Advances in Mathematics of Communications
Volume 00, No. 0, 2008, 1–9

Web site: http://www.aimSciences.org

PROPERTIES OF SUBSPACE SUBCODES OF GABIDULIN CODES

Ernst M. Gabidulin

Moscow Institute of Physics and Technology
Institutskii per. 9, 141700 Dolgoprudny
Moscow Region, Russia

Pierre Loidreau

CELAr and IRMAR, Université de Rennes
La Roche Marguerite
BP 57419, 35171 Bruz, France

Abstract. We investigate properties of subspace subcodes of Gabidulin codes. They are isomorphic to Gabidulin codes with the same minimum rank distance and smaller parameters. We design systematic encoding and decoding algorithms for subspace subcodes. We show that the direct sum of subspace subcodes of Gabidulin codes is isomorphic to the direct product of Gabidulin codes with smaller parameters. Thanks to this structure there is a great deal of correctable error-patterns whose rank exceeds the error-correcting capability. Finally we show that for particular sets of parameters, subfield subcodes of Gabidulin codes can be uniquely characterised by elements of the general linear group $\mathrm{GL}_n(GF(q))$ of non-singular q-ary matrices of size n.

1. Introduction

Gabidulin codes were introduced in [8]. They form a family of optimal codes for the so-called rank distance. There are polynomial-time algorithms decoding errors of rank less or equal to their error-correcting capability [8, 9, 24, 23, 16]. Gabidulin codes and more generally codes correcting rank errors found their first applications when data were stored on tapes, and errors occurred along specific rows or columns of the arrays, [4, 24, 3].

Recently, interest in Gabidulin codes was reactivated in two main fields:

- In the field of space-time coding: Codes with optimal rate-diversity tradeoff are sets of matrices over a finite constellation and such that, for a given size of the code, the matricial rank between two codewords is maximized. Lu and Kumar showed how to construct such codes from Gabidulin codes, [17].
- In the field of random network coding: Errors and erasures occur in some definite vector space of upper-bounded dimension. Suitable codes with efficient decoding algorithms can be constructed from Gabidulin codes, [25].

Apart from applications in coding theory, rank distance and the family of Gabidulin codes have been employed in the design of McEliece-like public-key cryptosystems, see [11]. The motivation for the use of codes correcting rank errors is that for similar parameters the work factor of decoding a random linear code in rank metric is larger than in Hamming metric, see [5, 20]. Therefore this enables to use smaller public keys than in the original system.

For the same reason that GRS codes shall not be used in cryptographic applications without being properly scrambled, Gabidulin codes have to be scrambled before being used. A procedure for scrambling was proposed in the original paper [11] and others were proposed recently, see [19, 15, 1]. It was shown however that the structure of Gabidulin codes could be recovered by an attacker if the parameters of the scrambler were not chosen adequately. Thus the public-key

2000 *Mathematics Subject Classification:* Primary: 11T71, 11T55; Secondary: 14G50.
Key words and phrases: Coding theory, subcodes structure, Gabidulin codes.

size must be increased and it reduces the interest of using rank distance, rather than Hamming distance, [21, 22].

Because of growing importance of rank distance and decodable codes for rank distance in modern applications, it is of interest to study the structure of codes derived from Gabidulin codes like subspace and subfield subcodes, not only for themselves but in the perspective of finding other classes of good codes for coding and cryptographic applications.

In Hamming metric the mere question of determining the minimum distance of a subfield subcode remains open. For the generic case, only bounds were obtained, [6, 27, 2]. For the wider family of subspace subcodes, the same type of bounds can be obtained, [13]. In the case of Reed-Solomon codes, the bounds were improved at the price of a more complicated formula involving the structure of the chosen subspace, [18, 12]. The problem of efficiently encoding information with subspace subcodes was investigated in the case of *bit shortened Reed-Solomon codes* and in the more general case of linear MDS codes [26, 7]. In the latter case the authors designed a very efficient systematic encoding algorithm. This algorithm is non optimal in the sense that it does not always encode all the theoretically possible amount of information.

This paper extends the results previously obtained and presented in [10] and shows that in some cases questions remaining open for subspace subcodes of Reed-Solomon codes in Hamming metric can be answered for Gabidulin codes in rank metric: When the length of the parent Gabidulin code is equal to the degree of the alphabet field, there exists a rank-preserving isomorphism between the subspace subcode and a Gabidulin code with smaller parameters. In that case we design a systematic procedure encoding all the possible information as well as a decoding algorithm correcting up to the capability of the subspace subcode. Then, we generalise the results to the direct sum of subspace subcodes and show that the number of decodable error-patterns is larger than what is theoretically possible for a code with the same parameters, but without this additional structure. Finally we prove that subfield subcodes of Gabidulin codes can be seen, modulo the action of the general linear group, as the direct sum of Gabidulin codes with smaller parameters.

