# Randomized Decoding of Gabidulin Codes Beyond the Unique Decoding Radius

Julian Renner[1], Thomas Jerkovits[2], Hannes Bartz[2], Sven Puchinger[3], Pierre Loidreau[4], and Antonia Wachter-Zeh[1]

[1] Technical University of Munich (TUM), Munich, Germany
{julian.renner, antonia.wachter-zeh}@tum.de*
[2] German Aerospace Center (DLR), Oberpfaffenhofen-Wessling, Germany
{hannes.bartz, thomas.jerkovits}@dlr.de
[3] Technical University of Denmark (DTU), Lyngby, Denmark
svepu@dtu.dk**
[4] Univ Rennes, DGA MI, CNRS, IRMAR - UMR 6625, F-35000 Rennes, France
pierre.loidreau@univ-rennes1.fr

**Abstract.** We address the problem of decoding Gabidulin codes beyond their error-correcting radius. The complexity of this problem is of importance to assess the security of some rank-metric code-based cryptosystems. We propose an approach that introduces row or columns erasures to decrease the rank of the error in order to use any proper polynomial-time Gabidulin code error-erasure decoding algorithm. This approach improves on generic rank-metric decoders by an exponential factor.

**Keywords:** Gabidulin codes, decoding, rank metric, code-based cryptography

## 1 Introduction

In the Hamming metric as well as in the rank metric, it is well-known that the problem of decoding beyond the unique decoding radius, in particular *Maximum-Likelihood* (ML) decoding, is a difficult problem concerning the complexity. In Hamming metric, many works have analyzed how hard it actually is, cf. [5, 26], and it was finally shown for general linear codes that ML decoding is NP-hard by Vardy in [28]. For the rank metric, some complexity results were obtained more recently in [13], emphasizing the difficulty of ML decoding. This potential hardness was also corroborated by the existing practical complexities of the generic rank metric decoding algorithms [12].

* The work of J. Renner and A. Wachter-Zeh was supported by the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No 801434).

** Sven Puchinger has received funding from the European Union's Horizon 2020 research and innovation program under the Marie Sklodowska-Curie grant agreement no. 713683 (COFUNDfellowsDTU).

For specific well-known families of codes such as *Reed–Solomon* (RS) codes in the Hamming metric, (ML or list) decoding can be done efficiently up to a certain radius. Given a received word, an ML decoder returns *the* (or one if there is more than one) *closest codeword* to the received word whereas a list decoder returns *all codewords* up to a fixed radius. The existence of an efficient list decoder up to a certain radius therefore implies an efficient ML decoder up to the same radius. Vice versa, this is however not necessarily true, but we cannot apply a list decoder to solve the ML decoding problem efficiently.

In particular, for an RS code of length $n$ and dimension $k$, the following is known, depending on the Hamming weight $w$ of the error:

- If $w \leq \lfloor \frac{n-k}{2} \rfloor$, the (ML and list) decoding result is unique and can be found in quasi-linear time,
- If $w < n - \sqrt{n(k-1)}$, i.e., the weight of the error is less than the Johnson bound, list decoding and therefore also ML decoding can be done efficiently by Guruswami–Sudan's list decoding algorithm [14],
- The renewed interest in RS codes after the design of the Guruswami–Sudan list decoder [14] motivated new studies of the theoretical complexity of ML and list decoding of RS codes. In [15] it was shown that ML decoding of RS codes is indeed NP-hard when $w \geq d - 2$, even with some pre-processing.
- Between the Johnson radius and $d - 2$, it has been shown in [4] that the number of codewords in radius $w$ around the received word might become a number that grows super-polynomially in $n$ which makes list decoding of RS codes a hard problem. It has been shown by Rudra and Wootters [22] that over large enough alphabets, *most* RS codes can be efficiently list-decoded beyond the Johnson radius (which implies efficient ML decoding). This result has recently been improved and analyzed more precisely in [23], showing also that most RS codes of rate at most $1/9$ are list-decodable beyond the Johnson radius. However, these are combinatorial results and no efficient decoders for these codes are known.

*Gabidulin codes* [6, 9, 21] can be seen as the rank-metric analog of RS codes. ML decoding of Gabidulin codes is in the focus of this paper which is much less investigated than for RS codes (see the following discussion). However, both problems (ML decoding of RS and Gabidulin codes) are of cryptographic interest. The security of the public-key cryptosystem from [2] relied on the hardness of ML decoding of RS codes but was broken by a structural attack. More recently, some public-key cryptosystems base their security partly upon the difficulty of solving the problem Dec-Gab (Decisional-Gabidulin defined in the following) and Search-Gab (Search-Gabidulin), i.e., decoding Gabidulin codes beyond the unique decoding radius or derived instances of this problem [8, 31].

Dec-Gab has not been well investigated so far. Therefore, we are interested in designing efficient algorithms to solve Dec-Gab which in turn assesses the security of several public-key cryptosystems. We deal with analyzing the problem of decoding Gabidulin codes beyond the unique radius where a Gabidulin code of length $n$ and dimension $k$ is denoted by $Gab_k(\boldsymbol{g})$ and $\boldsymbol{g} = (g_0, g_1, \ldots, g_{n-1})$ denotes the vector of linearly independent code locators.

**Problem 1 (Dec-Gab)**

- *Instance:* $Gab_k(\boldsymbol{g}) \subset \mathbb{F}_{q^m}^n$, $\boldsymbol{r} \in \mathbb{F}_{q^m}^n$ *and an integer* $w > 0$.
- *Query: Is there a codeword* $\boldsymbol{c} \in Gab_k(\boldsymbol{g})$*, such that* $\mathrm{rk}(\boldsymbol{r} - \boldsymbol{c}) \leq w$*?*

It is trivial that Dec-Gab($Gab_k(\boldsymbol{g})$, $\boldsymbol{r}$, $w$) can be solved in deterministic polynomial time whenever:

- $w \leq \left\lfloor \frac{n-k}{2} \right\rfloor$, with applying a deterministic polynomial-time decoding algorithm for Gabidulin codes to $\boldsymbol{r}$.
- $w \geq n - k$: In this case the answer is always `yes` since this just tantamounts to finding a solution to an overdetermined full rank linear system (Gabidulin codes are *Maximum Rank Distance* codes).

