Right-hand side decoding of Gabidulin codes and applications

Maxime Bombar[1,2] and Alain Couvreur[2,1]

[1] LIX, CNRS UMR 7161, École Polytechnique,
Institut Polytechnique de Paris,
1 rue Honoré d'Estienne d'Orves
91120 Palaiseau Cedex
[2] Inria
{maxime.bombar, alain.couvreur}@inria.fr

Abstract. We discuss the decoding of Gabidulin and interleaved Gabidulin codes. We give the full presentation of a decoding algorithm for Gabidulin codes, which as Loidreau's seminal algorithm consists in localizing errors in the spirit of Berlekamp–Welch algorithm for Reed–Solomon codes. On the other hand this algorithm consists in acting on codewords on the right while Loidreau's algorithm considers an action on the left. This *right–hand side* decoder was already introduced by the authors in a previous work for cryptanalytic applications. We give a generalised version which applies to non–full length Gabidulin codes. Finally, we show that this algorithm turns out to provide a very clear and natural approach for the decoding of interleaved Gabidulin codes.

Keywords: Gabidulin codes · Decoding · Interleaved codes

Introduction

Rank metric codes have been introduced in [7] by Gabidulin and have found applications in cryptography [8,6,1,11,16,3,2], in network communications [18] or in data storage [15]. Compared to the Hamming world, only few families of codes endowed with the rank metric are known to have efficient decoding algorithms. Gabidulin codes are the rank-metric analogue of Reed-Solomon codes and are somehow optimal because they reach the rank-metric Singleton bound and come with efficient decoders up to the unique decoding radius $\frac{n-k}{2}$. However, there exist no known decoder beyond this bound, even probabilistic ones. More, there exist families of Gabidulin codes that cannot be list decoded in polynomial time [14]. Nonetheless, if we consider u codewords in parallel, it is possible to overcome this restriction and decode up to $\frac{u}{u+1}(n-k)$ rank errors with overwhelming probability.

In the present article, we recall a right-hand side decoder for Gabidulin codes recently introduced in [5] for cryptanalytic applications. While the aforementioned reference restricted to the case of full length Gabidulin codes (*i.e.* $n{=}m$), in the present article we extend it to handle Gabidulin codes of any length $n \leqslant m$.

Next, we show how this decoder can be used to provide a simple decoder for u-interleaved Gabidulin codes. We claim that the use of this algorithm provides a much simpler point of view on the decoding of interleaved Gabidulin codes because it only involves solving an overdetermined linear system. In particular, this algorithm is very similar to the decoder for Interleaved Reed-Solomon codes presented in [4], and its decoding radius is given by comparing the number of equations to the number of unknowns. Moreover, it permits to clarify a cryptographic attack based on the decoding of interleaved Gabidulin codes and provides a very simple explanation of the decoding failures.

1 Notations and Prerequisites

In this article, q is a prime power and k, m, n, u are non negative integers. $\mathbb{F}_q$ denotes the finite field with q elements, and for a non negative integer ℓ, $\mathbb{F}_{q^\ell}$ is the algebraic extension of $\mathbb{F}_q$ of degree ℓ. The space of $m \times n$ matrices with entries in a field $\mathbb{K}$ is denoted by $\mathcal{M}_{m\times n}(\mathbb{K})$. Lower case bold face letters such as $\boldsymbol{x}$ represent vectors, and upper case bold face letters such as $\boldsymbol{X}$ denote matrices.

1.1 Rank metric codes

Given a vector $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$, the *column support* (or *support*) of $\boldsymbol{x}$, denoted $\mathrm{Supp}(\boldsymbol{x})$ is the $\mathbb{F}_q$-vector subspace of $\mathbb{F}_{q^m}$ spanned by the entries of $\boldsymbol{x}$:

$$\mathrm{Supp}(\boldsymbol{x}) = \mathbf{Span}_{\mathbb{F}_q}\{x_1, \ldots, x_n\}.$$