2. Subspace subcodes in rank metric

This section is an introductory section: in a first part, we introduce rank metric and Gabidulin codes. In a second part, we recall the definition and general properties of subspace subcodes.

2.1. Codes in rank metric.

Let $GF(q)$ be the field with q elements and let $GF(q^m)$, $m \geq 1$ be the extension field with q^m elements. In the following, we regard $GF(q^m)$ either as a field or as an m-dimensional vector space over $GF(q)$.

Definition 1 (Rank of a vector, see [8])**.**
Let $\gamma_1, \ldots, \gamma_m$ be a basis of $GF(q^m)/GF(q)$ and let $\mathbf{e} = (e_1, \ldots, e_n) \in GF(q^m)^n$. The rank of $\mathbf{e}$ over $GF(q)$ is by definition the rank of the matrix $(e_{ij})_{i=1,j=1}^{m,n}$, where $e_j = \sum_{i=1}^{m} e_{ij}\gamma_j$. The rank of vector $\mathbf{e}$ is written $Rk(\mathbf{e})$.

Given a code $\mathcal{C} \subset GF(q^m)^n$, its minimum rank distance is

$$d \stackrel{def}{=} \min_{\mathbf{c}_1 \neq \mathbf{c}_2 \in \mathcal{C}} (\mathrm{Rk}(\mathbf{c}_1 - \mathbf{c}_2))$$

Definition 2. *A code $\mathcal{C}$ is a $(n, M, d)_r$ code over $GF(q^m)$ if*

- $\mathcal{C} \subset GF(q^m)^n$
- $|\mathcal{C}| = M$
- *$\mathcal{C}$ has minimum rank distance d*

Moreover if $\mathcal{C}$ is a k-dimensional linear code, it is said to be a $[n, k, d]_r$ code. The parameters are related by an equivalent of Singleton bound for rank distance see [8, 19]:

$$M \leq q^{\min(m(n-d+1), n(m-d+1))}, \tag{2.1}$$

And a code satisfying the equality $M = q^{\min(m(n-d+1), n(m-d+1))}$ is called a Maximum Rank Distance (MRD) code.

Let $[i] \stackrel{def}{=} q^i$, when $i \geq 0$ and $[i] \stackrel{def}{=} q^{m+i}$ when $i < 0$. Let $n \leq m$ and

$$\mathbf{G} = \begin{pmatrix} g_1 & \cdots & g_n \\ \vdots & \ddots & \vdots \\ g_1^{[k-1]} & \cdots & g_n^{[k-1]} \end{pmatrix}, \tag{2.2}$$

where $g_1, \ldots, g_n \in GF(q^m)$ are linearly independent elements over $GF(q)$. The code $\mathcal{G}$ generated by $\mathbf{G}$ is called a *Gabidulin code*, [8]. A parity-check matrix $\mathbf{H}$ of $\mathcal{G}$ has the same structure as $\mathbf{G}$:

$$\mathbf{H} = \begin{pmatrix} h_1 & \cdots & h_n \\ \vdots & \ddots & \vdots \\ h_1^{[d-2]} & \cdots & h_n^{[d-2]} \end{pmatrix}, \tag{2.3}$$

for elements $h_1, \ldots, h_n \in GF(q^m)$ linearly independent over $GF(q)$. The code $\mathcal{G}$ is an MRD-code and there are efficient polynomial-time decoding algorithms correcting errors of rank up to $C = \lfloor (d-1)/2 \rfloor$, see [8, 9, 24, 23, 16].

2.2. Subspace subcodes in rank metric.

Definition 3 (see [13], for instance)**.** *Let $\mathcal{G}$ be a linear code of length n over $GF(q^m)$. Let V_s ($s \leq m$) be an s-dimensional subspace of $GF(q^m)$. Then*

$$(\mathcal{G}|V_s) \stackrel{def}{=} \mathcal{G} \cap V_s^n,$$

is an $GF(q)$-linear subspace of $\mathcal{G}$ called subspace subcode *or* subgroup subcode *of $\mathcal{G}$ restricted to V_s.*

The following proposition lower bounds the cardinality of $(\mathcal{G}|V_s)$:

Proposition 1. *Let $\mathcal{G}$ be a $[n,k,d]_r$ code over $GF(q^m)$. Let V_s ($s \leq m$) be an s-dimensional subspace of $GF(q^m)$. If $ns - m(n-k) > 0$ then*

$$q^{ns-m(n-k)} \leq |(\mathcal{G}|V_s)|$$

A similar result was already proved in [13]. The principle of the proof is the following:

Let $\mathbf{c} = (c_1, \ldots, c_n) \in V_s^n$ and let $\mathbf{b} = (\beta_1, \ldots, \beta_s)$ be a bases of V_s. The vector $\mathbf{c}$ is uniquely decomposable under the form

$$\mathbf{c} = \mathbf{b}U = (\beta_1, \ldots, \beta_s)U, \tag{2.4}$$

where $U = (U_{i,t})_{i=1,t=1}^{s,n} \in GF(q)^{s \times n}$. Let $\mathbf{H} = (h_{j,t})_{j=1,t=1}^{n-k,n}$ be a parity-check matrix of $\mathcal{G}$. We have

$$\mathbf{c} \in (\mathcal{G}|V_s) \Leftrightarrow \begin{cases} \mathbf{c} = \mathbf{b}U, \\ (\beta_1, \ldots, \beta_s)U\mathbf{H}^T = \mathbf{0}, \end{cases} \tag{2.5}$$

where U is a q-ary matrix of size $s \times n$. By developing the equation we obtain the following linear system

$$\forall j = 1, \ldots, n-k, \quad \sum_{i=1,t=1}^{s,n} \underbrace{\beta_i h_{j,t}}_{\in GF(q^m)} \underbrace{U_{i,t}}_{\in GF(q)} = 0, \tag{2.6}$$

where the unknowns are the $U_{i,t}$ for $i = 1, \ldots, s$ and $t = 1, \ldots, n$. Let $\gamma_1, \ldots, \gamma_m$ be a basis of $GF(q^m)/GF(q)$. We can write

$$\forall i, j, t, \quad \beta_i h_{j,t} = \sum_{k=1}^{m} \delta_{i,t}^{(j,k)} \gamma_k$$

where $\delta_{i,t}^{(j,k)} \in GF(q)$. Therefore solving (2.6) in $GF(q)$ is equivalent to solving the following linear system:

$$\forall j = 1, \ldots, n-k, \ \forall k = 1, \ldots, m \quad \sum_{i=1,t=1}^{s,n} \delta_{i,t}^{(j,k)} U_{i,t} = 0.$$

It is a linear system in sn unknowns and $m(n-k)$ equations. Therefore the space of solution has dimension at least $sn - m(n-k)$.

3. Subspace subcodes of Gabidulin codes

In the case where $\mathcal{G} \subset GF(q^m)^n$ is a Gabidulin code, we deduce an upper-bound on the cardinality of subspace subcodes. If $n = m$, we show that subspace subcodes of Gabidulin codes are MRD, and we show how to design specific encoding and decoding algorithms for subspace subcodes of Gabidulin codes.

3.1. Size of subspace subcodes of Gabidulin codes.

Proposition 2. *Let $\mathcal{G}$ be the Gabidulin code over $GF(q^m)$ with parity-check matrix (2.3). Let V_s ($s \leq m$) be an s-dimensional subspace of $GF(q^m)$. We have*

$$q^{ns-m(d-1)} \leq |(\mathcal{G}|V_s)| \leq q^{m(s-d+1)}$$

Proof. The lower bound comes from proposition 1: A Gabidulin code being an MRD-code we have $d-1 = n-k$.

The mapping

$$\begin{array}{ccc} GF(q^m) & \rightarrow & GF(q^m) \\ x & \mapsto & x^{[i]} \end{array}$$

is $GF(q)$-linear. Therefore, solving (2.5) is equivalent to solving

$$(v_1, \ldots, v_s) \underbrace{\begin{pmatrix} \beta_1^{[m]} & \ldots & \beta_1^{[m-d+2]} \\ \vdots & \ddots & \vdots \\ \beta_s^{[m]} & \ldots & \beta_s^{[m-d+2]} \end{pmatrix}}_{\mathbf{H}_{V_s}^T} = \mathbf{0}, \tag{3.7}$$

where $v_1 = \sum_{t=1}^n U_{1,t} h_t, \ldots, v_s = \sum_{t=1}^n U_{s,t} h_t \in GF(q^m)$ are the unknowns. This implies that $(\mathcal{G}|V_s)$ can be regarded as an $GF(q)$-linear subcode of the $[s, s-d+1, d]_r$ Gabidulin code with parity-check matrix $\mathbf{H}_{V_s}$. $\diamond$ □

Definition 4 (Parent Code)**.** *The linear code over $GF(q^m)$ with parity-check matrix $\mathbf{H}_{V_s}$ is called the parent code of $(\mathcal{G}|V_s)$. It is denoted by $\mathcal{P}_{(\mathcal{G}|V_s)}$.*

If $n = m$ both inequalities of proposition 2 match and $|(\mathcal{G}|V_s)| = q^{m(s-d+1)}$. In that case $(\mathcal{G}|V_s)$ is an MRD code. In the following we will suppose that $m = n$.