However, between $\left\lfloor \frac{n-k}{2} \right\rfloor$ and $n-k$, the situation for Dec-Gab is less clear than for RS codes (which was analyzed above).

For instance, concerning RS codes, the results from [15] and [4] state that there is a point in the interval $[\left\lfloor \frac{n-k}{2} \right\rfloor, n-k]$ where the situation is not solvable in polynomial-time unless the polynomial hierarchy collapses. For RS codes, we can refine the interval to $[n-\sqrt{n(k-1)}, n-k]$, because of the Guruswami-Sudan polynomial-time list decoder up to Johnson bound [14].

On the contrary, for Gabidulin codes, there is no such a refinement. In [29], it was shown that for *all* Gabidulin codes, the list size grows exponentially in $n$ when $w > n - \sqrt{n(k-1)}$. Further, [19] showed that the size of the list is exponential for some Gabidulin codes as soon as $w = \left\lfloor \frac{n-k}{2} \right\rfloor + 1$. This result was recently generalized in [27] to other classes of Gabidulin codes (e.g., twisted Gabidulin codes) and, more importantly, it showed that any Gabidulin code of dimension at least two can have an exponentially-growing list size for $w \geq \left\lfloor \frac{n-k}{2} \right\rfloor + 1$.

To solve the decisional problem Dec-Gab we do not know a better approach than trying to solve the associated *search* problem, which is usually done for all decoding-based problems.

**Problem 2 (Search-Gab)**

- *Instance:* $Gab_k(\boldsymbol{g}) \subset \mathbb{F}_{q^m}^n$, $\boldsymbol{r} \in \mathbb{F}_{q^m}^n$ *and* $w > 0$ *integer*
- *Search for a codeword* $\boldsymbol{c} \in Gab_k(\boldsymbol{g})$*, such that* $\mathrm{rk}(\boldsymbol{r} - \boldsymbol{c}) \leq w$

Since Dec-Gab and Search-Gab form the security core of some rank-metric based cryptosystems, it necessary to evaluate the effective complexity of solving these problems to be able to parametrize the systems in terms of security.

In this paper, we propose a randomized approach to solve Search-Gab in the most efficient way and analyze its work factor.

## 2 Preliminaries

### 2.1 Notation

Let $q$ be a power of a prime and let $\mathbb{F}_q$ denote the finite field of order $q$ and $\mathbb{F}_{q^m}$ its extension field of order $q^m$. This definition includes the important cases for cryptographic applications $q = 2$ or $q = 2^r$ for a small positive integer $r$. It is well-known that any element of $\mathbb{F}_q$ can be seen as an element of $\mathbb{F}_{q^m}$ and that $\mathbb{F}_{q^m}$ is an $m$-dimensional vector space over $\mathbb{F}_q$.

We use $\mathbb{F}_q^{m \times n}$ to denote the set of all $m \times n$ matrices over $\mathbb{F}_q$ and $\mathbb{F}_{q^m}^n = \mathbb{F}_{q^m}^{1 \times n}$ for the set of all row vectors of length $n$ over $\mathbb{F}_{q^m}$. Rows and columns of $m \times n$-matrices are indexed by $1, \ldots, m$ and $1, \ldots, n$, where $A_{i,j}$ is the element in the $i$-th row and $j$-th column of the matrix $\boldsymbol{A}$. In the following of the paper, we will always consider that $n \leq m$. This is the necessary and sufficient condition to design Gabidulin codes.

For a vector $\boldsymbol{a} \in \mathbb{F}_{q^m}^n$, we define its ($\mathbb{F}_q$-)rank by $\mathrm{rk}(\boldsymbol{a}) := \dim_{\mathbb{F}_q} \langle a_1, \ldots, a_n \rangle_{\mathbb{F}_q}$, where $\langle a_1, \ldots, a_n \rangle_{\mathbb{F}_q}$ is the $\mathbb{F}_q$-vector space spanned by the entries $a_i \in \mathbb{F}_{q^m}$ of $\boldsymbol{a}$. Note that this rank equals the rank of the matrix representation of $\boldsymbol{a}$, where the $i$-th entry of $\boldsymbol{a}$ is column-wise expanded into a vector in $\mathbb{F}_q^m$ w.r.t. a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$.

The Grassmannian $\mathcal{G}(\mathcal{V}, k)$ of a vector space $\mathcal{V}$ is the set of all $k$-dimensional subspaces of $\mathcal{V}$.

A linear code over $\mathbb{F}_{q^m}$ of length $n$ and dimension $k$ is a $k$-dimensional subspace of $\mathbb{F}_{q^m}^n$ and denoted by $[n, k]_{\mathbb{F}_{q^m}}$.

### 2.2 Gabidulin Codes and Channel Model

Gabidulin codes are a special class of rank-metric codes and can be defined by a generator matrix as follows. The codes are maximum rank distance (MRD) codes, i.e., they attain the maximal possible minimum distance $d = n - k + 1$ for a given length $n$ and dimension $k$ [9].

**Definition 1 (Gabidulin Code [9]).** *A linear $Gab_k(\mathbf{g})$ code over $\mathbb{F}_{q^m}$ of length $n \leq m$ and dimension $k$ is defined by its $k \times n$ generator matrix*

$$\boldsymbol{G}_{\mathrm{Gab}} = \begin{pmatrix} g_0 & g_1 & \cdots & g_{n-1} \\ g_0^q & g_1^q & \cdots & g_{n-1}^q \\ \vdots & \vdots & \ddots & \vdots \\ g_0^{q^{k-1}} & g_1^{q^{k-1}} & \cdots & g_{n-1}^{q^{k-1}} \end{pmatrix} \in \mathbb{F}_{q^m}^{k \times n},$$

*where $g_0, g_1, \ldots, g_{n-1} \in \mathbb{F}_{q^m}$ are linearly independent over $\mathbb{F}_q$.*

