On the decoding of the sum of Gabidulin codes

Pierre Loidreau, Pham Ba Duc

On the decoding of the sum of Gabidulin codes

Pham Ba Duc
University Rennes1
Email: ba-duc.pham@univ-rennes1.fr

Pierre Loidreau
University Rennes 1
Email: pierre.loidreau@univ-rennes1.fr

***Abstract*—We investigate the decoding of the sum of Gabidulin codes. We show that there exists a probabilistic polynomial-time decoder up to some bound. We then give some potential applications of constructing and decoding a sum of Gabidulin codes. This approach can lead to a new insight in designing rank-metric based cryptographic schemes.**

I. Introduction

There are very few families of decodable codes in rank metric. Namely, the family of trivial codes [1], the family of Gabidulin codes [2], and the family of LRPC codes [3]. Apart from that, there are codes derived from Gabidulin codes that are used in [4]. These codes are masked versions of Gabidulin codes, enabling to design public-key encryption schemes.

The problem that we investigate in this paper is the problem of decoding the sum of Gabidulin codes. Interestingly enough, this is a problem which appears when one analyzes cryptosystems based on the problem of reconstructing linearized polynomials, [5], [6].

We show that the formulation of this problem can give some insight in decoding problems and give rise to further understanding on how to design public-key cryptosystems.

In the first section, we introduce notations and especially the notion of skew polynomial rings which are an elegant and simple manner to deal algebraically with rank metric and Gabidulin codes. Under this setting, Gabidulin codes are just the evaluation codes of bounded degree skew polynomials using the operator evaluation.

Then, we state the problem of decoding the sum of Gabidulin codes and show that there is a simple probabilistic polynomial-time decoder up to some bound. Under some assumptions, we show that the failure probability of this algorithm is exponentially small.

Finally, we present some potential applications. We show that by considering a random k-dimensional code as the sum of k 1-dimensional Gabidulin codes, we recover the result of [7] for the decoding of random codes. We also show that investigating properties of the sum of Gabidulin codes could be of interest in designing and analyzing rank metric based public-key cryptography based on algebraic decoding.

II. Preliminaries and notations

Let q be a power of a prime and let $\mathbb{F}_q$ denote the finite field of order q. We consider the finite field extension of degree m: $\mathbb{F}_{q^m}/\mathbb{F}_q$.

We use $\mathbb{F}_q^{m\times n}$ to denote the set of all $m \times n$ matrices over $\mathbb{F}_q$ and $\mathbb{F}_{q^m}^n$ for the set of all row vectors of length n over $\mathbb{F}_{q^m}$.

Let θ be a generator of the Galois group. For instance, it could be the mapping $x \mapsto x^q$, but everything we write stays true for any generator of the Galois group. Moreover, for simplicity, we denote by $x^{[i]}$ the value $\theta^i(x)$.

In this setting, we define the skew polynomial ring or Ore ring [8] denoted by $\mathbb{F}_{q^m}[X;\theta]$ by defining the usual operations

- Addition is classical addition;
- $X \cdot a = \theta(a) \cdot X$.

With these operations, this ring is left and right Euclidean. We denote by $P\langle X\rangle = \sum_{i=0}^{\ell} p_i X^i$ any element P of $\mathbb{F}_{q^m}[X;\theta]$ of degree ℓ to distinguish it from the usual polynomial ring.

There are several ways to define an evaluation map on this ring [9]. Here, we choose the so-called operator evaluation, meaning that for any α in some finite field where the action θ is meaningful (for instance any finite field with the same characteristic as $\mathbb{F}_q$), we have

$$\forall P \in \mathbb{F}_{q^m}[X;\theta], \quad P\langle\alpha\rangle \stackrel{def}{=} \sum_{i=0}^{\ell} p_i \theta^i(\alpha).$$

If θ corresponds to the Frobenius automorphism, then this evaluation corresponds to the evaluation of so-called ring of linearized polynomials defined in [9]. We naturally extend the notion of evaluation to a vector :

$$\forall \boldsymbol{y} = (y_1, \ldots, y_n), \quad P\langle \boldsymbol{y}\rangle = (P\langle y_1\rangle, \ldots, P\langle y_n\rangle).$$

Let $\boldsymbol{M}$ be a matrix over $\mathbb{F}_{q^m}$, we denote by $\mathrm{rk}_{q^m}(\boldsymbol{M})$ its rank over $\mathbb{F}_{q^m}$. Rank metric is naturally related to the evaluation of skew polynomials. Namely, let $\boldsymbol{y} = (y_1, \ldots, y_n) \in \mathbb{F}_{q^m}^n$, then by definition the rank of $\boldsymbol{y}$ is the dimension of the $\mathbb{F}_q$-vector space generated by its components, *i.e.*

$$\mathrm{rk}_q(\boldsymbol{y}) = \dim(\langle y_1, \ldots, y_n\rangle_q).$$

Theorem 1 ([10]): Let $\boldsymbol{y} = (y_1, \ldots, y_n) \in \mathbb{F}_{q^m}^n$, then if $\mathrm{rk}_q(\boldsymbol{y}) = t$, there exist a unique $A_{\boldsymbol{y}} \in \mathbb{F}_{q^m}[X;\theta]$, monic of degree t such that $A_{\boldsymbol{y}}\langle \boldsymbol{y}\rangle = 0$.