Proposition 3. *Let $m = n$, let $\mathcal{G} \subset GF(q^n)^n$ be the Gabidulin code with parity-check matrix (2.3). Let $\mathbf{h} = (h_1, \ldots, h_n)$ be the first row. Let V_s be an s-dimensional subspace of $GF(q^n)$ and let $\mathbf{b} = (\beta_1, \ldots, \beta_s)$ be a basis of V_s. The mapping*

$$\begin{array}{rccc} f_{\mathbf{b}}: & V_s^n & \rightarrow & GF(q^n)^s \\ & \mathbf{c} = \mathbf{b}U & \mapsto & f_{\mathbf{b}}(\mathbf{c}) = \mathbf{h}U^T \end{array}$$

satisfies the following properties

1. *$f_{\mathbf{b}}$ is $GF(q)$-linear and bijective*
2. *$f_{\mathbf{b}}$ preserves the rank,* i.e. *$Rk(f_{\mathbf{b}}(\mathbf{c})) = Rk(\mathbf{c})$*
3. *$f_{\mathbf{b}}(\mathcal{G}|V_s) = \mathcal{P}_{(\mathcal{G}|V_s)}$*
4. *$f_{\mathbf{b}}$ can be computed in $\mathcal{O}(sn^2)$ multiplications in $GF(q)$ and $\mathcal{O}(sn)$ additions in $GF(q^n)$*
5. *$f_{\mathbf{b}}^{-1}$ can be computed in $\mathcal{O}(n^3)$ multiplications in $GF(q)$ and $\mathcal{O}(sn)$ additions in $GF(q^n)$*

Proof. 1. Let $\mathbf{d} \in GF(q^n)^s$. Since by construction $\mathbf{h} = (h_1, \ldots, h_n)$ is a basis of $GF(q^n)/GF(q)$, there is a unique q-ary matrix U such that $\mathbf{d} = \mathbf{h}U^T$. Therefore the unique $\mathbf{c} \in V_s^n$ such that $f_{\mathbf{b}}(\mathbf{c}) = \mathbf{d}$ is $\mathbf{c} = \mathbf{b}U$. This proves the bijectivity. $GF(q)$-linearity is immediate.

2. $\mathbf{b} = (\beta_1, \ldots, \beta_s)$ is a basis of V_s. From definition 1 we have $\mathrm{Rk}(\mathbf{c} = \mathbf{b}U) = \mathrm{Rk}(U)$. Moreover, since $f_{\mathbf{b}}(\mathbf{c}) = \mathbf{h}U^T$, and since $h_1, \ldots, h_n$ are linearly independent over $GF(q)$, we have
$$\mathrm{Rk}(f_{\mathbf{b}}(\mathbf{c})) = \mathrm{Rk}(U^T) = \mathrm{Rk}(U) = \mathrm{Rk}(\mathbf{c}).$$
3. Any vector of $(\mathcal{G}|V_s)$ satisfies (2.5) for some q-ary matrix U. Since $\mathcal{G}$ is a Gabidulin code, $\mathbf{v} = (\sum_{t=1}^n U_{1,t}h_t, \ldots, \sum_{t=1}^n U_{s,t}h_t)$ satisfies (3.7). Therefore $\mathbf{v} \in \mathcal{P}_{(\mathcal{G}|V_s)}$. This implies that $f_{\mathbf{b}}(\mathcal{G}|V_s) \subset \mathcal{P}_{(\mathcal{G}|V_s)}$. Since both sets have the same cardinality, then they are equal.
4. A vector of V_s^n is characterised by a unique q-ary $s \times n$ matrix U. Therefore, computing $f_{\mathbf{b}}$ consists of computing the product of $\mathbf{h} = (h_1, \ldots, h_n)$ by U^T (sn^2 multiplications in $GF(q)$ and sn additions in $GF(q^n)$). Conversely, to compute $f_{\mathbf{b}}^{-1}(v_1, \ldots, v_s)$ one needs to
   (a) determine U such that $(v_1, \ldots, v_s) = (h_1, \ldots, h_n)U^T$: By considering the elements of $GF(q^n)$ as q-ary vectors of length n this implies solving a matricial system over $GF(q)$, and this gives a complexity of $\mathcal{O}(n^3)$ multiplications in $GF(q)$.
   (b) compute $\mathbf{b}U$: s^2n multiplications in $GF(q)$ and sn additions in $GF(q^n)$.

◇ □

3.2. Encoding and decoding. The rank preserving isomorphism $f_{\mathbf{b}}$ is the tool for designing encoding and decoding procedures for subspace subcodes.

3.2.1. *Encoding.* From Proposition 2 we encode up to $n(s-d+1)$ q-ary digits with $\mathcal{P}_{(\mathcal{G}|V_s)}$. Let $\mathbf{x} = (x_1, \ldots, x_{s-d+1}) \in GF(q^n)^{s-d+1}$ be an information vector. Let $\mathbf{G}_{V_s}$ be a generator matrix of $\mathcal{P}_{(\mathcal{G}|V_s)}$.