Let $\boldsymbol{r} \in \mathbb{F}_{q^m}^n$ be a codeword of a Gabidulin code of length $n \leq m$ and dimension $k$ that is corrupted by an error of rank weight $w$, i.e.,

$$\boldsymbol{r} = \boldsymbol{m}\boldsymbol{G}_{\mathrm{Gab}} + \boldsymbol{e},$$

where $\boldsymbol{m} \in \mathbb{F}_{q^m}^k$, $\boldsymbol{G}_{\mathrm{Gab}} \in \mathbb{F}_{q^m}^{k \times n}$ is a generator matrix of an $[n, k]$ Gabidulin code and $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ with $\mathrm{rk}(\boldsymbol{e}) = w > \frac{n-k}{2}$. Each error $\boldsymbol{e}$ of rank weight $w$ can be decomposed into

$$\boldsymbol{e} = \boldsymbol{a}\boldsymbol{B},$$

where $\boldsymbol{a} \in \mathbb{F}_{q^m}^w$ and $\boldsymbol{B} \in \mathbb{F}_q^{w \times n}$. The subspace $\langle a_1, \ldots, a_w \rangle_{\mathbb{F}_q}$ is called the column space of the error and the subspace spanned by the rows of $\boldsymbol{B}$, i.e. $\mathcal{R}_{\mathbb{F}_q}\left(\boldsymbol{B}\right)$, is called the row space of the error.

We define the excess of the error weight $w$ over the unique decoding radius as

$$\xi := w - \frac{n-k}{2}.$$

Note that $2\xi$ is always an integer, but $\xi$ does not necessarily need to be one.

The error $\boldsymbol{e}$ can be further decomposed into

$$\boldsymbol{e} = \boldsymbol{a}_{\mathrm{C}} \boldsymbol{B}_{\mathrm{C}} + \boldsymbol{a}_{\mathrm{R}} \boldsymbol{B}_{\mathrm{R}} + \boldsymbol{a}_{\mathrm{E}} \boldsymbol{B}_{\mathrm{E}}, \tag{1}$$

where $\boldsymbol{a}_{\mathrm{C}} \in \mathbb{F}_{q^m}^{\gamma}$, $\boldsymbol{B}_{\mathrm{C}} \in \mathbb{F}_q^{\gamma \times n}$, $\boldsymbol{a}_{\mathrm{R}} \in \mathbb{F}_{q^m}^{\rho}$, $\boldsymbol{B}_{\mathrm{R}} \in \mathbb{F}_q^{\rho \times n}$, $\boldsymbol{a}_{\mathrm{E}} \in \mathbb{F}_{q^m}^{t}$ and $\boldsymbol{B}_{\mathrm{E}} \in \mathbb{F}_q^{t \times n}$.

Assuming neither $\boldsymbol{a}_{\mathrm{E}}$ nor $\boldsymbol{B}_{\mathrm{E}}$ are known, the term $\boldsymbol{a}_{\mathrm{E}} \boldsymbol{B}_{\mathrm{E}}$ is called full rank errors. Further, if $\boldsymbol{a}_{\mathrm{C}}$ is unknown but $\boldsymbol{B}_{\mathrm{C}}$ is known, the product $\boldsymbol{a}_{\mathrm{C}} \boldsymbol{B}_{\mathrm{C}}$ is called column erasures and assuming $\boldsymbol{a}_{\mathrm{R}}$ is known but $\boldsymbol{B}_{\mathrm{R}}$ is unknown, the vector $\boldsymbol{a}_{\mathrm{R}} \boldsymbol{B}_{\mathrm{R}}$ is called row erasures, see [25, 30]. There exist efficient algorithms for Gabidulin codes [10, 20, 24, 30] that can correct $\delta := \rho + \gamma$ erasures (sum of row and column erasures) and $t$ errors if

$$2t + \delta \leq n - k. \tag{2}$$

## 3 Solving Problem 2 Using Generic RSD Algorithms

A generic RSD decoder is an algorithm which solves Problem 2 where the Gabidulin code is replaced by a random code $\mathcal{C}$ with the same parameters. There are potentially many solutions to the decoding problem related to Problem 2 but we consider that it is sufficient to find only one solution.

Given a target vector $\boldsymbol{r}$ to Problem 2 instantiated by a random code, the probability that $\boldsymbol{c} \in \mathcal{C}$ is such that $\mathrm{rk}(\boldsymbol{r} - \boldsymbol{c}) \leq w$ satisfies

$$\Pr_{\boldsymbol{c} \in \mathcal{C}}[\mathrm{rk}(\boldsymbol{r} - \boldsymbol{c}) \leq w] = \frac{\sum_{i=0}^{w-1} \left[\prod_{j=0}^{i-1} (q^m - q^j)\right] \begin{bmatrix} n \\ i \end{bmatrix}_q}{q^{mk}}$$

There are two standards approach to solving Problem 2:

- *Combinatorial decoding:* It consists in enumerating vector spaces and specifying some variables. The complexity for an $[n, k]_{\mathbb{F}_{q^m}}$ code decoding errors of rank $w$ if there is only one solution to the problem is equal to [1]

  $$\mathcal{W}_{Comb} = P(n, k) q^{w\lceil (k+1)m/n \rceil - m}.$$

  Where essentially, $P(n, k)$ is a cubic polynomial. In the security evaluations, this polynomial is often neglegted and only the exponential term is taken into account. Note that in the case where $m > n$ there might be a better

combinatorial bound [12], but since we do not address this setting, we do not consider this case.
In the quantum setting Grover algorithm improves on the bound, since the complexity of enumeration is square-rooted. Thus the estimated complexity is

$$\mathcal{W}_{PQ\_Comb} = P(n,k) q^{0.5(w\lceil (k+1)m/n \rceil - m)}.$$

Since this is enumerative approache the workfactors for solving the problem on input $\boldsymbol{r}$ have to be divided by $\mathcal{N} = \max(|\mathcal{C}| \cdot \Pr_{\boldsymbol{c}\in\mathcal{C}}[\mathrm{rk}(\boldsymbol{r}-\boldsymbol{c}) \leq w], 1)$, corresponding to the estimated number of candidates.