We consider also another notion of support, namely the *row* support. Let $\mathscr{B}$ be a basis of the extension field $\mathbb{F}_{q^m}/\mathbb{F}_q$. Then we define the extension of $\boldsymbol{x}$ with respect to $\mathscr{B}$ as the matrix $\mathrm{Ext}_{\mathscr{B}}(\boldsymbol{x}) \in \mathcal{M}_{m\times n}(\mathbb{F}_q)$ whose columns are the decompositions of the entries of $\boldsymbol{x}$ in the basis $\mathscr{B}$. The row space of $\mathrm{Ext}_{\mathscr{B}}(\boldsymbol{x})$ is called the *row* support of $\boldsymbol{x}$, *i.e.*

$$\mathrm{RowSupp}(\boldsymbol{x}) \stackrel{\text{def}}{=} \{\boldsymbol{y}\mathrm{Ext}_{\mathscr{B}}(\boldsymbol{x}) \mid \boldsymbol{y} \in \mathbb{F}_q^m\} \subset \mathbb{F}_q^n.$$

It is a vector subspace of $\mathbb{F}_q^n$. Notice that the above definition does not depend on the choice of the basis $\mathscr{B}$. The *rank weight* $\mathbf{rank}_q(\boldsymbol{x})$ (or *rank*) of $\boldsymbol{x}$ is the rank of $\mathrm{Ext}_{\mathscr{B}}(\boldsymbol{x})$ with respect to any basis $\mathscr{B}$. The *rank distance* or *distance* between two vectors $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_{q^m}^n$ is defined as $d(\boldsymbol{x}, \boldsymbol{y}) = \mathbf{rank}_q(\boldsymbol{x} - \boldsymbol{y})$. In this article, we consider only $\mathbb{F}_{q^m}$-linear codes: a code $\mathscr{C}$ of length n and dimension k is an $\mathbb{F}_{q^m}$-subspace of $\mathbb{F}_{q^m}^n$ whose dimension, as an $\mathbb{F}_{q^m}$-vector space, is k. The *minimum distance* of $\mathscr{C}$ is defined as

$$d_{min}(\mathscr{C}) = \min\{\mathbf{rank}_q(\boldsymbol{c}) \mid \boldsymbol{c} \in \mathscr{C}, \boldsymbol{c} \neq 0\}.$$

1.2 Gabidulin codes and q-polynomials

A q–polynomial is a polynomial of the form

$$P(X) = p_0 X + p_1 X^q + \cdots + p_r X^{q^r}, \quad p_r \neq 0.$$

The integer r is called the *q-degree* of P and is denoted by $\deg_q(P)$. A q-polynomial P induces an $\mathbb{F}_q$-linear map $\mathbb{F}_{q^m} \to \mathbb{F}_{q^m}$ whose kernel has dimension bounded by $\deg_q(P)$. The *rank* of a q-polynomial will denote the rank of the induced linear map. Let $\mathcal{L}$ be the space of q-polynomials and given a positive integer $k < m$, we denote by $\mathcal{L}_{<k}$ (resp. $\mathcal{L}_{\leqslant k}$) the space of q-polynomials of q-degree less than (resp. less than or equal to) k. Equipped with the addition and the composition law, $\mathcal{L}$ is a non commutative ring which is left and right euclidean [10] and the two-sided ideal $(X^{q^m} - X)$ is the kernel of the canonical map

$$\mathcal{L} \to \mathrm{Hom}_{\mathbb{F}_q}(\mathbb{F}_{q^m}, \mathbb{F}_{q^m}),$$

inducing an isomorphism

$$\mathcal{L}/(X^{q^m} - X) \simeq \mathrm{Hom}_{\mathbb{F}_q}(\mathbb{F}_{q^m}, \mathbb{F}_{q^m}).$$

Let $n \leqslant m$, $k \leqslant n$ and $\boldsymbol{g} = (g_1, \ldots, g_n) \in \mathbb{F}_{q^m}^n$ whose entries are linearly independent. The *Gabidulin code* of dimension k and evaluation vector $\boldsymbol{g}$ is defined as

$$\mathscr{G}_k(\boldsymbol{g}) \stackrel{\text{def}}{=} \{(P(g_1), \ldots, P(g_n)) \mid P \in \mathcal{L}_{<k}\} \subset \mathbb{F}_{q^m}^n.$$

Notice that the canonical map

$$\begin{cases} \mathcal{L}_{<k} \longrightarrow & \mathscr{G}_k(\boldsymbol{g}) \\ \;\; P \;\longmapsto & (P(g_1), \ldots, P(g_n)). \end{cases}$$

is rank preserving, which allows to identify $\mathscr{G}_k(\boldsymbol{g})$ with $\mathcal{L}_{<k}$. It is well known that Gabidulin codes are *Maximum Rank Distance* (MRD), which means that they reach the rank metric analogue of the *Singleton* bound

$$d_{min}(\mathcal{L}_{<k}) = n - k + 1.$$

Moreover, Gabidulin codes come with efficient decoders able to correct errors up to the unique decoding radius $\frac{n-k}{2}$. However, contrary to Reed-Solomon codes, there exists families of Gabidulin codes that *cannot* be list decoded in polynomial time beyond this bound [14].