$\mathbf{x}$ is encoded into a codeword $\mathbf{c}$ by a two steps procedure:

1. Compute $\mathbf{y} = \mathbf{x}\mathbf{G}_{V_s}$
2. Compute $\mathbf{c} = f_{\mathbf{b}}^{-1}(\mathbf{y})$

From proposition 3, $\mathbf{c}$ belongs to $(\mathcal{G}|V_s)$. The complexity of the encoding procedure is essentially the complexity of computing $\mathbf{x}\mathbf{G}_{V_s}$ that is: $(s-d+1) \times s$ products in $GF(q^n)$.

3.2.2. *Decoding.* Let $\mathbf{y} = \mathbf{c}+\mathbf{e}$ be a received vector where $\mathbf{c} \in (\mathcal{G}|V_s)$ and $\mathbf{e} \in V_s^n$ is an error-vector of rank $t \leq \lfloor (d-1)/2 \rfloor$. From proposition 3, we deduce
$$f_{\mathbf{b}}(\mathbf{y}) = f_{\mathbf{b}}(\mathbf{c}) + f_{\mathbf{b}}(\mathbf{e}),$$
and $\mathrm{Rk}(f_{\mathbf{b}}(\mathbf{e})) = t$. The decoding procedure is:

1. Decode $f_{\mathbf{b}}(\mathbf{y})$ in $\mathcal{P}_{(\mathcal{G}|V_s)}$ and recover $\mathbf{c}' \in \mathcal{P}_{(\mathcal{G}|V_s)}$ and $\mathbf{e}'$ such that $f_{\mathbf{b}}(\mathbf{y}) = \mathbf{c}' + \mathbf{e}'$.
2. Compute $\mathbf{c} = f_{\mathbf{b}}^{-1}(\mathbf{c}')$ and $\mathbf{e} = f_{\mathbf{b}}^{-1}(\mathbf{e}')$.

It is the decoding step of a Gabidulin code which has the main contribution for the evaluation of the complexity. Therefore it strongly depends on the chosen decoding algorithm. For instance if we use the one described in [9], where $2t = d-1$ then the complexity is roughly equal to $t(2s+n+t^2)$ products in $GF(q^n)$. If we use the algorithm in [16] the complexity is $s^2 - 5st + 6t^2$ products in $GF(q^n)$.

4. Direct sum of subspace subcodes

For $i = 1, \ldots, u$, let $1 \leq s_i \leq n$ and let V_{s_i} be an s_i-dimensional subspace of $GF(q^n)$ over $GF(q)$. We suppose that
$$\forall i, j = 1, \ldots, s_u, \quad i \neq j, \quad V_{s_i} \cap V_{s_j} = \{0\}.$$
It implies that $\sum_{i=1}^u s_i \leq n$. For all $i = 1, \ldots, u$, let $\mathbf{b}_i$ be a basis of V_{s_i} and let $f_{\mathbf{b}_i}$ be the associated mappings defined in proposition 3. We define
$$\begin{array}{rccl} f_{(\mathbf{b}_1,\ldots,\mathbf{b}_u)}: & V_{s_1}^n \oplus \cdots \oplus V_{s_u}^n & \to & GF(q^n)^{s_1+\cdots+s_u} \\ & \mathbf{c} = \mathbf{c}_1 + \cdots + \mathbf{c}_u & \mapsto & f_{(\mathbf{b}_1,\ldots,\mathbf{b}_u)}(\mathbf{c}) = (f_{\mathbf{b}_1}(\mathbf{c}_1), \ldots, f_{\mathbf{b}_u}(\mathbf{c}_u)) \end{array}$$

Let $\mathcal{M} = (\mathcal{G}|V_{s_1}) \oplus \cdots \oplus (\mathcal{G}|V_{s_u})$. $\mathcal{M}$ is a $GF(q)$-linear subcode of $\mathcal{G}$. For all $i = 1, \ldots, u$, let $\mathbf{H}_{V_{s_i}}$ be the matrix given by (3.7). Let $\mathcal{P}_{\mathcal{M}}$ be the $[\sum_{i=1}^{u} s_i, \sum_{i=1}^{u} (s_i - d + 1), d]_r$-code over $GF(q^n)$ with parity-check matrix

$$\mathbf{H}_{\mathcal{M}} = \begin{pmatrix} \mathbf{H}_{V_{s_1}} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \mathbf{H}_{V_{s_u}} \end{pmatrix}. \tag{4.8}$$

From proposition 3 we have

PROPOSITION 4.