– *Algebraic decoding:* It consists in expressing the problem under the form of a multivariate polynomial system and compute a Gröbner basis to solve it. A very recent result estimates rather precisely the cost of the attack and gives generally much better estimations than the combinatorial approach, [3]. Though it works when there is a unique solution to the system, we estimate it as an upper bound to solving the problem.
  - If $m\binom{n-k-1}{w} \leq \binom{n}{w}$ then the work factor of the algorithm is

$$\mathcal{W}_{Alg} = O\left(\left[\frac{((m+n)w)^w}{w!}\right]^\mu\right)$$

  - Else

$$\mathcal{W}_{Alg} = O\left(\left[\frac{((m+n)w)^{w+1}}{(w+1)!}\right]^\mu\right)$$

  where $\mu = 2.807$ is the linear algebra constant. In this case, there is no known way to improve the complexity by using the fact that there are multiple solutions, nor one knows how to speed up the algorithm in the quantum world. Note that in [3], the result only applies to the case where $q = 2$. Further investigations would be necessary to analyze the cases where $q \neq 2$. Contrarily to the combinatorial approach, it is not clear how to use the property that Problem 2 might have more than one solution.

*Example 1.* Suppose the parameters of the problem are $m = n = 64,\ k = 32$ and $w = 19$. Then the estimated list size is $2^{24.8}$.

– *Combinatorial decoding:* By dividing the complexity of the attack by the number of solutions we obtain an estimated average complexity of $2^{571.21}$.
– *Algebraic decoding:* We are in the second case and the estimated work factor would be approximately $2^{435.22}$.

In the following we will see how to improve this complexity by using the fact that there is an underlying Gabidulin code.

## 4 A New Algorithm Solving Problem 2

In the considered problem, $\mathrm{rk}(\boldsymbol{e}) = w > \frac{n-k}{2}$ and we do not have any knowledge about the row space or the column space of the error, i.e., $\delta = 0$ and $t > \frac{n-k}{2}$, meaning that the known decoders are not able to decode $\boldsymbol{r}$ efficiently.

The idea of the proposed algorithm is to guess parts of the row space and/or the column space of the error and use a basis for the guessed spaces to solve the corresponding error and column/row erasures (see (1)). This approach is a generalization of the algorithm used in [17], where only criss-cross erasures are used to decode certain error patterns beyond the unique decoding radius.

In the following, we denote by $\delta$ the total number of guessed dimensions (sum of guessed dimensions of the row space and the column space) and by $\epsilon$ the dimension of the intersection of our guess and the true error subspaces. As stated above, if

$$2(w-\epsilon)+\delta \leq n-k, \tag{3}$$

any Gabidulin error-erasure decoder is able to correct the error, e.g., [25, 30].

**Lemma 1.** *Let $\mathcal{U}$ be a fixed $u$-dimensional $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^\ell}$. Let $\mathcal{V}$ be chosen uniformly at random from $\mathcal{G}(\mathbb{F}_{q^\ell}, v)$. Then, the probability that the intersection of $\mathcal{U}$ and $\mathcal{V}$ has dimension at least $\omega$ is*

$$\begin{aligned}\Pr[\dim(\mathcal{U}\cap\mathcal{V})\geq\omega] &= \frac{\sum_{i=\omega}^{\min\{u,v\}}\begin{bmatrix}\ell-u\\v-i\end{bmatrix}_q\begin{bmatrix}u\\i\end{bmatrix}_q q^{(u-i)(v-i)}}{\begin{bmatrix}\ell\\v\end{bmatrix}_q}\\ &\leq 16(\min\{u,v\}+1-\omega)q^{(j^*-v)(\ell-u-j^*)},\end{aligned}$$

*where* $j^* := \min\{v-\omega, \frac{1}{2}(\ell+v-u)\}$.

*Proof.* The number of $q$-vector spaces of dimension $v$, which intersections with $\mathcal{U}$ have dimension at least $\omega$, is equal to

$$\sum_{i=\omega}^{\min\{u,v\}}\begin{bmatrix}\ell-u\\v-i\end{bmatrix}_q\begin{bmatrix}u\\i\end{bmatrix}_q q^{(u-i)(v-i)} = \sum_{j=\max\{0,v-u\}}^{v-\omega}\begin{bmatrix}\ell-u\\j\end{bmatrix}_q\begin{bmatrix}u\\v-j\end{bmatrix}_q q^{j(u-v+j)},$$

see [7]. Since the total number of $v$-dimensional subspaces of a $\ell$-dimensional space is equal to $\begin{bmatrix}\ell\\v\end{bmatrix}_q$, the probability

$$\begin{aligned}\Pr[\dim(\mathcal{U}\cap\mathcal{V})\geq\omega] &= \frac{\sum_{i=\omega}^{\min\{u,v\}}\begin{bmatrix}\ell-u\\v-i\end{bmatrix}_q\begin{bmatrix}u\\i\end{bmatrix}_q q^{(u-i)(v-i)}}{\begin{bmatrix}\ell\\v\end{bmatrix}_q}\\ &= \frac{\sum_{j=\max\{0,v-u\}}^{v-\omega}\begin{bmatrix}\ell-u\\j\end{bmatrix}_q\begin{bmatrix}u\\v-j\end{bmatrix}_q q^{j(u-v+j)}}{\begin{bmatrix}\ell\\v\end{bmatrix}_q}.\end{aligned}$$

Using the upper bound on the Gaussian coefficient derived in [18, Lemma 4], it follows that

$$\begin{aligned}\Pr[\dim(\mathcal{U}\cap\mathcal{V})\geq\omega] &\leq 16\sum_{j=\max\{0,v-u\}}^{v-\omega} q^{j(\ell-u-j)+v(u-v+j)-v(\ell-v)}\\ &= 16\sum_{j=\max\{0,v-u\}}^{v-\omega} q^{(j-v)(\ell-u-j)}\\ &\leq 16\,(\min\{u,v\}+1-\omega)q^{(j^*-v)(\ell-u-j^*)},\end{aligned}$$

where $j^* := \min\{v-\omega, \frac{1}{2}(\ell+v-u)\}$. The latter inequality follows from the fact that the term $(j-v)(\ell-u-j)$ is a concave function in $j$ and is maximum for $j=\frac{1}{2}(\ell+v-u)$.