Following [5, § 1], to any class $P \in \mathcal{L}/(X^{q^m} - X)$, corresponds an adjoint $P^\vee$ defined as follows:

$$\text{for} \quad P(X) = \sum_{i=0}^{m-1} p_i X^{q^i} \qquad \text{and} \qquad P^\vee(X) = \sum_{i=0}^{m-1} p_i^{q^{m-i}} X^{q^{m-i}}.$$

This corresponds to the usual notion of the adjoint endomorphism with respect to the non degenerate bilinear form on $\mathbb{F}_{q^m}$: $(x, y) \longmapsto \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(xy)$.

2 Right hand side decoding algorithm

Let $k < n \leqslant m$, $\boldsymbol{g} = (g_1, \ldots, g_n) \in \mathbb{F}_{q^m}^n$ whose entries are linearly independent, and let $\mathscr{C} \stackrel{\text{def}}{=} \mathscr{G}_k(\boldsymbol{g})$. In [12], Loidreau introduced a Berlekamp-Welch-like decoding algorithm, which can decode up to $\lfloor \frac{n-k}{2} \rfloor$ rank errors. This algorithm works *on the left* and can be applied to Gabidulin codes of arbitrary length $n \leqslant m$. Indeed, representing vectors in $\mathbb{F}_{q^m}^n$ as matrices, the left–hand side decoding consists in acting on matrices on the left, which is possible whatever the length n (which corresponds to the number of columns of the corresponding matrices).

In [5], the authors proposed to work on the right-hand side instead, which was useful to provide an attack on the code-based encryption scheme Ramesses [11]. However, their decoding algorithm was only considered in the case where $n = m$ (which was enough for cryptanalysis). The right-hand side algorithm is not completely straightforward when $n < m$. In particular, one can no longer transpose the matrices representing codewords.

In the present section, we recall a self-contained presentation of the right-hand side version, and prove that restricting n to be maximal is unnecessary. In particular, we show how the right-hand side decoding algorithm applied to any $[n, k]$ Gabidulin code can correct up to $\lfloor \frac{n-k}{2} \rfloor$ errors.

2.1 $n = m$

Suppose we receive a word $\boldsymbol{y} = \boldsymbol{c} + \boldsymbol{e} \in \mathbb{F}_{q^m}^n$ where $\boldsymbol{c} \in \mathscr{C} \stackrel{\text{def}}{=} \mathscr{G}_k(\boldsymbol{g})$ and $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ has rank $t \leqslant \frac{n-k}{2}$. By linear interpolation, there exist three q-polynomials $C \in \mathcal{L}_{<k}$ and $Y, E \in \mathcal{L}_{<m}$ such that

$$Y = C + E,$$

and Y is known to the receiver (See for instance [19, Chapter 3]). Since $n = m$, $(g_1, \dots, g_n)$ forms a basis of the extension field $\mathbb{F}_{q^m}/\mathbb{F}_q$. Therefore, $\mathbf{rank}_q(E) = \mathbf{rank}_q(\boldsymbol{e}) = t$. The core of the algorithm relies in the following proposition:

Proposition 1. *Let E be a q-polynomial of rank t. There exists a unique monic q-polynomial Λ such that $\deg_q(\Lambda) \leqslant t$ and $E \circ \Lambda = 0$ modulo $(X^{q^m} - X)$.*

The goal is now to compute this right annihilator Λ. It satisfies the equation

$$Y \circ \Lambda = C \circ \Lambda + E \circ \Lambda \equiv C \circ \Lambda \mod (X^{q^m} - X),$$

which yields a non linear system of n equations whose unknowns are the $k+t+1$ coefficients of C and Λ.

$$\begin{cases} (Y \circ \Lambda)(g_i) = C \circ \Lambda(g_i) \\ \deg_q \Lambda \leqslant t \\ \deg_q C \leqslant k - 1. \end{cases} \tag{1}$$

In order to linearize the system, set $N = C \circ \Lambda$ and consider instead

$$\begin{cases} (Y \circ \Lambda)(g_i) = N(g_i) \\ \deg_q \Lambda \leqslant t \\ \deg_q N \leqslant k + t - 1, \end{cases} \tag{2}$$

whose unknowns are the $k + 2t + 1$ coefficients of N and Λ. The relationships between those two systems are specified in the following proposition.