1. $f_{(\mathbf{b}_1,\ldots,\mathbf{b}_u)}$ *is* $GF(q)$*-linear, bijective and preserves the rank.*
2. $f_{(\mathbf{b}_1,\ldots,\mathbf{b}_u)}(\mathcal{M}) = \mathcal{P}_{\mathcal{M}}$.

The code $\mathcal{P}_{\mathcal{M}}$ is called parent code of $\mathcal{M}$. From the structure of matrix (4.8) it is clear that $\mathcal{P}_{\mathcal{M}}$ is the direct product of Gabidulin codes over $GF(q^n)$ with parameters $[s_i, s_i - (d-1), d]_r$ for $i = 1, \ldots, u$. We deduce the following corollary

COROLLARY 1. $\mathcal{M}$ *is a* $(n, M, D)_r$ *additive code, where*

- $M = q^{n \sum_{i=1}^{u} (s_i - (d-1))}$.
- $D = d$.

4.1. ENCODING WITH $\mathcal{M}$. Let $\mathbf{x}$ be a q^n-ary vector of length $\sum_{i=1}^{u} s_i - u(d-1)$.

1. Write $\mathbf{x} = (\mathbf{x}_1, \ldots, \mathbf{x}_u)$ where, for all $i = 1, \ldots, u$, $\mathbf{x}_i$ has length $s_i - d + 1$.
2. For $i = 1, \ldots, u$, $\mathbf{x}_i$ is encoded into $\mathbf{c}_i \in (\mathcal{G} \mid V_{s_i})$, using the procedure described in section 3.2 with mapping $f_{\mathbf{b}_i}$.
3. The encoded codeword is $\mathbf{c} = \mathbf{c}_1 + \cdots + \mathbf{c}_u \in \mathcal{M}$.

The complexity of the encoding procedure is equal to $\sum_{i=1}^{u} s_i(s_i - d + 1)$ products in $GF(q^n)$.

4.2. DECODING IN $\mathcal{M}$. Suppose the receiver gets $\mathbf{y} \in GF(q^n)^n$, where

$$\mathbf{y} = \underbrace{\mathbf{c}}_{\in \mathcal{M}} + \mathbf{e} \in V_{s_1}^n \oplus \cdots \oplus V_{s_u}^n$$

For all $i = 1, \ldots, u$, let $\mathbf{y}_i$ be the projection of $\mathbf{y}$ onto V_{s_i}. We have

$$\begin{cases} \mathbf{y}_1 = \mathbf{c}_1 + \mathbf{e}_1, \text{ where } \mathbf{c}_1 \in (\mathcal{G}|V_{s_1}), \\ \vdots \\ \mathbf{y}_u = \mathbf{c}_u + \mathbf{e}_u, \text{ where } \mathbf{c}_u \in (\mathcal{G}|V_{s_u}). \end{cases}$$

If for all $i = 1, \ldots, u$, $\mathbf{e}_i$ has rank less than $C \stackrel{def}{=} \lfloor (d-1)/2 \rfloor$, $\mathbf{y}$ can be decoded in polynomial time. Namely, for $i = 1, \ldots, u$, it suffices to decode $\mathbf{y}_i$ in $(\mathcal{G}|V_{s_i})$ with the decoding procedure described in section 4.2.

Furthermore some error-patterns $\mathbf{e}$ of rank larger than C can be also decoded with the same algorithms. Namely, if

$$\begin{cases} \mathrm{Rk}(\mathbf{e}) > C, \\ \forall i = 1, \ldots, u, \ \mathrm{Rk}(\mathbf{e}_i) \leq C. \end{cases}$$

Then it is clear that $\mathbf{e}$ can be recovered in polynomial time. This increases the number of correctable patterns by a factor that we want to evaluate.

Let $\mathcal{N}_C(n, s)$ be the number of error-patterns of V_s^n and of rank less than C. We have, see [14] page 455

$$\mathcal{N}_C(n, s) = \sum_{j=0}^{C} \prod_{i=0}^{j-1} \frac{(q^n - q^i)(q^s - q^i)}{q^C - q^i}.$$