In the following, we analyze guessing only the row space of the error, i.e., $\delta=\gamma$ and $\rho=0$.

**Lemma 2.** *Let $\boldsymbol{r}'=\boldsymbol{m}\boldsymbol{G}_{\text{Gab}}+\boldsymbol{e}'\in\mathbb{F}_{q^m}^n$, where $\text{rk}(\boldsymbol{e}')=j$, $\boldsymbol{e}'=\boldsymbol{a}'\boldsymbol{B}'$ with $\boldsymbol{a}'\in\mathbb{F}_{q^m}^j$, $\boldsymbol{B}'\in\mathbb{F}_q^{j\times n}$ and neither parts of the error row space nor column space are known, i.e., $\gamma=\rho=0$ and $t=j$. For $\delta\in[2\xi,n-k]$, the probability that an error-erasure decoder using a random $\delta$-dimensional guess of the error row space outputs $\boldsymbol{m}\boldsymbol{G}_{\text{Gab}}$ is*

$$\begin{aligned}P_{n,k,\delta,j} &:= \frac{\sum_{i=\lceil j-\frac{n-k}{2}+\frac{\delta}{2}\rceil}^{\min\{\delta,j\}} \begin{bmatrix} n-j\\ \delta-i\end{bmatrix}_q \begin{bmatrix} j\\ i\end{bmatrix}_q q^{(j-i)(\delta-i)}}{\begin{bmatrix} n\\ \delta\end{bmatrix}_q}\\ &\leq 16nq^{-(\lceil\frac{\delta}{2}+j-\frac{n-k}{2}\rceil)(\frac{n+k}{2}-\lceil\frac{\delta}{2}\rceil)},\end{aligned}$$

*if $2j+\delta>n-k$ and $P_{n,k,\delta,j}:=1$ else.*

*Proof.* First, consider the case where $2j+\delta>n-k$ and define $\xi'=j-\frac{n-k}{2}$. Let the rows of $\hat{\boldsymbol{B}}_{\text{C}}\in\mathbb{F}_q^{\delta\times n}$ be a basis of the random guess. From (3) follows that if

$$n-k\geq 2j-2\epsilon+\delta = n-k+2\xi'-2\epsilon+\delta, \tag{4}$$

where $\epsilon$ is the dimension of the intersection of the $\mathbb{F}_q$-row spaces of $\hat{\boldsymbol{B}}_{\text{C}}$ and $\boldsymbol{B}'$, an error and erasure decoder is able to decode efficiently. Since $\epsilon\leq\delta$, equation (4) gives a lower bound on the dimension $\delta$ of the subspace that we have to estimate:

$$2\xi'\leq 2\epsilon-\delta\leq\delta\leq n-k. \tag{5}$$

From (4) follows further that the estimated space doesn't have to be a subspace of the row space of the error. In fact, it is sufficient that the dimension of the intersection of the estimated column space and the true column space has dimension

$\epsilon \geq \xi' + \frac{\delta}{2}$. This condition is equivalent to the condition that the subspace distance (see [18]) between $\mathcal{U}$ and $\mathcal{V}$ satisfies $d_s(\mathcal{U},\mathcal{V}) := \dim(\mathcal{U}) + \dim(\mathcal{V}) - 2\dim(\mathcal{U}\cap\mathcal{V}) \geq j - 2\xi'$.

From Lemma 1 follows that the probability that the randomly guessed space intersects in enough dimensions such that an error-erasure decoder can decode to one particular codeword in distance $j$ to $\boldsymbol{r}$ is

$$\begin{aligned}
&\frac{\sum_{i=\lceil \xi' + \frac{\delta}{2}\rceil}^{\min\{\delta,j\}} \begin{bmatrix} n-j \\ \delta-i \end{bmatrix}_q \begin{bmatrix} j \\ i \end{bmatrix}_q q^{(j-i)(\delta-i)}}{\begin{bmatrix} n \\ \delta \end{bmatrix}_q} \\
\leq &16\Big(\min\{j,\delta\} + 1 - \Big(\xi' + \frac{\delta}{2}\Big)\Big)\, q^{-(\lceil \frac{\delta}{2} + \xi' \rceil)(\frac{n+k}{2} - \lceil \frac{\delta}{2}\rceil)} \\
\leq &16 n q^{-(\lceil \frac{\delta}{2} + \xi' \rceil)(\frac{n+k}{2} - \lceil \frac{\delta}{2}\rceil)}.
\end{aligned}$$

For the case $2j + \delta \leq n - k$, it is well known that that an error erasure decoder always outputs $\boldsymbol{m}\boldsymbol{G}_{\mathrm{Gab}}$. □

Lemma 2 gives the probability that the error-erasure decoder outputs exactly the codeword $\boldsymbol{m}\boldsymbol{G}_{\mathrm{Gab}}$. Depending on the application, it might not be necessary to find exactly $\boldsymbol{m}\boldsymbol{G}_{\mathrm{Gab}}$ but any codeword $\boldsymbol{c} \in \mathcal{C}_{\mathcal{G}}$ such that $\mathrm{rk}(\boldsymbol{r} - \boldsymbol{c}) \leq w$, which corresponds to Problem 2. In the following lemma, we derive an upper bound on the success probability of solving Problem 2 using the proposed algorithm.

**Lemma 3.** *Let $\boldsymbol{r}$ be a uniformly distributed random element of $\mathbb{F}_{q^m}^n$. Then, for $\delta \in [2\xi, n-k]$ the probability that an error-erasure decoder using a random $\delta$-dimensional guess of the error row space outputs $\boldsymbol{c} \in \mathcal{C}_{\mathcal{G}}$ such that $\mathrm{rk}(\boldsymbol{r} - \boldsymbol{c}) \leq w$ is smaller or equal to*

$$\sum_{j=0}^{w} \bar{A}_j P_{n,k,\delta,j} \leq 64 n q^{m(k-n) + w(n+m) - w^2 - (\lceil \frac{\delta}{2} + w - \frac{n-k}{2} \rceil)(\frac{n+k}{2} - \lceil \frac{\delta}{2} \rceil)},$$

*where* $\bar{A}_j = q^{m(k-n)} \prod_{i=0}^{j-1} \frac{(q^m - q^i)(q^n - q^i)}{q^j - q^i}$.