Proposition 2.

- *Any solution* (Λ, C) *of* (1) *gives a solution* $(\Lambda, N = C \circ \Lambda)$ *of* (2).
- *Assume that* E *is of rank* $t \leqslant \lfloor \frac{n-k}{2} \rfloor$. *If* (Λ, N) *is a nonzero solution of* (2) *then* $N = C \circ \Lambda$ *where* $C = Y - E$ *is the interpolating* q*–polynomial of the codeword.*

Therefore, it is possible to recover the codeword C from any non zero solution (Λ, N) of (2) by computing the right hand side euclidean division of N by Λ which can be done efficiently.

Remark 1. Actually, the previous system is only linear over $\mathbb{F}_q$, not over $\mathbb{F}_{q^m}$. To address this issue, one can use the adjunction operation. Details can be found in [5].

2.2 $n < m$

Assume now that n is not maximal, and consider a received word $\boldsymbol{y} = \boldsymbol{c} + \boldsymbol{e}$, where $\boldsymbol{c} = (C(g_1), \dots, C(g_n))$ for some q–polynomial C of q–degree $< k$ and $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ has rank t whose value is discussed further.

As in the previous section, our first objective is to reformulate the decoding problem in terms of q–polynomials instead of vectors. Here lies the first issue. Indeed, since $\boldsymbol{y}$ has length $n < m$ there is not a unique q–polynomial Y in $\mathcal{L}/(X^{q^m} - X)$ such that $\boldsymbol{y} = (Y(g_1), \dots, Y(g_n))$. For this reason, when choosing such an arbitrary interpolator Y for $\boldsymbol{y}$, one can define $E \stackrel{\text{def}}{=} Y - C$ and get a new q–polynomial formulation of the decoding problem as

$$Y = C + E,$$

but here there is no longer any reason that E would have rank t, we only know that the vector $(E(g_1), \dots, E(g_n))$ has rank t. In terms of linear operators, this means that the restriction of E to the span V of $g_1, \dots, g_n$ over $\mathbb{F}_q$ has rank t.

To fix this issue we proceed as follows. First we choose Y as the interpolator of lowest degree by choosing the unique monic interpolator of degree $< n$. Since $\deg_q(C) < k < n$, this entails that $\deg_q(E) < n$. Next we will change the interpolating polynomials Y and E in order E to have rank t. This should be done without knowing the error. We need a slight generalization of Proposition 1 which we prove here for the sake of completeness.

Proposition 3. *There exists a* q*–polynomial* G *of* q*–degree* $\leqslant m-n$ *whose image equals the* $\mathbb{F}_q$*–span of* $g_1, \dots, g_n$.

Proof. Let V denote the $\mathbb{F}_q$–span of $g_1, \dots, g_n$. By interpolation, it is well-known that there exists G_0 of q–degree $\leqslant m - n$ whose kernel equals the $(m-n)$–dimensional space $V^\perp$ for the inner product $(x, y) \mapsto \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(xy)$. Then, the q–polynomial $G_1 \stackrel{\text{def}}{=} X^{q^n} \circ G_0$ has the same kernel V and is in the span of the q–monomials $X^{q^n}, \dots, X^{q^m}$. Then, let $G \stackrel{\text{def}}{=} G_1^\vee$ be the adjoint as introduced in

§ 1.2. It has q–degree $\leqslant m-n$ and, by adjunction properties, satisfies $\mathrm{Im}(G) = \mathrm{Im}(G_1^\vee) = \mathrm{Ker}(G_1)^\perp = V$. □