In this setting, Gabidulin codes are defined as evaluation codes of skew polynomials over linearly independent elements.

Definition 1 ([2], [11]): Let $\boldsymbol{g} = (g_1, \ldots, g_n) \in \mathbb{F}_{q^m}^n$, formed with $\mathbb{F}_q$-linearly independent elements. The Generalized Gabidulin code of dimension k and of support $\boldsymbol{g}$ denoted by $\mathcal{G}_k(\boldsymbol{g})$ is defined by

$$\mathcal{G}_k(\boldsymbol{g}) = \left\{ f\langle \boldsymbol{g} \rangle, \quad \begin{array}{l} f \in \mathbb{F}_{q^m}[X;\theta] \\ \deg(f) \leq k-1 \end{array} \right\}.$$

In the following, and since we are in finite fields we will simply call them Gabidulin codes rather than Generalized Gabidulin codes.

III. Decoding of the sum of Gabidulin codes

Let $\{\mathcal{G}_{k_j}(\boldsymbol{g}_j) \subset \mathbb{F}_{q^m}^n\}_{j=1}^{\ell}$ be a set of k_j-dimensional Gabidulin codes with support vectors $\boldsymbol{g}_j$. We define by

$$\mathcal{C} = \sum_{j=1}^{\ell} \mathcal{G}_{k_j}(\boldsymbol{g}_j)$$

the code formed with the sum of the Gabidulin codes and k, d_{min} be the dimension and the minimum distance of the code $\mathcal{C}$. To be convenient, we denote $k_a := \sum_{j=1}^{\ell} k_j$.

Our goal is to study in which case we can decode it and up to which bound in the rank metric.

A. Problem

The decoding problem we address is the following: Let

$$\boldsymbol{y} = \mathbf{c} + \mathbf{e}$$

where $\mathbf{c} \in \mathcal{C}$ and $\mathbf{e}$ has rank t. This implies that

- There exists skew polynomials $f_j \in \mathbb{F}_{q^m}[X;\theta]$ with degree $\leq k_j - 1$, such that

$$\mathbf{c} = \sum_{j=1}^{\ell} f_j \langle \boldsymbol{g}_j \rangle.$$

- There exists a unique skew polynomial $A_{\mathbf{e}} \in \mathbb{F}_{q^m}[X;\theta]$, monic and of degree t such that $A_{\mathbf{e}}\langle \mathbf{e} \rangle = 0$

From the $\mathbb{F}_q$-linearity of the evaluation of skew polynomials, we can rewrite the decoding problem as follows:

$$A_{\mathbf{e}}\langle \boldsymbol{y} \rangle = \sum_{j=1}^{\ell} (A_{\mathbf{e}} \cdot f_j)\langle \boldsymbol{g}_j \rangle. \tag{1}$$

The unknowns of the system are the coefficients of the skew polynomials. Hence, we obtain a non homogenous bivariate system with $t + k_a + 1$ unknowns and n equations.

A way to decode would then be to homogeneize the system and solve it by using Gröbner bases, but this is not the direction we investigate. As in [12], [13], we prefer to linearize the system and understand when the solution space is 1-dimensional to relate it directly to the decoding of $\mathcal{C}$.

B. Linearizing the problem

We now consider the following system:

$$A\langle \boldsymbol{y} \rangle = \sum_{j=1}^{\ell} N_j \langle \boldsymbol{g}_j \rangle. \tag{2}$$

where A has degree t and for $j \in \{1, \ldots, \ell\}$, $\deg(N_j) \leq t + k_j - 1$. The number of equations is equal to n and the number of variables can be counted as follows:

- $t + 1$ variables to characterize the skew polynomial A;
- $\ell t + k_a$ to characterize the polynomials N_j.

Hence, the number of variables is $(\ell+1)t + k_a + 1$. In case $(\ell+1)t + k_a < n$, this implies that the matrix of the system is degenerate, and the solution space often is of small dimension, typically 1.

We can relate the solutions of system (1) and (2) by the following immediate theorem.

Theorem 2: Let $(f_1, \ldots, f_\ell, A)$ be a solution of (1) then $(A \cdot f_1, \ldots, A \cdot f_\ell, A)$ is a solution to (2)

This theorem is a straightforward generalization of the systems written for the Welch-Berlekamp decoding algorithm [12], [13]. More precisely, we can prove the following theorem

Theorem 3: Let $\boldsymbol{y} \in \mathbb{F}_{q^m}^n$. Let

$$\mathcal{L}_{\boldsymbol{y},t}(\mathcal{C}) = \{(\boldsymbol{c}_i, \boldsymbol{e}_i) \mid \boldsymbol{y} = \boldsymbol{c}_i + \boldsymbol{e}_i,\ \boldsymbol{c}_i \in \mathcal{C}, \mathrm{rk}_q(\boldsymbol{e}_i) \leq t\}.$$

If the solution space of (2) is 1-dimensional, then there is at most one element in $\mathcal{L}_{\boldsymbol{y},t}(\mathcal{C})$. Moreover, any non zero solution $(A, N_1, \ldots, N_\ell)$ of the system provides the same solution $(A, A\backslash N_1, \ldots, A\backslash N_\ell)$ to (1), where $A\backslash N$ denotes the left Euclidean division of N by A in $\mathbb{F}_{q^m}[X;\theta]$.