*Proof.* Let $\hat{\mathcal{C}}$ be the set of codewords that have rank distance at most $w$ from the received word, i.e.,

$$\hat{\mathcal{C}} := \{\boldsymbol{c} \in \mathcal{C}_{\mathcal{G}} : \mathrm{rk}(\boldsymbol{r} - \boldsymbol{c}) \leq w\} = \{\hat{\boldsymbol{c}}_1, \ldots, \hat{\boldsymbol{c}}_{\mathcal{N}}\}.$$

Further, let $X_i$ be the event that the error-erasure decoder outputs $\hat{\boldsymbol{c}}_i$ for $i = 1, \ldots, \mathcal{N}$ and $\mathcal{A}_j := \{i : \mathrm{rk}(\boldsymbol{r} - \hat{\boldsymbol{c}}_i) = j\}$. Observe that $P_{n,k,\delta,j} = \Pr[X_i]$ for $i \in \mathcal{A}_j$, where $\Pr[X_i]$ is the probability that the error-erasure decoder outputs $\hat{\boldsymbol{c}}_i$ and $P_{n,k,\delta,j}$ is defined as in Lemma 2. Then we can write

$$\Pr[\mathit{success}] = \Pr\left[\bigcup_{i=1}^{\mathcal{N}} X_i\right] \leq \sum_{i=1}^{\mathcal{N}} \Pr[X_i] = \sum_{j=0}^{w} |\mathcal{A}_j| P_{n,k,\delta,j}.$$

Let $\bar{A}_j$ be the average cardinality of the set $\mathcal{A}_j$, we have that

$$\bar{A}_j = q^{m(k-n)} \prod_{i=0}^{j-1} \frac{(q^m - q^i)(q^n - q^i)}{q^j - q^i} \leq 4q^{m(k-n)+j(n+m)-j^2}.$$

Since $\bar{A}_w$ is exponentially larger than $\bar{A}_{w-i}$ for $i > 0$, one can approximate

$$\begin{aligned} \Pr[success] &= \bar{A}_w P_{n,k,\delta,w} \\ &\leq 64nq^{m(k-n)+w(n+m)-w^2-(\lceil \frac{\delta}{2}+w-\frac{n-k}{2}\rceil)(\frac{n+k}{2}-\lceil\frac{\delta}{2}\rceil)}. \end{aligned}$$

The pseudocode for the proposed algorithm is given in Algorithm 1. Let $\mathsf{Dec}(\boldsymbol{r}, \boldsymbol{a}_R, \boldsymbol{B}_C)$ denote a row/column error-erasure decoder for the Gabidulin code $Gab_k(\boldsymbol{g})$ that returns a codeword $\hat{\boldsymbol{c}}$ (if $\mathrm{rk}(\boldsymbol{r} - \hat{\boldsymbol{c}}) \leq t + \rho + \gamma$) or $\emptyset$ (decoding failure).

**Algorithm 1:** Column-Erasure-Aided Generic Decoder

**Input :** Received word $\boldsymbol{r} \in \mathbb{F}_{q^m}^n$,
Gabidulin error/erasure decoder $\mathsf{Dec}(\cdot, \cdot, \cdot)$,
Dimension of guessed row space $\delta$,
Error weight $w$,
Maximum number of iterations $N_{max}$

**Output:** $\hat{\boldsymbol{c}} \in \mathbb{F}_{q^m}^n : \mathrm{rk}(\boldsymbol{r} - \hat{\boldsymbol{c}}) \leq w$ or $\emptyset$ (failure)

**foreach** $i \in [1, N_{max}]$ **do**
  $\mathcal{U} \xleftarrow{\$} \mathcal{G}(\mathbb{F}_q^n, \delta)$ `// guess` $\delta$`-dimensional subspace of` $\mathbb{F}_q^n$
  $\boldsymbol{B}_C \leftarrow$ full-rank matrix whose row space equals $\mathcal{U}$
  $\hat{\boldsymbol{c}} \leftarrow \mathsf{Dec}(\boldsymbol{r}, \boldsymbol{0}, \boldsymbol{B}_C)$ `// error and row erasure decoding`
  **if** $\hat{\boldsymbol{c}} \neq \emptyset$ **then**
    **if** $\mathrm{rk}(\boldsymbol{r} - \hat{\boldsymbol{c}}) \leq w$ **then**
      **return** $\hat{\boldsymbol{c}}$

**return** $\emptyset$ *(failure)*

**Theorem 1.** *Let $\boldsymbol{r}$ be a uniformly distributed random element of $\mathbb{F}_{q^m}^n$. Then, the proposed Algorithm 1 requires on average at least*

$$\begin{aligned}
\mathcal{W}_{GD} &= \min_{\delta \in [2\xi, n-k]} \left\{ \frac{n^2}{\sum_{j=0}^{w} \bar{A}_j P_{n,k,\delta,j}} \right\} \qquad (6)\\
&= \min_{\delta \in [2\xi, n-k]} \left\{ \frac{n^2 \begin{bmatrix} n \\ \delta \end{bmatrix}_q}{\sum_{j=0}^{\lfloor \frac{n-k-\delta}{2} \rfloor} q^{m(k-n)} \prod_{\ell=0}^{j-1} \frac{(q^m - q^\ell)(q^n - q^\ell)}{q^j - q^\ell} + \sum_{j=\lfloor \frac{n-k-\delta}{2} \rfloor + 1}^{w} q^{m(k-n)} \cdots \left( \prod_{\ell=0}^{j-1} \frac{(q^m - q^\ell)(q^n - q^\ell)}{q^j - q^\ell} \right) \left( \sum_{i=\lceil j - \frac{n-k}{2} + \frac{\delta}{2} \rceil}^{\min\{\delta, j\}} \begin{bmatrix} n-j \\ \delta - i \end{bmatrix}_q \begin{bmatrix} j \\ i \end{bmatrix}_q q^{(j-i)(\delta-i)} \right)} \right\}\\
&\geq \frac{n}{64} \cdot q^{m(n-k) - w(n+m) + w^2 + \min\{2\xi(\frac{n+k}{2} - \xi), wk\}}
\end{aligned}$$

*operations to output $\boldsymbol{c} \in Gab_k(\boldsymbol{g})$, such that* $\mathrm{rk}(\boldsymbol{r} - \boldsymbol{c}) \leq w$.