Let G be the q–polynomial of degree $\leqslant m-n$ given by Proposition 3 and consider $Y \circ G$ instead of Y, then we get a new problem which is

$$Y \circ G = C \circ G + E \circ G. \tag{3}$$

First, since $\boldsymbol{y}$ and $\boldsymbol{g}$ are known, the q–polynomials Y, G are computable using interpolation. Then, the q–polynomial $C \circ G$ has q–degree $< k+m-n$ and hence corresponds to a codeword of a Gabidulin code of dimension $k+m-n$. Finally, $E \circ G$ has rank t. Indeed, as mentioned earlier, t is the rank of the restriction of E to the span of $g_1, \ldots, g_n$, which is precisely the image of G. Thus, the reformulated problem (3) can be regarded as correcting a rank t error in a Gabidulin code of length m and dimension $k+m-n$. Using our right-hand decoding algorithm it is hence possible to correct an amount of errors up to

$$t = \frac{m-(k+m-n)}{2} = \frac{n-k}{2} \cdot$$

Remark 2. The previous results may be interpreted in terms of decoding a length m Gabidulin code which was column–punctured on the right at $\delta = m-n$ positions (see [17, § 2.3] for a definition of column–puncturing). Similarly, this can be unterstood in terms of decoding a length m Gabidulin code under δ rank erasures and t rank errors. In this situation we recover the usual fact that $2t + \delta \leqslant n-k$.

3 Decoding interleaved Gabidulin codes

3.1 Interleaving

Interleaving a code $\mathscr{C}$ consists in considering several codewords of $\mathscr{C}$ *at the same time*, corrupted by errors having the same support. In the Hamming metric, interleaved Reed-Solomon codes have been extensively studied and come with efficient *probabilistic* decoders allowing to correct *uniquely* almost all error patterns slightly beyond the error capability of the code. See [4] for further reference. In the rank metric, interleaved Gabidulin codes have been introduced by Loidreau and Overbeck in [13]. Let $\boldsymbol{g}$ be an evaluation vector, and let $u \in \mathbb{N}$. The u-interleaved Gabidulin code of evaluation vector $\boldsymbol{g}$ and dimension k is

$$I\mathscr{G}_{u,k}(\boldsymbol{g}) \stackrel{\text{def}}{=} \left\{ \begin{pmatrix} \mathbf{c^{(1)}} \\ \vdots \\ \mathbf{c^{(u)}} \end{pmatrix} \mid \mathbf{c^{(i)}} \in Gab_k(\mathbf{g}) \right\}.$$

Remark 3. For $u = 1$, we recover usual Gabidulin codes.

Each codeword $\boldsymbol{C} \in I\mathscr{G}_{u,k}(\boldsymbol{g})$ is the evaluation of a *column* vector of q-polynomials of bounded q-degrees on $\boldsymbol{g}$:

$$\boldsymbol{C} = (\boldsymbol{\Gamma}(\boldsymbol{g}_1), \ldots, \boldsymbol{\Gamma}(\boldsymbol{g}_n)), \quad \boldsymbol{\Gamma} = \begin{pmatrix} C^{(1)} \\ \vdots \\ C^{(u)} \end{pmatrix} \text{ where } C^{(i)} \in \mathcal{L}_{<k}.$$

Using the inverse extension map, each $\boldsymbol{\Gamma}(g_i)$ can be interpreted as an element of $\mathbb{F}_{q^{mu}}$, and $I\mathscr{G}_{u,k}(\boldsymbol{g})$ is then a code of length n and dimension k over $\mathbb{F}_{q^{mu}}$. Moreover, they are known to be MRD (see [19, Lemma 2.17]), so the error correction capability of $I\mathscr{G}_{u,k}(\boldsymbol{g})$ is $\frac{n-k}{2}$. However, their specific structure allows to design efficient algorithms being able to *uniquely* decode $I\mathscr{G}_{u,k}(\boldsymbol{g})$ up to $\frac{u}{u+1}(n-k) > \frac{n-k}{2}$ for $u > 1$, with very high probability [13,20].

In this section we show how to use the right-hand side variant of the Berlekamp-Welch algorithm introduced before to decode u-interleaved Gabidulin codes, up to $\frac{u}{u+1}(n-k)$. Since this is beyond the error capability of the code, this algorithm might fail but the probability of failure is very low.