This gives a natural decoding algorithm consisting in enumerating the solution space of system (2). Let d be the dimension of this solution space this gives a list decoding algorithm recovering $\mathcal{L}_{\boldsymbol{y},t}$ with complexity

$$\mathcal{O}\left(P(n,m)q^{m(d-1)}\right),$$

where P is a polynomial of degree at most 3. The exponent is $d-1$ and not d since we only need to enumerate the 1-dimensional vector spaces and not all the elements in the solution space. Namely, we need to enumerate the solution space of the linear system, and then perform the left Euclidean division in $\mathbb{F}_{q^m}[X;\theta]$ corresponding to the linear algebra operations.

Corollary 1: A necessary condition for the dimension of solution space of the system (1) to be ≤ 1 is

$$(\ell+1)t + k_a < n.$$

Proof: Suppose that $|\mathcal{L}_{\boldsymbol{y},t}(\mathcal{C})| \geq 2$. Let $(\boldsymbol{c}_1, \boldsymbol{e}_1)$ and $(\boldsymbol{c}_2, \boldsymbol{e}_2)$ be two distinct elements of $\mathcal{L}_{\boldsymbol{y},t}(\mathcal{C})$. Then they respectively correspond to solutions $(A_{\boldsymbol{e}_1}, f_1, \ldots, f_\ell)$ and $(A_{\boldsymbol{e}_2}, h_1, \ldots, h_\ell)$ of (1). Therefore $(A_{\boldsymbol{e}_1}, A_{\boldsymbol{e}_1} \cdot f_1, \ldots, A_{\boldsymbol{e}_1} \cdot f_\ell)$ and $(A_{\boldsymbol{e}_2}, A_{\boldsymbol{e}_2} \cdot h_1, \ldots, A_{\boldsymbol{e}_2} \cdot h_\ell)$ are solutions of (2) . From the hypothesis that the solution vector space is 1-dimensional,

and the fact that $A_{\boldsymbol{e}_1}$ and $A_{\boldsymbol{e}_2}$ are monic, this implies that $A_{\boldsymbol{e}_1} = A_{\boldsymbol{e}_2}$, and that any solution has the form

$$\alpha \cdot (A_{\boldsymbol{e}_1}, A_{\boldsymbol{e}_1} \cdot f_1, \ldots, A_{\boldsymbol{e}_1} \cdot f_\ell),\ \alpha \in \mathbb{F}_{q^m}$$

■

C. Discussion on the failure probability

In this section, we investigate the failure probability, that is we consider that we are in the conditions of Corollary 1, where $(\ell+1)t + k_a < n$ and where the solution space of (2) has dimension $d \geq 2$. This corresponds to the case where the decoding cannot be completed in polynomial-time.

As in [14], we define the operator λ_t which map a matrix $\boldsymbol{M} = (m_{ij}) \in \mathbb{F}_{q^m}^{s\times n}$ to a block matrix:

$$\begin{array}{rccc} \lambda_t: & \mathbb{F}_{q^m}^{s\times n} & \to & \mathbb{F}_{q^m}^{s(t+1)\times n} \\ & \boldsymbol{M} & \mapsto & \begin{pmatrix} \boldsymbol{M} \\ \vdots \\ \boldsymbol{M}^{[t]} \end{pmatrix}, \end{array}$$

where $\boldsymbol{M}^{[u]} := (\theta^u(m_{ij}))$. Let $(A, N_1, \ldots, N_\ell) \in \mathbb{F}_{q^m}[X;\theta]$ be a solution to the linear system (2). We now identify any polynomial in $\mathbb{F}_{q^m}[X;\theta]$ with the vector formed by its coefficients. Then solving (2) is equivalent to solving the following linear system

$$\boldsymbol{M} \cdot \begin{pmatrix} -A \\ N_1 \\ \vdots \\ N_\ell \end{pmatrix} = 0,$$

where $\boldsymbol{M} = (\lambda_t(\boldsymbol{y})^\top, \lambda_{t+k_1-1}(\boldsymbol{g}_1)^\top, \cdots, \lambda_{t+k_\ell-1}(\boldsymbol{g}_\ell)^\top)$.

The matrix $\boldsymbol{M}$ is $n \times ((\ell+1)t + k_a + 1)$ - matrix in $\mathbb{F}_{q^m}$. Its kernel $\ker(\boldsymbol{M})$ is the solution space of (2). From our hypotheses, the dimension of $\ker(\boldsymbol{M})$ is at least 1. A necessary condition to be able to decode in polynomial-time is that $\dim\ker(\boldsymbol{M})$ is exactly 1.

We need to compute the probability of non-unique decoding $\mathcal{P}(|\mathcal{L}_{\boldsymbol{y},t}(\mathcal{C})| > 1) = \mathcal{P}(\dim\ker(\boldsymbol{M}) > 1)$. By the rank-nullity theorem, $\dim\ker(\boldsymbol{M}) + \mathrm{rk}_{q^m}(\boldsymbol{M}) = (\ell+1)t + k_a + 1$. If the dimension of the solution space is greater than 1, then $\mathrm{rk}_{q^m}(\boldsymbol{M}) < (\ell+1)t + k_a$.

