes

Let $GF(q)$ be the base field and $GF(q^n)$ be an extension field of $GF(q)$.

Definition 1 (Rank of a vector): Let $\mathbf{e} = (e_1, \ldots, e_n) \in GF(q^n)^n$, then, the rank of $\mathbf{e}$ is the the rank of the $n \times n$ q-ary matrix obtained by extending every component e_i over a basis of $GF(q^n)/GF(q)$. It is denoted $\mathrm{Rk}(\mathbf{e})$

A (n, k, d) MRD-code $\mathcal{G}$ over the field $GF(q^n)$ is defined by a generator matrix of the form

$$\mathbf{G} = \begin{bmatrix} g_1 & \cdots & g_n \\ g_1^{[1]} & \cdots & g_n^{[1]} \\ \vdots & \ddots & \vdots \\ g_1^{[k-1]} & \cdots & g_n^{[k-1]} \end{bmatrix}, \qquad \text{(II.1)}$$

where $g_1, \ldots, g_n \in GF(q^n)$ are linearly independent over the base field $GF(q)$. We define $[i] := q^i$, when $i \geq 0$ and $[i] := q^{n-i}$ when $i < 0$.

This code can be defined in terms of a parity check matrix $\mathbf{H}$ such that

$$\mathbf{G}\mathbf{H}^T = \mathbf{0}, \qquad \text{(II.2)}$$

where

$$\mathbf{H} = \begin{bmatrix} h_1 & \cdots & h_n \\ h_1^{[1]} & \cdots & h_n^{[1]} \\ \vdots & \ddots & \vdots \\ h_1^{[d-2]} & \cdots & h_n^{[d-2]} \end{bmatrix}, \qquad \text{(II.3)}$$

and $h_1, \ldots, h_n \in GF(q^n)$ are linearly independent over the base field $GF(q)$. These codes are optimum for rank distance (their minimum distance is $d = n - k + 1$), and there exists polynomial-time decoding algorithms decoding up to their error-correcting capability, [2], [3], [7].

III. Subspace subcodes of rank codes

Let $\mathcal{G}$ be the code with generating matrix (II.1) and parity-check matrix (II.3). Let V_m be a m-dimensional subspace of the extended field $GF(q^n)$ considered as a vector space over $GF(q)$. Let $\mathbf{c} = (c_1, \ldots, c_n) \in \mathcal{G}$, such that $c_j \in V_m,\ j = 1, \ldots, n$.

We denote by $(\mathcal{G} \mid V_m)$ the set of all such code words and refer to this set as the *subspace subcode*. The dimension m must be greater than $d-1$ to avoid triviality. The code $(\mathcal{G} \mid V_m)$ is a group code (i.e., $GF(q)$-linear) but not $GF(q^n)$-linear. Thus, generally speaking it is not straightforward to design an efficient encoding procedure for group codes, [8].

In our case however, we show these subspace subcodes can be put into one to one correspondence with MRD codes over the same alphabet but of smaller length. This can be done with simple linear transformations over the base field. Therefore, it enables us to design an efficient encoding and decoding procedure.

A. Characterization

Let $\mathbf{b} = (\beta_1, \dots, \beta_m)$ be a basis of V_m over $GF(q)$. Let $\mathbf{c} = (c_1, \dots, c_n),\ c_j \in V_m$ for all j. The vector $\mathbf{c}$ is written in a unique manner under the form

$$\mathbf{c} = \mathbf{b}U = (\beta_1, \dots, \beta_m)U, \tag{III.4}$$

where $U = (U_{ij})_{i=1,j=1}^{m,n}$ is a q-ary $m \times n$ matrix. The vector $\mathbf{c}$ is a code word of $\mathcal{G}$ if and only if

$$\mathbf{c}\mathbf{H}^T = (\beta_1, \dots, \beta_m)U\mathbf{H}^T = \mathbf{0}. \tag{III.5}$$

The subspace subcode $(\mathcal{G} \mid V_m)$ is defined completely by the *fixed* basis $(\beta_1, \dots, \beta_m)$ and the set of $m \times n$ matrices U with coefficients in $GF(q)$ satisfying the condition (III.5). This condition is equivalent to the following one:

$$(\beta_1, \dots, \beta_m) \begin{pmatrix} v_1 & \cdots & v_1^{[d-2]} \\ \vdots & \ddots & \vdots \\ v_m & \cdots & v_m^{[d-2]} \end{pmatrix} = \mathbf{0}, \tag{III.6}$$

where

$$v_i = \sum_{j=1}^{n} U_{ij}h_j,\ i = 1, \dots, m. \tag{III.7}$$

Note that, given $(v_1, \dots, v_m)$ one recovers uniquely matrix U by taking the representation of every coordinate v_i in the basis $(h_1, \dots, h_n)$. The subspace subcode $(\mathcal{G}|V_m)$ is completely defined by the *fixed* basis $(\beta_1, \dots, \beta_m)$ and by the set of *all* vectors $(v_1, \dots, v_m)$ over the extended field $GF(q^n)$ satisfying the condition (III.6).