3.2 Error model

Similarly to the Hamming metric, we consider a channel model where errors happen *in burst*. In this model, the transmitted codeword is a matrix $\boldsymbol{C} \in \mathcal{M}_{u\times n}(\mathbb{F}_{q^m})$ representing u codewords of $\mathscr{G}_k(\boldsymbol{g})$ *in parallel*, and the error is a matrix $\boldsymbol{E} \in \mathcal{M}_{u\times n}(\mathbb{F}_{q^m})$ of $\mathbb{F}_q$-rank t, *i.e.* such that the matrix of $\mathcal{M}_{um\times n}(\mathbb{F}_q)$ obtained from $\boldsymbol{E}$ by extending every *row* in a basis of $\mathbb{F}_{q^m}/\mathbb{F}_q$ is of rank t. The receiver then gets a word $\boldsymbol{Y} = \boldsymbol{C} + \boldsymbol{E}$, and the goal is to recover $\boldsymbol{C}$.
In the Hamming metric, the receiver gets u noisy $\boldsymbol{y}^{(i)} = \boldsymbol{c}^{(i)} + \boldsymbol{e}^{(i)}$ such that $\boldsymbol{c}^{(i)}$ are codewords of some code $\mathscr{C}$ (*e.g.* a Reed-Solomon code) and *all* the $\boldsymbol{e}^{(i)}$ have the *same* support of cardinality t.
In the current setting, each row of $\boldsymbol{Y}$ is of the form $\boldsymbol{y}^{(i)} = \boldsymbol{c}^{(i)} + \boldsymbol{e}^{(i)}$ where $\boldsymbol{c}^{(i)} \in \mathscr{G}_k(\boldsymbol{g})$. The following proposition whose proof is straightforward justifies the term *burst rank-errors*.

Proposition 4. *The row support of each $\mathbf{e}^{(i)}$ is contained in the $\mathbb{F}_q$-row space of E which is of dimension t.*

Remark 4. In this article the error model consists in considering error vectors $\mathbf{e}^{(i)}$ sharing the same *row support*. It seems to be the most natural error model when considering the code regarded as a code over $\mathbb{F}_{q^{mu}}$, and it is the one used in most references. On the other hand, on may consider another error model where the errors share a common *column support*. In the latter case, the usual left–hand side decoder can be used, see for instance [13].

3.3 Right-hand side decoding of interleaved Gabidulin codes

Let $\boldsymbol{Y} = \boldsymbol{C} + \boldsymbol{E} \in \mathcal{M}_{u\times n}(\mathbb{F}_{q^m})$ be a received word. By linear interpolation of each row of $\boldsymbol{Y}$, there exist u triple of q-polynomials (Y_i, C_i, E_i) such that

$$Y_i = C_i + E_i,$$

and $\deg_q(C_i) < k$. Since the errors have the same support of dimension t, there exists a q-polynomial Λ with $\deg_q(\Lambda) \leqslant t$ that locates *all* the errors. More specifically, Proposition 4 induces the following lemma:

Lemma 1. *Denoting by E_i the interpolator q-polynomial of $\mathbf{e}^{(i)}$, there exists $\Lambda \in \mathcal{L}_{\leqslant t}$ such that*

$$E_i \circ \Lambda = 0 \mod (X^{q^m} - X), \quad \forall i \in \{1, \ldots, u\}.$$

Lemma 1 yields the following non-linear system of $u \times n$ equations

$$\begin{cases} (Y_i \circ \Lambda)(g_j) = (C_i \circ \Lambda)(g_j) \\ \deg_q \Lambda \leqslant t \\ \deg_q C_i \leqslant k-1, \quad \text{for } i \in \{1, \ldots, u\}. \end{cases} \tag{4}$$

which can be linearized into the following system, setting $N_i \stackrel{\text{def}}{=} C_i \circ \Lambda$:

$$\begin{cases} (Y_i \circ \Lambda)(g_j) = N_i(g_j) \\ \deg_q \Lambda \leqslant t \\ \deg_q N_i \leqslant k+t-1, \quad \text{for } i \in \{1, \ldots, u\}. \end{cases} \tag{5}$$

This system has $u \times n$ equations, and $t + 1 + u(k + t)$ unknowns, and therefore one can expect to retrieve $(\Lambda, N_1, \ldots, N_u)$ whenever $t \leqslant \frac{u}{u+1}(n-k)$. Since $N_i = C_i \circ \Lambda$, the codewords $C_1, \ldots, C_u$ can then be recovered by computing euclidean division on the right.