Let $\mathcal{M}$ be the set of all $n \times ((\ell+1)t + k_a + 1)$ - matrices in $\mathbb{F}_{q^m}$ of the form

$$\left(\lambda_t(\boldsymbol{g}_0)^\top, \lambda_{t+k_1-1}(\boldsymbol{g}_1)^\top, \cdots, \lambda_{t+k_\ell-1}(\boldsymbol{g}_\ell)^\top\right).$$

Let us also define $\mathcal{A}$ as the set of all $n \times (\ell+1)$ - matrices in $\mathbb{F}_{q^m}$ of the form

$$\left(\boldsymbol{g}_0^\top, \boldsymbol{g}_1^\top, \ldots, \boldsymbol{g}_\ell^\top\right)$$

such that $\boldsymbol{g}_0, \boldsymbol{g}_1, \ldots, \boldsymbol{g}_\ell \in \mathbb{F}_{q^m}^n$ and $\forall j \in \{1, \ldots, \ell\}, \mathrm{rk}(\boldsymbol{g}_j) = n$. Given a set of integers $(k_0 = 1, k_1, \ldots, k_\ell)$, we define the following bijection

$$\begin{array}{rccc} \varphi: & \mathcal{A} & \to & \mathcal{M} \\ & \left(\boldsymbol{g}_0^\top, \ldots, \boldsymbol{g}_\ell^\top\right) & \mapsto & \left(\lambda_{t+k_0-1}(\boldsymbol{g}_0)^\top, \ldots, \lambda_{t+k_\ell-1}(\boldsymbol{g}_\ell)^\top\right) \end{array}$$

Theorem 4: For $\boldsymbol{A}$ is chosen uniformly from $\mathcal{A}$, and $\boldsymbol{M} = \varphi(\boldsymbol{A})$ of rank r, then

$$\mathcal{P}_{\mathcal{A}}\left[r < (\ell+1)t + k_a\right] \leq \frac{\binom{n}{r+1}4^\ell}{q^{2m}} \leq \frac{1}{q^m}.$$

Proof: Let

$$\mathcal{S} := \{\boldsymbol{h} \in \mathbb{F}_{q^m}^n | \boldsymbol{h} \text{ has } n-(r+1) \text{ coordinates } 0\}$$

Since $r < (\ell+1)t + k_a$, there exists $\boldsymbol{h} \in \mathcal{S}$ such that $\boldsymbol{h}\boldsymbol{M} = 0$. Thus, for $j \in \{0, \ldots, \ell\}$,

$$\lambda_{t+k_j-1}(\boldsymbol{g}_j)\boldsymbol{h}^\top = 0. \tag{3}$$

This in particular implies that $\boldsymbol{h} \in \bigcap_{j=1}^{\ell} \mathcal{G}^\perp_{t+k_j-1}(\boldsymbol{g}_j)$. Therefore $\mathrm{rk}_q(\boldsymbol{h}) \geq t + k_{\max}$ where $k_{\max} := \max\{k_j\}$. Let

$$\mathcal{A}_{\boldsymbol{h}} = \{\boldsymbol{A} \in \mathcal{A} \mid \boldsymbol{h}\varphi(\boldsymbol{A}) = 0\}.$$

We determine the probability that for a fixed $\boldsymbol{h} \in \mathcal{S}$ with $\mathrm{rk}_q(\boldsymbol{h}) \geq t + k_{\max}$, there exists $\boldsymbol{A} \in \mathcal{A}_{\boldsymbol{h}}$. This probability will be $\frac{|\mathcal{A}_{\boldsymbol{h}}|}{|\mathcal{A}|}$. Then,

$$\mathcal{P}_{\mathcal{A}}\left[r < (\ell+1)t + k_a\right] \leq \frac{1}{q^m - 1} \sum_{\boldsymbol{h}\in\mathcal{S}, \mathrm{rk}_q(\boldsymbol{h}) \geq t+k_{\max}} \frac{|\mathcal{A}_{\boldsymbol{h}}|}{|\mathcal{A}|}. \tag{4}$$

The term $1/(q^m-1)$ comes from the fact that for any vector $\boldsymbol{h} \in \mathcal{S}$, and for any $\alpha \in \mathbb{F}_{q^m} \setminus \{0\}$, we have $\mathcal{A}_{\boldsymbol{h}} = \mathcal{A}_{\alpha\boldsymbol{h}}$. For a given $\boldsymbol{h} \in \mathcal{S}$, we now look at the cardinality of $\mathcal{A}_{\boldsymbol{h}}$. Now, let $\boldsymbol{A} \in \mathcal{A}_{\boldsymbol{h}}$, this implies that $\lambda_{t+k_j-1}(\boldsymbol{g}_j)\boldsymbol{h}^\top = 0$, for $j \in \{0, \ldots, \ell\}$. In particular, this implies

$$\forall i \in \{0, \ldots, t + k_j - 1\}, \quad \boldsymbol{g}_j^{[i]}\boldsymbol{h}^\top = 0.$$

Therefore, by applying the inverse of θ a sufficient number of times, we obtain

$$\forall i \in \{0, \ldots, t + k_j - 1\}, \boldsymbol{g}_j(\boldsymbol{h}^{[-i]})^\top = 0.$$

Now let $\boldsymbol{h}_j := \boldsymbol{h}^{[-(t+k_j-1)]}$, then

$$\forall i \in \{0, \ldots, t + k_j - 1\}, \boldsymbol{g}_j(\boldsymbol{h}_j^{[i]})^\top = 0.$$

It implies that $\lambda_{t+k_j-1}(\boldsymbol{h}_j)\boldsymbol{g}_j^\top = 0$. We need the following lemma:

Lemma 1 (Lemma 3.51 [15]): Given $\boldsymbol{g} \in \mathbb{F}_{q^m}^n$ then $\mathrm{rk}_{q^m}(\lambda_k(\boldsymbol{g})) = \min\{k+1, \mathrm{rk}_q(\boldsymbol{g})\}$.