*Proof.* Lemma 3 gives the probability that an error-erasure decoder using a $\delta$ dimensional guess of the row space finds $\boldsymbol{c} \in \mathcal{C}_{\mathcal{G}}$ such that $\mathrm{rk}(\boldsymbol{r} - \boldsymbol{c}) \leq w$. This means that one has to estimate on average at least

$$\min_{\delta \in [2\xi, n-k]} \left\{ \frac{1}{\sum_{j=0}^{w} \bar{A}_j P_{n,k,\delta,j}} \right\}$$

row spaces in order to output $\boldsymbol{c} \in Gab_k(\boldsymbol{g})$. Since the complexity of error-erasure decoding is in $O(n^2)$, we get a work factor of

$$\mathcal{W}_{GD} = \min_{\delta \in [2\xi, n-k]} \left\{ \frac{n^2}{\sum_{j=0}^{w} \bar{A}_j P_{n,k,\delta,j}} \right\}.$$

One observes that the upper bound on the probability given in Lemma 3 is a convex function in $\delta$ and maximized for either $2\xi$ or $n-k$. Thus, we get lower bound on the work factor of

$$\frac{n}{64} \cdot q^{m(n-k) - w(n+m) + w^2 + \min\{2\xi(\frac{n+k}{2} - \xi), wk\}}.$$

□

If $\boldsymbol{r} \in \mathbb{F}_{q^m}^n$ is defined as in Section 2.2, where neither parts of the error row space nor column space are known, i.e., $\gamma = \rho = 0$ and $t = w$, the vector $\boldsymbol{r}$ can be seen as a uniformly distributed random element of $\mathbb{F}_{q^m}^n$. Thus, Theorem 1 gives an estimation of the workfactor of the proposed algorithm to solve Problem 2. To verify this assumption, we conducted simulations which show that the estimation is very accurate, see Section 5.

*Remark 1.* In Theorem 1, we give a lower bound on the workfactor of the proposed algorithm. One observes that especially for small parameters, this bound is not tight which is mainly caused by the approximations of the Gaussian binomials. For larger values, the relative difference to the true workfactor becomes smaller.

Another idea is to guess only the column space or the row and column space jointly. Guessing the column space is never advantageous over guessing the row space for Gabidulin codes since we always have $n \leq m$. Hence, replacing $n$ by $m$ in the formulas of Lemma 2 and in the expression of the probability $P_j$ inside the proof of Theorem 3 would only increase the resulting work factor. For joint guessing, some examples indicate that it is not advantageous, either. See Appendix A for more details.

## 5 Examples and Simulation Results

We validated the bounds on the work factor of the proposed algorithm in Section 4 by simulations. The simulations were performed with the row/column error-erasure decoder from [30] that can correct $t$ rank errors, $\rho$ row erasures and $\gamma$ column erasures up to $2t + \rho + \gamma \leq d - 1$. Alternatively, the decoders in [11, 25] may be considered.

The results in Table 1 show, that the proposed algorithm solves Problem 2 with a significantly lower computational complexity than the fastest generic decoding algorithms. One can also observe that the derived lower bounds on the work factor give a good estimate of the actual runtime of the algorithm.

## 6 Open Problems

There is a list decoding algorithm for Gabidulin codes based Gröbner bases that allows to correct errors beyond the unique decoding radius [16]. However, there is no upper bound on the list size and the complexity of the decoding algorithm. In future work, the algorithm from [16] should be adapted to solve Problem 2 which could allow for estimating the complexity of the resulting algorithm.

## References

1. Aragon, N., Gaborit, P., Hauteville, A., Tillich, J.: A new algorithm for solving the rank syndrome decoding problem. In: IEEE Int. Symp. Inform. Theory (ISIT). pp. 2421–2425 (June 2018). https://doi.org/10.1109/ISIT.2018.8437464

**Table 1.** Comparison of workfactors $\mathcal{W}_{GD}$, $\mathcal{W}_{Comb}$ and $\mathcal{W}_{Alg}$ for several parameter sets including simulation results for one specific parameter set.

| $q$ | $m$ | $n$ | $k$ | $w$ | $\xi$ | $\delta$ | Iterations | Success | $\mathcal{W}_{Sim}$ | $\mathcal{W}_{GD}$ | $\frac{\mathcal{W}_{Comb}}{\mathcal{N}}$ | $\mathcal{W}_{Alg}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 | 24 | 24 | 16 | 6 | 2 | 4 | 6844700 | 4488 | $2^{19.74}$ | $2^{19.65}$ | $2^{38.99}$ | $2^{126.01}$ |
| 2 | 64 | 64 | 32 | 19 | 3 | 6 | - | - | - | $2^{257.20}$ | $2^{571.21}$ | $2^{460.01}$ |
| 2 | 80 | 80 | 40 | 23 | 3 | 6 | - | - | - | $2^{401.85}$ | $2^{897.93}$ | $2^{576.15}$ |
| 2 | 96 | 96 | 48 | 27 | 3 | 6 | - | - | - | $2^{578.38}$ | $2^{1263.51}$ | $2^{694.93}$ |
| 2 | 61 | 61 | 31 | 16 | 1 | 2 | - | - | - | $2^{233.48}$ | $2^{483.51}$ | $2^{385.92}$ |
| 2 | 62 | 62 | 31 | 17 | 1.5 | 3 | - | - | - | $2^{248.12}$ | $2^{514.72}$ | $2^{410.50}$ |
| 2 | 83 | 83 | 48 | 21 | 3.5 | 7 | - | - | - | $2^{304.96}$ | $2^{838.72}$ | $2^{530.39}$ |