Remark 5. The decoding algorithm mentioned in [13,20] can be re-interpreted in terms of the aforementioned decoder. The present section permits in particular to shed light on the fact that previous algorithms are actually very comparable to Loidreau's original algorithm when acting on the right instead of acting on the left.

3.4 Application to cryptography: LIGA encryption scheme

Let $\mathbb{F}_{q^m}, \mathbb{F}_{q^{mu}}$ be two algebraic extensions of the finite field $\mathbb{F}_q$. In [6], Faure and Loidreau introduced a rank metric encryption scheme with small key size. The originality of the cryptosystem was to base the security on the hardness of decoding a (public) Gabidulin code beyond the unique decoding radius. Indeed, the public key was of the form $\boldsymbol{k}_{pub} = \boldsymbol{x}\boldsymbol{G} + \boldsymbol{z}$ where $\boldsymbol{G}$ is a generator matrix of a public $[n, k]$ Gabidulin code over $\mathbb{F}_{q^m}$ and $\boldsymbol{x} \in \mathbb{F}_{q^{mu}}^k$, $\boldsymbol{z} \in \mathbb{F}_{q^{mu}}^n$ together with $t \stackrel{\text{def}}{=} \mathbf{rank}_q(z) > \frac{n-k}{2}$ form the secret key.

However, it was shown in [9] that an attacker could easily compute u noisy codewords of the Gabidulin code generated by $\boldsymbol{G}$ using the $\mathbb{F}_{q^m}$–linearity of the trace map $\mathrm{Tr}_{\mathbb{F}_{q^{mu}}/\mathbb{F}_{q^m}}$, and then recover the secret providing that $t \leqslant \frac{u}{u+1}(n-k)$ (which was always the case to resist other attacks). This really amounts to decoding the public key with a decoder of u–interleaved Gabidulin codes. In order to repair the scheme, the authors of LIGA proposed instead to base the security on the hardness of decoding u–interleaved Gabidulin codes. Indeed, they proved that by reducing the rank of $\boldsymbol{z}$ over $\mathbb{F}_{q^m}$ (while keeping its rank weight t over $\mathbb{F}_q$ higher than the unique decoding radius), it was no longer possible to recover the secret key. More precisely, denoting by $\zeta \stackrel{\text{def}}{=} \mathbf{rank}_{q^m}(\boldsymbol{z})$ this rank, they proved by a careful analysis of known interleaved decoders that a condition for making the decoder to fail was $\zeta < \frac{t}{n-k-t}$. In particular, in LIGA they proposed to set $\zeta = 2$.

Using our decoder, we propose a new interpretation of this condition. Indeed, let $\boldsymbol{Y} = \boldsymbol{C} + \boldsymbol{E} \in \mathcal{M}_{u \times n}(\mathbb{F}_{q^m})$ be a noisy codeword of an u-interleaved Gabidulin code. The results of Section 3.3 can be strengthen as follows: If some rows of $\boldsymbol{E}$ share a linear dependency, then the equations in system (5) are no longer independent. In particular, if $\zeta \leqslant u$ denotes the rank of $\boldsymbol{E}$ over $\mathbb{F}_{q^m}$, one can refine the reasoning and deduce an equivalent linear system with $\zeta \times n$ independent equations for $t+1+\zeta(k+t)$ unkowns. Therefore, when $t > \frac{\zeta}{\zeta+1}(n-k)$, there are more unknowns than equations and the decoder fails. This inequality is exactly the condition $\zeta < \frac{t}{n-k-t}$ from LIGA.

Conclusion

We presented a full version of a right-hand side decoding algorithm for Gabidulin codes. This algorithm is close to a verbatim translation of its well–known left–hand counterpart. However, compared to its left–hand counterpart, it was unclear how to apply it to non full length Gabidulin codes. This issue has been addressed in the present article. Moreover, we claim that this algorithm is of interest for various applications. First, it provides a very natural approach for the decoding of interleaved Gabidulin codes. It is actually very comparable to the algorithm proposed by Loidreau and Overbeck [13] but the strong connection with a Berlekamp–Welch like decoder was not that clear in the aforementioned reference. Second, this right-hand side decoder already appeared to provide an interesting tool for cryptanalytic applications.