Since $\mathrm{rk}_q(\boldsymbol{h}) \geq t + k_{\max}$, Lemma 1 implies that for $j \in \{0, \ldots, \ell\}$, $\mathrm{rk}_{q^m}(\lambda_{t+k_j-1}(\boldsymbol{h}_j)) = t + k_j$. Moreover,

$$\dim\ker(\lambda_{t+k_j-1}(\boldsymbol{h}_j)) + \mathrm{rk}_{q^m}(\lambda_{t+k_j-1}(\boldsymbol{h}_j)) = n.$$

Hence, $\dim\ker(\lambda_{t+k_j-1}(\boldsymbol{h}_j)) = n-(t+k_j)$. It implies that the number of possible vectors $\boldsymbol{g}_j$ is at most $(q^m)^{n-(t+k_j)}$. Therefore,

$$|\mathcal{A}_{\boldsymbol{h}}| \leq \prod_{j=0}^{\ell} (q^m)^{n-(t+k_j)} = (q^m)^{(\ell+1)(n-t)-k_a-1}.$$

To complete the proof, we also need the following lemma

Lemma 2 (Lemma 3.13 [14]): Given $n \leq m$, the number of matrices $\boldsymbol{A} \in \mathbb{F}_q^{m\times n}$ such that $\mathrm{rk}_q(\boldsymbol{A}) = n$ is larger than $\frac{q^{mn}}{4}$.

As a consequence, it is also the lower bound for the number of vectors $\boldsymbol{u} \in \mathbb{F}_{q^m}^n$ such that $\mathrm{rk}_q(\boldsymbol{u}) = n$. Since $\forall j \in \{1,\dots,\ell\},\ \mathrm{rk}_q(\boldsymbol{g}_j) = n$, from Lemma 2, the number of possible vectors $\boldsymbol{g}_j$ is $\frac{q^{mn}}{4}$. Moreover $\boldsymbol{g}_0$ can be chosen completely arbitrarily, thus adding a factor of q^{mn}. Hence, the number of possible matrices $\boldsymbol{A} \in \mathcal{A}$ is greater than $\left(\frac{q^{mn}}{4}\right)^{\ell} q^{mn}$. Thus,

$$|\mathcal{A}| \geq \frac{(q^m)^{n(\ell+1)}}{4^\ell} \text{ and } \frac{|\mathcal{A}_{\boldsymbol{h}}|}{|\mathcal{A}|} \leq \frac{4^\ell}{(q^m)^{k_a+(\ell+1)t+1}}.$$

Finally we have

$$\frac{|\mathcal{S}|}{q^m-1} = \frac{\binom{n}{r+1}(q^m-1)^{r+1}}{q^m-1} \approx \binom{n}{r+1} q^{mr}.$$

From the inequality (4), we obtain that

$$\mathcal{P}_{\mathcal{A}}\left[r < (\ell+1)t + k_a\right] \leq \frac{\binom{n}{r+1} 4^\ell q^{mr}}{q^{m\cdot(k_a+(\ell+1)t+1)}}.$$

Now since $1 \leq k_a + (\ell+1)t - r$, we have

$$\mathcal{P}_{\mathcal{A}}\left[r < (\ell+1)t + k_a\right] \leq \frac{\binom{n}{r+1} 4^\ell}{q^{2m}} \leq \frac{1}{q^m}.$$

■

Now we can sum up and establish our main result

Theorem 5 (Main theorem): Let $\boldsymbol{g}_1,\dots,\boldsymbol{g}_\ell$ be a randomly chosen set of vectors of rank n in $\mathbb{F}_{q^m}^n$. Let

$$\mathcal{C} = \sum_{j=1}^{\ell} \mathcal{G}_{k_j}(\boldsymbol{g}_j),$$

then $\mathcal{C}$ can be decoded up to t errors with a failure probability upper-bounded by q^{-m} with a polynomial-time complexity, under the condition that $(\ell+1)t + k_a < n$.

D. Discussion on the dimension and minimum distance

1) Dimension of the code:

Let $\boldsymbol{G}$ be the generator matrix of the code $\mathcal{C}$. Then

$$\boldsymbol{G}^\top = ((\lambda_{k_1-1}(\boldsymbol{g}_1))^\top,\dots,(\lambda_{k_\ell-1}(\boldsymbol{g}_\ell))^\top).$$

The matrix $\boldsymbol{G}$ is $n \times k_a$ matrix in $\mathbb{F}_{q^m}$. Similar to the Theorem 4, for $\boldsymbol{g}_j$ are chosen uniformly in $\mathbb{F}_{q^m}$ such that $\mathrm{rk}(\boldsymbol{g}_j) = n$, then the probability such that $\mathrm{rk}_{q^m}(\boldsymbol{G}) < k_a$ is smaller than q^{-m}. Therefore, the dimension of the code $\mathcal{C}$ is equal to k_a with high probability.

2) The minimum distance:

We investigate the bound for the minimum distance d_{min} of the code $\mathcal{C}$. By Singleton bound [16], $d_{min} \leq n - k + 1$.