This quantity is lower and upper bounded by

$$q^{(n+s-1)C - C^2} \leq \mathcal{N}_C(n, s) \leq q^{(n+s+1)C - C^2 + 1}$$

Let $N \stackrel{def}{=} \sum_{i=1}^{u} s_i$. We have

- The number $\mathcal{N}$ of error-patterns of length n over $V_{s_1} \oplus \cdots \oplus V_{s_u}$ and of rank less than C satisfies
$$q^{(n+N-1)C-C^2} \leq \mathcal{N} \leq q^{(n+N+1)C-C^2+1}$$
- The number $\mathcal{N}'$ of error-vectors that can be corrected in polynomial-time is equal to the number of vectors $\mathbf{e} = \sum_{i=1}^{u} \mathbf{e}_i$ of length n such that for all $i = 1, \ldots, u$ $\mathrm{Rk}(\mathbf{e}_i) \leq C$ satisfies
$$q^{(un+N-u)C-uC^2} \leq \mathcal{N}' = \prod_{i=1}^{u} \mathcal{N}_C(n, s_u) \leq q^{(un+N+u)C-uC^2+u}$$
- A Gabidulin code with the same length and cardinality has minimum rank distance $D = u(d-1)+1$. It corrects error-patterns of rank between uC and $(u+1)C$ according to the parity of $d-1$. The number $\mathcal{N}_{Gab}$ of correctable error-patterns therefore satisfies
$$q^{(n+N-1)uC-(uC)^2} \leq \mathcal{N}_{Gab} \leq q^{(n+N+u)(u+1)C-(u+1)^2C^2+1}$$

Example. Let $\mathcal{C}$ be a $(20, 2^{240}, 5)_r$ additive code over $GF(2^{20})$, and let $\mathcal{M}$ be a $(20, 2^{240}, 5)_r$-code obtained from a parent code with parameters $[20, 16, 5]_r$ over $GF(2^{20})$, and $u = 2,\ s_1 = 10,\ s_2 = 10$. Then

- The number $\mathcal{N}$ of correctable error patterns in $\mathcal{C}$ satisfies
$$2^{74} \leq \mathcal{N} \leq 2^{79}$$
- The number $\mathcal{N}'$ or correctable error patterns in $\mathcal{M}$ satisfies
$$2^{108} \leq \mathcal{N}' \leq 2^{116}$$

A Gabidulin code with the same length and cardinality has a minimum rank distance $D = 9$. Therefore it can correct a number $\mathcal{N}_{Gab}$ of error-patterns bounded by
$$2^{140} \leq \mathcal{N}_{Gab} \leq 2^{149}$$

Although the number of polynomial-time correctable error-patterns remains lower than for a Gabidulin code with same length and cardinality, our construction enables to correct significantly more error-patterns than for a code with same parameters but without the direct sum structure.

5. A particular case: subfield subcodes

When the subspace V_s is the field $GF(q^s)$ the results of the previous sections can be extended. We prove the following result: Given $GF(q^s) \subset GF(q^n)$ and a parity-check matrix of a $[s, k', d]_r$ Gabidulin code over $GF(q^s)$, the subfield subcode restricted to $GF(q^s)$ of a $[n, k, d]_r$ Gabidulin code over $GF(q^n)$ and minimum rank distance d is uniquely characterised by an element of the general linear group $GL_n(GF(q))$.

More precisely:

Proposition 5.
Let $\mathcal{G}$ be the code over $GF(q^n)$ with parity-check matrix (2.3), Let $s|n$ 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 $a_i \in GF(q^s) \subset GF(q^n)$ for all $i = 1, \ldots, s$, are $GF(q)$-linearly independent. Then, there exists a unique *matrix $S \in GL_n(GF(q))$ such that $(\mathcal{G}|GF(q^s))$ has parity-check matrix*
$$\mathbf{H}_{q^s} = \begin{pmatrix} A & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & A \end{pmatrix} S,$$

Proof.
Let $\mathbf{h}$ denote the first row of matrix $\mathbf{H}$ given by (2.3). It can be rewritten

$$\mathbf{H} = \begin{pmatrix} \mathbf{h} \\ \vdots \\ \mathbf{h}^{[d-2]} \end{pmatrix}$$

where $\mathbf{h}^{[i]} \stackrel{def}{=} \left(h_1^{[i]}, \ldots, h_n^{[i]}\right)$. Trivially a parity-check matrix of $(\mathcal{G}|GF(q^s))$ can be obtained by:

1. Choosing a basis of $GF(q^n)/GF(q^s)$.
2. Expanding the rows of $\mathbf{H}$ columnwise with respect to the chosen basis: A row of length n with coefficients in $GF(q^n)$ is transformed into a matrix of size $n/s \times n$ with coefficients in $GF(q^s)$, that is

$$\mathbf{h} = (h_1, \ldots, h_n) \mapsto \mathcal{H} = \begin{pmatrix} h_{1,1} & \cdots & h_{1,n} \\ \vdots & \ddots & \vdots \\ h_{n/s,1} & \cdots & h_{n/s,n} \end{pmatrix}$$

Since the rows of $\mathbf{H}$ are the $\mathbf{h}^{[i]}$ for $i = 0, \ldots, d-2$, there exists a $n/s \times n/s$ non-singular q^s-ary matrix Q_i satisfying

$$\mathbf{h}^{[i]} = (h_1^{[i]}, \ldots, h_n^{[i]}) \mapsto Q_i \mathcal{H}^{[i]},$$

where $\mathcal{H}^{[i]}$ denotes matrix $\mathcal{H}$ whose components have been elevated to the power $[i]$. Therefore, there exists a parity-check matrix of $(\mathcal{G}|GF(q^s))$ which has the form

$$\mathbf{H}_{q^s} = \begin{pmatrix} \mathcal{H} \\ \vdots \\ \mathcal{H}^{[d-2]} \end{pmatrix}.$$