References

1. Aguilar Melchor, C., Aragon, N., Bettaieb, S., Bidoux, L., Blazy, O., Deneuville, J.C., Gaborit, P., Zémor, G.: Rank quasi cyclic (RQC). First round submission to the NIST post-quantum cryptography call (Nov 2017), `https://pqc-rqc.org`
2. Aragon, N., Blazy, O., Gaborit, P., Hauteville, A., Zémor, G.: Durandal: a rank metric based signature scheme. IACR Cryptology ePrint Archive (2018), `https://eprint.iacr.org/2018/1192`
3. Aragon, N., Gaborit, P., Hauteville, A., Ruatta, O., Zémor, G.: Ranksign – a signature proposal for the NIST's call. First round submission to the NIST post-quantum cryptography call (Nov 2017), `https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-1/submissions/RankSign.zip`

4. Bleichenbacher, D., Kiayias, A., Yung, M.: Decoding of interleaved Reed Solomon codes over noisy data. In: International Colloquium on Automata, Languages, and Programming. pp. 97–108. Springer (2003)
5. Bombar, M., Couvreur, A.: Decoding supercodes of Gabidulin codes and applications to cryptanalysis. In: Cheon, J.H., Tillich, J.P. (eds.) Post-Quantum Cryptography. pp. 3–22. Springer International Publishing, Cham (2021)
6. Faure, C., Loidreau, P.: 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. pp. 304–315 (2005)
7. Gabidulin, E.M.: Theory of codes with maximum rank distance. Problemy Peredachi Informatsii **21**(1), 3–16 (1985)
8. Gabidulin, E.M., Paramonov, A.V., Tretjakov, O.V.: Ideals over a non-commutative ring and their applications to cryptography. In: Advances in Cryptology - EUROCRYPT'91. pp. 482–489. No. 547 in LNCS, Brighton (Apr 1991)
9. Gaborit, P., Otmani, A., Talé-Kalachi, H.: Polynomial-time key recovery attack on the Faure-Loidreau scheme based on Gabidulin codes. Des. Codes Cryptogr. **86**(7), 1391–1403 (2018). https://doi.org/10.1007/s10623-017-0402-0, `https://doi.org/10.1007/s10623-017-0402-0`
10. Goss, D.: Basic Structures of Function Field arithmetic, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 35. Springer-Verlag, Berlin (1996)
11. Lavauzelle, J., Loidreau, P., Pham, B.D.: RAMESSES, a Rank Metric Encryption Scheme with Short Keys (Jan 2020), `https://hal.archives-ouvertes.fr/hal-02426624`, working paper or preprint
12. Loidreau, P.: A Welch–Berlekamp like algorithm for decoding Gabidulin codes. In: Ytrehus, Ø. (ed.) Coding and Cryptography. pp. 36–45. Springer Berlin Heidelberg, Berlin, Heidelberg (2006)
13. Loidreau, P., Overbeck, R.: Decoding rank errors beyond the error-correction capability. In: Proceedings of the Tenth International Workshop on Algebraic and Combinatorial Coding Theory, ACCT-10. pp. 168–190 (2006)
14. Raviv, N., Wachter-Zeh, A.: Some Gabidulin codes cannot be list decoded efficiently at any radius. In: 2015 IEEE International Symposium on Information Theory (ISIT). pp. 6–10 (2015)
15. Rawat, A.S., Koyluglu, O.O., Silberstein, N., Vishwanath, S.: Optimal locally repairable and secure codes for distributed storage systems. IEEE Trans. Inform. Theory **60**(1), 212–236 (2014)
16. Renner, J., Puchinger, S., Wachter-Zeh, A.: LIGA: A cryptosystem based on the hardness of rank–metric list and interleaved decoding. Des. Codes Cryptogr. **89**, 1279–1319 (2021)
17. Sheekey, J.: 13. MRD codes: constructions and connections, pp. 255–286. De Gruyter (2019)
18. Silva, D., Kschischang, F.R.: Universal secure network coding via rank-metric codes. IEEE Trans. Inform. Theory **57**(2), 1124–1135 (Feb 2011). https://doi.org/10.1109/TIT.2010.2090212
19. Wachter-Zeh, A.: Decoding of block and convolutional codes in rank metric. Ph.D. thesis, Université Rennes 1 (2013)
20. Wachter-Zeh, A., Zeh, A.: List and unique error-erasure decoding of interleaved Gabidulin codes with interpolation techniques. Des. Codes Cryptogr. **73**(2), 547–570 (2014)