E. Comparison with the Hamming metric case

If Gabidulin codes are evaluation codes for the skew polynomial rings, and since their sum can be in some sense decoded, it could be of interest to see if this can be adapted in some way to Hamming metric and generalized Reed-Solomon codes. Unfortunately, this is not the case. Consider the following decoding problem:

$$\boldsymbol{y} = \boldsymbol{c} + \boldsymbol{e},$$

where

- $\boldsymbol{c} = \sum_{j=1}^{\ell} f_j(\boldsymbol{b}_j)$, where the f_j are polynomials of degree $k_j - 1$ and $\boldsymbol{b}_j \in \mathbb{F}_{q^m}^n$ are formed of distinct elements;
- $\boldsymbol{e} = (e_1,\dots,e_n) \in \mathbb{F}_{q^m}^n$ has Hamming weight t.

Let $\mathcal{E}$ be the support of size t of $\boldsymbol{e}$, that is the set of non-zero positions. Then, for any $j \in \{1,\dots,\ell\}$, there exists a unique monic polynomial $A_j(x)$ of degree t such that

$$\forall i \in \mathcal{E}, \quad A_j(b_{ji}) = 0.$$

This raises the problem that the annihilator polynomial depends on the chosen elements thus obtaining the following systems

$$\forall i = 1,\dots,\ell, \quad A_i(\boldsymbol{b}_i)\boldsymbol{y} = \sum_{j=1}^{\ell} A_i(\boldsymbol{b}_i) f_j(\boldsymbol{b}_j).$$

We would like to transform the product of elements into the product of polynomials as in the case rank metric. Let us fix b_1. Then for all $i = 2,\dots,\ell$, there exists a polynomial $B_i(x)$ of degree $\leq n$, such that $\boldsymbol{b}_i = B_i(\boldsymbol{b}_1)$. Therefore, by setting $F_j(x) = f_j(B_j)(x)$ we now obtain

$$A_1(\boldsymbol{b}_1)\boldsymbol{y} = \sum_{j=1}^{\ell} (A_1 F_j)(\boldsymbol{b}_1).$$

This system is very similar to system (1). The problem when we linearize is that the degree of F_j is with high probability larger than n. Therefore, the number of unknowns is very probably always larger than n.

IV. Applications

In this section, we give examples where the previous theorem has some applications. We do not claim to have obtained extraordinary new results, but we emphasize that this new point of view in decoding could have interesting cryptographic applications.

A. Decoding of Interleaved code

As in [17], we consider the following model of channel: The error positions are all taken in the same q-ary vector space $\mathcal{E}$, of dimension t, i.e, every error vector $\boldsymbol{e} = (e_1,\dots,e_n)$ of length n such that for all $i \in \{1,\dots,n\},\ e_i \in \mathcal{E}$. Let A be the unique monic linearized polynomial of degree t such that for all $e \in \mathcal{E}, A\langle e\rangle = 0$. Suppose that through this channel, one receive u messages $\boldsymbol{y}^{(1)},\dots,\boldsymbol{y}^{(u)}$, such that

$$\forall i \in \{1,\dots,u\},\ \boldsymbol{y}^{(i)} = \boldsymbol{c}_i + \boldsymbol{e}_i,$$

where $\boldsymbol{c}_i \in \mathcal{C}$.

Thus, for all $i \in \{1, \ldots, u\}$, $\boldsymbol{y}^{(i)} = \sum_{j=1}^{\ell} f_j^{(i)} \langle \boldsymbol{g}_j \rangle + \boldsymbol{e}_i$ and

$$A\langle \boldsymbol{y}^{(i)} \rangle = \sum_{j=1}^{\ell} (A \cdot f_j^{(i)}) \langle \boldsymbol{g}_j \rangle. \tag{5}$$

As in the normal case of interleaving, this implies that

$$A\langle \boldsymbol{y}^{(i)} \rangle = \sum_{j=1}^{\ell} N_j^{(i)} \langle \boldsymbol{g}_j \rangle \tag{6}$$

where, for $i \in \{1, \ldots, u\}$, $N_j^{(i)} \in \mathbb{F}_{q^m}[X;\theta]$ has degree $\leq t + k_j - 1$. The system (6) is linear in $t(u\ell + 1) + uk_a + 1$ unknowns (the coefficients of polynomials) and nu equations. Therefore, we can hope to decode up to errors of rank

$$t \leq \lfloor (u\,(n - k_a)) \,/\, (u\ell + 1) \rfloor .$$

B. On McEliece type rank-metric based cryptosystem

In GPT-type cryptosystem, we could expect to replace the family of Gabidulin codes with the family of sum of Gabidulin codes. However, by studying the effect of Overbeck's distinguisher, we show that it cannot be replaced directly. More recently [4], a new technique was introduced to scramble Gabidulin codes. If the parameters are not carefully chosen, there exists a simple distinguisher leading to an efficient key recovery attack [18]. We investigate the effect of this attack if the family of Gabidulin codes is replaced by a sum of Gabidulin codes. We show that the attack cannot be easily adapted.

1) Overbeck 's distinguisher:

Let $\mathcal{C} = \sum_{j=1}^{\ell} \mathcal{G}_{k_j}(\boldsymbol{g}_j)$ and $\mathcal{C}_{rand}$ a random code of dimension k. The idea of Overbeck's distinguisher is to use the automorphism θ to distinguish $\mathcal{C}$ from a random code of same dimension.