Condition (III.6) is equivalent to

$$(v_1, \dots, v_m) \begin{pmatrix} \beta_1^{[n]} & \dots & \beta_1^{[n-d+2]} \\ \vdots & \ddots & \vdots \\ \beta_m^{[n]} & \dots & \beta_m^{[n-d+2]} \end{pmatrix} = \mathbf{0}. \tag{III.8}$$

Relation (III.8) implies that $\mathbf{v} = (v_1, \dots, v_m)$ is a code word of a $GF(q^n)$-linear MRD code with parameters $[m, m-d+1, d]$. From now on this code will be denoted $\mathcal{LG}(V_m)$. A parity-check matrix of $\mathcal{LG}(V_m)$ is given by

$$\mathbf{H}(V_m) = \begin{pmatrix} \beta_1^{[n]} & \cdots & \beta_m^{[n]} \\ \vdots & \ddots & \vdots \\ \beta_1^{[n-d+2]} & \cdots & \beta_m^{[n-d+2]} \end{pmatrix}. \tag{III.9}$$

Definition 2: The code $\mathcal{LG}(V_m)$ is called the parent code of $(\mathcal{G}|V_m)$.

Thus, any subspace subcode of a MRD code is uniquely characterized by a MRD code with the same minimum distance but of smaller parameters. The subspace subcode $(\mathcal{G}|V_m)$ has cardinality $q^{n(m-d+1)}$.

We have the following proposition.

Proposition 1: Let $\mathbf{b} = \beta_1, \dots, \beta_m$ be a basis of V_m considered as a m-dimensional vector space over $GF(q)$. Then the mapping

$$\mathbf{c} \in (\mathcal{G}|V_m) \mapsto \mathbf{v} = (v_1, \dots, v_m) \in \mathcal{LG}(V_m),$$

is a bijection, and preserves the rank of vectors (*i.e.* $Rk(\mathbf{c}) = Rk(\mathbf{v})$).

B. Coding and decoding of subspace subcodes

Generally speaking, subspace subcodes are group codes, and there is no simple way to characterize their structure such as generating matrices or some parity-check matrix describing them in a compact way,see [5], [8]. However, thanks to our previous characterization we can design an efficient way to encode subspace subcodes of MRD codes.

Let $\mathbf{x} = (x_1, \dots, x_{m-d+1}) \in GF(q^n)^{m-d+1}$ be an information vector. Let $\mathbf{G}(V_m)$ be a generating matrix of the parent code $\mathcal{LG}(V_m)$. The encoding procedure is the following:

1) Compute $\mathbf{y} = \mathbf{x}\mathbf{G}(V_m)$;
2) Determine the q-ary matrix $U = (U_{ij})$, such that for all $i = 1, \dots, m$, we have $y_i = \sum_{j=1}^{n} U_{ij}h_j$;
3) Compute $\mathbf{c} = (\beta_1, \dots, \beta_m)U$;

Vector $\mathbf{c}$ is a codeword of the subspace subcode $(\mathcal{G}|V_m)$. The complexity of the encoding procedure consists in $(m-d+1)m$ multiplications in $GF(q^n)$, if we neglect the operations over the base field $GF(q)$.

Suppose we receive the vector $\mathbf{y} = \mathbf{c}+\mathbf{e}$, where $\mathbf{c} \in (\mathcal{G}|V_m)$ and $\mathbf{e}$ has coefficients in V_m and has rank $t \leq \lfloor (d-1)/2 \rfloor$. There are two ways to decode:

- In the code $\mathcal{G}$ by using the standard decoding algorithms for $\mathcal{G}$. The complexity is $\approx (d-1+t)n + t^3$ multiplications in $GF(q^n)$ if we take the decoding algorithm described in [3].
- By decoding in the parent code $\mathcal{LG}(V_m)$. Namely, $\mathbf{y}\mathbf{H}^T \overset{def}{=} (s_1, \dots, s_{d-1}) = \mathbf{e}\mathbf{H}^T$. Since $\mathbf{e}$ has rank t, we can write $\mathbf{e} = (\beta_1, \dots, \beta_m)E$, where $E = (E_{ij})_{i=1,j=1}^{m,n}$ is a $m \times n$ matrix of rank t over $GF(q)$. Let $\epsilon_i = \sum_{i=1}^{n} E_{ij}h_j$ for $i = 1, \dots, m$. We get the following equation

  $$(\epsilon_1, \dots, \epsilon_m)\mathbf{H}(V_m)^T = (s_1^{[n]}, s_2^{[n-1]}, \dots, s_{d-1}^{[n-d+2]}).$$

  Since $(\epsilon_1, \dots, \epsilon_m) = (h_1, \dots, h_n)E^T$ has rank t, it can be recovered by one decoding in $\mathcal{LG}(V_m)$. Afterwards, by expanding the elements ϵ_i on the basis $h_1, \dots, h_n$ we get E and then $\mathbf{e} = (\beta_1, \dots, \beta_m)E$. By neglecting the operations over the base field, the overall complexity of this algorithm is $\approx (d-1)m + tn + t^3$ multiplications in $GF(q^n)$.