The h_i's being by definition linearly independent over $GF(q)$), then the columns of $\mathcal{H}$ are vectors of rank n/s. Hence, there is a $n \times n$ matrix S with coefficients in $GF(q)$ such that

$$\mathcal{H} = \begin{pmatrix} \mathbf{a} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \mathbf{a} \end{pmatrix} S,$$

where $\mathbf{a} \stackrel{def}{=} (a_1, \ldots, a_s) \in GF(q^s)^s$. Let

$$\mathcal{A} = \begin{pmatrix} \mathbf{a} \\ \vdots \\ \mathbf{a}^{[d-2]} \end{pmatrix},$$

There exists a permutation matrix P such that

$$\mathbf{H}_{q^s} = \begin{pmatrix} \mathcal{H} \\ \vdots \\ \mathcal{H}^{[d-2]} \end{pmatrix} = P \begin{pmatrix} \mathcal{A} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \mathcal{A} \end{pmatrix} S$$

Multiplying a parity-check matrix on the left by a non-singular matrix generates the same code. A parity-check of $(\mathcal{G}|GF(q^s))$ is therefore given by

$$\begin{pmatrix} \mathcal{A} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \mathcal{A} \end{pmatrix} S$$

◇ □

<gab@pop3.mipt.ru ; Pierre.Loidreau@univ-rennes1.fr>

References

[1] T. P. Berger and P. Loidreau. How to mask the structure of codes for a cryptographic use. *Designs, Codes and Cryptography*, 35:63–79, 2005.

[2] J. Bierbrauer and Y. Edel. New code parameters from Reed-Solomon subfield subcodes. *IEEE Transactions on Information Theory*, 43(3):953–968, May 1997.

[3] M. Blaum, P. G. Farrell, and H. C. A. van Tilborg. *Handbook of Coding Theory, Vol. II*, chapter 22, pages 1855–1910. North–Holland, 1998.

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

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

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

[9] 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, 1991.

[10] E. M. Gabidulin and P. Loidreau. On subcodes of codes in rank metric. In *2005 IEEE International Symposium on Information Theory, ISIT'05*, pages 121–123, September 2005.

[11] E .M. Gabidulin, A. V. Paramonov, and O. V. Tretjakov. Ideals over a non-commutative ring and their application in cryptology. In D. W. Davies, editor, *Advances in Cryptology - EUROCRYPT'91*, volume 547 of *LNCS*, pages 482–489. Springer, 1991.

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

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

[14] R. Lidl and H. Niederreiter. *Finite Fields*. Cambridge University Press, 2 edition, 1997.

[15] P. Loidreau. Sur la reconstruction des polynÃ´mes linÃ©aires : un nouvel algorithme de dÃ©codage des codes de Gabidulin. *Comptes Rendus de l'AcadÃ©mie des Sciences : SÃ©rie I*, 339(10):745–750, 2004.

[16] P. Loidreau. A Welch-Berlekamp like algorithm for decoding Gabidulin codes. In Ø. Ytrehus, editor, *Coding and Cryptography - WCC 2005, 4th International workshop on Coding and Cryptography*, number 3969 in LNCS, pages 36–45. Springer, 2006.

[17] 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.

[18] R. J. McEliece and G. Solomon. Trace-shortened Reed–Solomon codes. Technical Report 42-117, TDA Progress Report, May 1994.

[19] 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.

[20] 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.

[21] R. Overbeck. A new structural attack for GPT and variants. In E. Dawson and S. Vaudenay, editors, *Proceedings of MyCrypt 2005*, volume 3715 of *LNCS*, pages 50–63. Springer, 2005.

[22] R. Overbeck. Structural attacks for public-key cryptosystems based on gabidulin codes. *Journal of Cryptology*, 2007.

[23] G. Richter and S. Plass. Fast decoding of rank-codes with rank errors and column erasures. In *2004 IEEE International Symposium on Information Theory, ISIT'04*, 2004.

[24] 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.

[25] D. Silva, F. R. Kschischang, and R. Koetter. A rank metric approach to error control in random network coding. In *IEEE Information Theory Workshop*, July 2007.

[26] G. Solomon. Nonlinear, nonbinary cyclic group codes. Technical Report 42-108, TDA Progress Report, February 1992.

[27] H. Stichtenoth. On the dimension of subfield subcodes. *IEEE Transactions on Information Theory*, 36, 1990.