For the random code $\mathcal{C}_{rand}$, we expect that $\dim_{\mathbb{F}_{q^m}} \left(\mathcal{C}_{rand} + \mathcal{C}_{rand}^{[1]} \right) = \min(n, 2k)$ with high probability, since the usual hypothesis in that case is to suppose that $\mathcal{C}_{rand}$ and $\mathcal{C}_{rand}^{[1]}$ behave like two k-dimensional vector spaces randomly and uniformly chosen.

By studying the dimension of $\mathcal{C} + \mathcal{C}^{[1]}$, we can show that it is at most $k + \ell$. For $\ell < k < n/2$, this implies a distinguisher between this code and the random ones. This indicates that substituting Gabidulin codes by sum of Gabidulin codes as such is probably not a good idea.

2) Loidreau-like encryption scheme: The security of the scheme is supported by two hypotheses

- The public code is indistinguishable from a random code
- Bounded distance decoding in rank metric is a cryptographically difficult problem

The second point is beyond the scope of this paper. We are interested in the first point. So let us recall the procedure for generating a public-key/private key pair.

- The private key is $\mathcal{C} = \sum_{j=1}^{\ell} \mathcal{G}_{k_j}(\boldsymbol{g}_j)$.
- The public-key is a randomly chosen generator matrix of $\mathcal{C}\boldsymbol{P}^{-1}$ where $\boldsymbol{P} \in M_n(\mathcal{V})$ where $\mathcal{V}$ is a random λ-dimensional $\mathbb{F}_q$- linear subspace of $\mathbb{F}_{q^m}$.

We observe the attack by distinguisher.

1) Distinguishing $\mathcal{C}\boldsymbol{P}^{-1}$ from random codes: If we raise a public-key $\boldsymbol{G}_{\text{pub}}^{[i]}$ to the i-th power of θ we have

$$\boldsymbol{G}_{\text{pub}}^{[i]} = \boldsymbol{S}^{[i]} \boldsymbol{G}^{[i]} (\boldsymbol{P}^{-1})^{[i]}.$$

The matrix $\boldsymbol{P}$ has entries in $\mathcal{V}$ but the matrix $\boldsymbol{P}^{-1}$ has no reason to belong to some strict subspace of $\mathbb{F}_{q^m}$. Thus we avoid the invariant subspace attack [19], [20].

2) Distinguishing $\mathcal{C}^{\perp}\boldsymbol{P}^{\top} := \mathcal{C}_{\text{pub}}^{\perp}$ from random codes. A generator matrix of $\mathcal{C}_{\text{pub}}^{\perp}$ is $\boldsymbol{H}_{\text{pub}} = \boldsymbol{H}\boldsymbol{P}^{\top}$, where $\boldsymbol{H}$ is a parity-check matrix of $\mathcal{C}$. The invariant subspace attack requires computing $\dim_{\mathbb{F}_{q^m}} \left(\mathcal{C}_{\text{pub}}^{\perp} + \cdots + \mathcal{C}_{\text{pub}}^{\perp\,[i]} \right)$ but we may not have enough information for $\mathcal{C}^{\perp}$.

Lemma 3: The dual code of $\mathcal{C}_{\text{pub}}$ is

$$\mathcal{C}_{\text{pub}}^{\perp} = \bigcap_{j=1}^{\ell} \mathcal{G}_{n-k_j}(\boldsymbol{h}_j)\boldsymbol{P}^{\top},$$

for some $\boldsymbol{h}_j \in \mathbb{F}_{q^m}^n$ such that $\mathrm{rk}(\boldsymbol{h}_j) = n$.

Proof: This lemma is straightforward from the fact that $\boldsymbol{H}_{\text{pub}} = \boldsymbol{H}\boldsymbol{P}^{\top}$ and $\mathcal{G}_k^{\perp}(\boldsymbol{g}) = \mathcal{G}_{n-k}^{\perp}(\boldsymbol{h})$ for some $\boldsymbol{h} \in \mathbb{F}_{q^m}^n$ [2]. ∎

The attack of Alain Couveur and Coggia [18] needs to compute $\dim_{\mathbb{F}_{q^m}} \left(\mathcal{C}_{\text{pub}}^{\perp} + \cdots + \mathcal{C}_{\text{pub}}^{\perp\,[i]} \right)$ corresponding to the construction of $\mathcal{C}^{\perp}$, so it requires a representation for the basis of $\mathcal{C}_{\text{pub}}^{\perp}$. However, from the lemma, it is only a $n-k$-dimensional subspace of $\mathcal{G}_{n-k_j}(\boldsymbol{h}_j)\boldsymbol{P}^{\top}$. Thus, this approach cannot directly lead to the recovery of the private key.

C. Probabilistic polynomial-time decoding of random codes

A direct consequence of Theorem 3, is just a reformulation of a result in [7] shows that it is possible to have a probabilistic polynomial-time decoder for random codes up to a certain dimension. Namely, a k-dimensional random code is the direct sum of k 1-dimensional random codes.