IV. A PARTICULAR CASE: SUBFIELD SUBCODES

Previous section showed that subspace subcodes of rank codes could be completely classified by designing a simple rank-preserving bijection between a maximum rank distance code and the considered subspace subcode. This is very different from the Reed-Solomon case, where even determining the order of subspace subcodes is not an easy problem, since it depends on the structure of the considered subspace with respect to the action of the Frobenius automorphism, [4].

Now we are more particularly interested in subfield subcodes. In Hamming metric, subfield subcodes of Reed–Solomon, or GRS codes provide very interesting families of decodable codes (BCH codes, classical Goppa codes). In rank metric, they can be studied as a subfamily of subspace subcodes and we have properties of previous section, but they can also be considered by themselves.

Namely we have the following theorem.

Theorem 1: Let $\mathbf{H}$ be a parity-check matrix of a $[n, n-d+1, d]$-MRD code $\mathcal{C}$ over $GF(q^n)$. Let s be a positive integer dividing n and let

$$A = \begin{pmatrix} a_1 & \cdots & a_s \\ \vdots & \ddots & \vdots \\ a_1^{[d-2]} & \cdots & a_s^{[d-2]} \end{pmatrix}.$$

where the $a_i \in GF(q^s)$ for all $i = 1, \ldots, s$ form a linearly independent family over $GF(q)$. Therefore, A is a parity-check matrix of a $[s, s-d+1, d]$-MRD code over $GF(q^s)$.

Then, there exists a non-singular q-ary matrix S of size $n \times n$, such that a parity-check matrix $\mathbf{H}_{GF(q^s)}$ of $(\mathcal{C}|GF(q^s))$ is equal to:

$$\mathbf{H}_{GF(q^s)} = \begin{pmatrix} A & 0 & \cdots & 0 \\ 0 & A & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A \end{pmatrix} S.$$

The theorem means that, somehow, the subfield subcode of a maximum rank distance code of full length (*i.e.* the length of the code is equal to the extension degree) is a direct sum of maximum rank distance codes taken over the subfield. Moreover, it also implies that, whatever be the MRD code over $GF(q^n)$, if we fix a basis of $GF(q^n)/GF(q^s)$, then the subfield subcode is uniquely determined by a q-ary matrix S.

The direct sum structure of the subfield subcode can be used to decode beyond the error-correcting capability of the code. Namely, suppose one receives a vector $\mathbf{y} = \mathbf{c} + \mathbf{e}$, where $\mathbf{c}$ is a codeword of $(\mathcal{C}|GF(q^s))$, where $\mathcal{C}$ has minimum distance d and where $\mathbf{e}$ is some vector with coefficients in $GF(q^s)$ and of rank t.

If $t \leq (d-1)/2$, then $\mathbf{y}$ can be straightly decoded by using a decoder for the subfield subcode as described in previous section.

Now we consider another type of algorithm. We compute the syndrome

$$\mathbf{e}S^T \begin{pmatrix} A^T & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & A^T \end{pmatrix} \overset{def}{=} \mathbf{s}.$$

If we define

$$\mathbf{s} \overset{def}{=} (\mathbf{s}_1|\cdots|\mathbf{s}_s)$$
$$\mathbf{e}S^T \overset{def}{=} (\mathbf{e}_1|\cdots|\mathbf{e}_s),$$

where each $\mathbf{e}_i$ has length n/s, we obtain the following equations to solve:

$$\mathbf{e}_i A^T = \mathbf{s}_i, \quad \forall i = 1, \ldots, s,$$

where A is a parity-check matrix of a maximum rank distance code with minimum distance d. Therefore, if $\mathbf{e}_i$ has rank less than $(d-1)/2 \overset{def}{=} C$ for all i, the vector $\mathbf{e}$ can be recovered, by completing s-decoding steps in the MRD code of parity-check matrix A.

To evaluate the probability of such an event, we have to evaluate

$$P \overset{def}{=} Pr(Rk(\mathbf{e}_1) \leq C, \ldots, Rk(\mathbf{e}_{n/s}) \leq C | Rk(\mathbf{e}) = t)$$

Whenever $s = 2$, computing the number of such occurrences divided by the number of possible vectors, we can show that

$$P \approx 2^{n/2(C-t)-(t-C)^2}.$$

Hence if, for example $q = 2$ and $t = C + 1$, we have

$$P \approx 2^{-n/2+1}.$$

References

[1] P. Delsarte. On subfield subcodes of modified Reed–Solomon codes. *IEEE Transactions on Information Theory*, 20:575–576, 1975.

[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] M. Hattori, R. J. McEliece, and G. Solomon. Subspace subcodes of Reed–Solomon codes. *IEEE Transactions on Information Theory*, 44(5), September 1998.

[5] J. M. Jensen. Subgroup subcodes. *IEEE Transactions on Information Theory*, 41(3):781–785, May 1995.

[6] G. Richter and S. Plass. Fast decoding of rank-codes with rank errors and column erasures. In *Proceedings of ISIT 2004*, 2004.

[7] 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.

[8] M. van Dijk and L. Tolhuizen. Efficient encoding for a class of subspace subcodes. *IEEE Transactions on Information Theory*, 45(6):2142–2146, 1999.