Suppose that $\mathcal{C}$ is a random code with generator matrix

$$G = \begin{pmatrix} \boldsymbol{g}_1 \\ \vdots \\ \boldsymbol{g}_k \end{pmatrix},$$

where $(\boldsymbol{g}_j)_{j=1}^k$ are linearly independent over $\mathbb{F}_{q^m}$. Then, $\mathcal{C} = \sum_{j=1}^{k} \mathcal{G}_1(\boldsymbol{g}_j)$ is a k-dimensional random code. Therefore, we have the immediate following corollary of theorem 3

Corollary 2: Let $\mathcal{C}$ be a $[n,k]_r$ linear code over $\mathbb{F}_{q^m}$, then there is a probabilistic polynomial time decoder for $\mathcal{C}$ up to errors of rank

$$t \leq \left\lfloor \frac{n-k}{k+1} \right\rfloor .$$

The sum of k 1-dimensional codes is a random code of dimension k. With this approach, we recover the decoding of a random rank-metric code [7].

REFERENCES

[1] D. Silva, F. R. Kschischang, and R. Kötter, "Communication over finite-field matrix channels," *IEEE Trans. Information Theory*, vol. 56, no. 3, pp. 1296–1305, 2010.

[2] E. M. Gabidulin, "Theory of codes with maximum rank distance," *Problemy Peredachi Informatsii*, vol. 21, no. 1, pp. 3–16, 1985.

[3] P. Gaborit, G. Murat, O. Ruatta, and G. Zémor, "Low rank parity check codes and their application to cryptography," in *Proceedings of the Workshop on Coding and Cryptography WCC'2013*, Bergen, Norway, 2013. [Online]. Available: www.selmer.uib.no/WCC2013/pdfs/Gaborit.pdf

[4] P. Loidreau, "A new rank metric codes based encryption scheme," in *Post-Quantum Cryptography 2017*, ser. LNCS, vol. 10346. Springer, 2017, pp. 3–17.

[5] C. Faure and P. Loidreau, "A new public-key cryptosystem based on the problem of reconstructing *p*-polynomials," in *Coding and Cryptography, International Workshop, WCC 2005, Bergen, Norway, March 14-18, 2005. Revised Selected Papers*, 2005, pp. 304–315.

[6] J. Lavauzelle, P. Loidreau, and B. Pham, "Ramesses, a rank metric encryption scheme with short keys," 2019. [Online]. Available: http://arxiv.org/abs/1911.13119

[7] N. Aragon, P. Gaborit, A. Hauteville, and J.-P. Tillich, "A new algorithm for solving the rank syndrome decoding problem," in *2018 IEEE International Symposium on Information Theory, ISIT 2018, Vail, CO, USA, June 17-22, 2018*. IEEE, 2018, pp. 2421–2425.

[8] O. Ore, "On a special class of polynomials," *Transactions of the American Mathematical Society*, vol. 35, no. 3, pp. 559–584, 1933.

[9] D. Boucher and F. Ulmer, "Linear codes using skew polynomials with automorphisms and derivations," *Des. Codes Cryptogr.*, vol. 70, no. 3, pp. 405–431, 2014.

[10] G. Schmidt, V. R. Sidorenko, and M. Bossert, "Error and erasure correction of interleaved Reed-Solomon codes," in *Coding and Cryptography*, Ø. Ytrehus, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 22–35.

[11] P. Delsarte, "Bilinear forms over a finite field, with applications to coding theory," *J. Comb. Theory, Ser. A*, vol. 25, no. 3, pp. 226–241, 1978.

[12] P. Loidreau, "A Welch–Berlekamp like algorithm for decoding Gabidulin codes," in *Coding and Cryptography*, Ø. Ytrehus, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 36–45.

[13] D. Augot, P. Loidreau, and G. Robert, "Generalized gabidulin codes over fields of any characteristic," *Des. Codes Cryptogr.*, vol. 86, no. 8, pp. 1807–1848, 2018.

[14] R. Overbeck, "Public key cryptography based on coding theory," Ph.D. dissertation, Technische Universität, Darmstadt, June 2007. [Online]. Available: http://tuprints.ulb.tu-darmstadt.de/823/

[15] R. Lidl and H. Niederreiter, *Finite fields*, 2nd ed., ser. Encyclopedia of Mathematics and its Applications. Cambridge University Press, Cambridge, 1997, vol. 20, with a foreword by P. M. Cohn.

[16] R. Singleton, "Maximum distance q-nary codes," *IEEE Transactions on Information Theory*, vol. 10, no. 2, pp. 116–118, 1964.

[17] J. Renner, S. Puchinger, and A. Wachter-Zeh, "Interleaving loidreau's rank-metric cryptosystem," *CoRR*, vol. abs/1901.10413, 2019. [Online]. Available: http://arxiv.org/abs/1901.10413

[18] D. Coggia and A. Couvreur, "On the security of a Loidreau's rank metric code based encryption scheme," in *WCC 2019 - Workshop on Coding Theory and Cryptography*, Saint Jacut de la mer, France, Mar. 2019. [Online]. Available: https://hal.archives-ouvertes.fr/hal-02064465

[19] A. Kshevetskiy, "Security of gpt-like public-key cryptosystems based on linear rank codes," in *2007 3rd International Workshop on Signal Design and Its Applications in Communications*, 2007, pp. 143–147.

[20] A. Otmani, H. T. Kalachi, and S. Ndjeya, "Improved cryptanalysis of rank metric schemes based on gabidulin codes," *CoRR*, vol. abs/1602.08549, 2016. [Online]. Available: http://arxiv.org/abs/1602.08549