2. Augot, D., Finiasz, M.: A public key encryption scheme based on the polynomial reconstruction problem. In: Adv. in Crypt. - EUROCRYPT 2003. vol. 2656, pp. 229–240. Springer (2003)
3. Bardet, M., Briaud, P., Bros, M., Gaborit, P., Neiger, V., Ruatta, O., Tillich, J.P.: An algebraic attack on rank metric code-based cryptosystems. Tech. rep. (2019), arXiv:1910.00810v1
4. Ben-Sasson, E., Kopparty, S., Radhakrishnan, J.: Subspace polynomials and limits to list decoding of Reed–Solomon codes. IEEE Trans. Inform. Theory **56**(1), 113–120 (Jan 2010). https://doi.org/10.1109/TIT.2009.2034780
5. Berlekamp, E., McEliece, R.J., van Tilborg, H.: On the inherent intractability of certain coding problems. IEEE Trans. Inform. Theory **24**(3), 384–386 (May 1978)
6. Delsarte, P.: Bilinear forms over a finite field with applications to coding theory. J. Combinatorial Theory Ser. A **25**(3), 226–241 (1978)
7. Etzion, T., Vardy, A.: Error-correcting codes in projective space. IEEE Trans. Inform. Theory **57**(2), 1165–1173 (2011)
8. Faure, C., Loidreau, P.: A new public-key cryptosystem based on the problem of reconstructing p-polynomials. In: Coding and Crypt., pp. 304–315. Springer (2006)
9. Gabidulin, E.M.: Theory of codes with maximum rank distance. Probl. Inf. Transm. **21**(1), 3–16 (1985)
10. Gabidulin, E.M., Paramonov, A.V., Tretjakov, O.V.: Rank errors and rank erasures correction. In: 4th International Colloquium on Coding Theory (1991)
11. Gabidulin, E.M., Pilipchuk, N.I.: Error and erasure correcting algorithms for rank codes. Des. Codes Crypt. **49**(1-3), 105–122 (2008)
12. Gaborit, P., Ruatta, O., Schrek, J.: On the complexity of the rank syndrome decoding problem. IEEE Trans. Inform. Theory **62**(2), 1006–1019 (Feb 2016). https://doi.org/10.1109/TIT.2015.2511786
13. Gaborit, P., Zémor, G.: On the hardness of the decoding and the minimum distance problems for rank codes. IEEE Trans. Inform. Theory **62**(12), 7245–7252 (2015)
14. Guruswami, V., Sudan, M.: Improved decoding of Reed-Solomon and algebraic-geometry codes. IEEE Trans. Inform. Theory **45**(6), 1757–1767 (1999)
15. Guruswami, V., Vardy, A.: Maximum-likelihood decoding of reed-solomon codes is np-hard. IEEE Trans. Inform. Theory **51**, 2249–2256 (2005)

16. Horlemann-Trautmann, A.L., Kuijper, M.: A module minimization approach to Gabidulin decoding via interpolation. Journal of Algebra Comb. Discrete Structures and Applications **5**(1) (2017)
17. Jerkovits, T., Bartz, H.: "Weak keys in the Faure–Loidreau cryptosystem". In: Baldi, M., Persichetti, E., Santini, P. (eds.) Code-Based Cryptography. pp. 102–114. Springer International Publishing, Cham (2019)
18. Koetter, R., Kschischang, F.R.: Coding for errors and erasures in random network coding. IEEE Trans. Inform. Theory **54**(8), 3579–3591 (2008)
19. Raviv, N., Wachter-Zeh, A.: Some Gabidulin codes cannot be list decoded efficiently at any radius. IEEE Trans. Inform. Theory **62**(4), 1605–1615 (Apr 2016)
20. Richter, G., Plass, S.: Error and erasure decoding of rank-codes with a modified Berlekamp-Massey algorithm. In: International ITG Conference on Systems, Communications and Coding 2004 (SCC) (2004)
21. Roth, R.M.: Maximum-rank array codes and their application to crisscross error correction. IEEE Trans. Inform. Theory **37**(2), 328–336 (Mar 1991)
22. Rudra, A., Wootters, M.: Every list-decodable code for high noise has abundant near-optimal rate puncturings. In: Proc. Forty-sixth Annual ACM Symp. on Theory of Computing. pp. 764–773. New York, NY, USA (2014). https://doi.org/10.1145/2591796.2591797
23. Shangguan, C., Tamo, I.: Combinatorial list-decoding of Reed-Solomon codes beyond the Johnson radius. preprint (2019), `https://arxiv.org/abs/1911.01502`
24. Silva, D.: Error control for network coding. Ph.D. thesis (2009)
25. Silva, D., Kschischang, F.R., Koetter, R.: A rank-metric approach to error control in random network coding. IEEE Trans. Inform. Theory **54**(9), 3951–3967 (2008)
26. Stern, J.: Approximating the number of error locations within a constant ratio is NP-complete. In: 10th Int. Symp., AAECC-10, San Juan de Puerto Rico, Puerto Rico. pp. 325–331. No. 673 (1993)
27. Trombetti, R., Zullo, F.: On the list decodability of rank metric codes. preprint (2019), `https://arxiv.org/abs/1907.01289`
28. Vardy, A.: The intractability of computing the minimum distance of a code. IEEE Trans. Inform. Theory **43**(6), 1757–1766 (Nov 1997)
29. Wachter-Zeh, A.: Bounds on list Decoding of rank-metric codes. IEEE Trans. Inform. Theory **59**(11), 7268–7277 (Nov 2013)
30. Wachter-Zeh, A.: Decoding of block and convolutional codes in rank metric. Ph.D. thesis, Ulm University and Université Rennes 1 (2013)
31. Wachter-Zeh, A., Puchinger, S., Renner, J.: Repairing the Faure–Loidreau public-key cryptosystem. In: IEEE Trans. Inform. Theory (2018)

# A Guessing Jointly the Column and Row Space of the Error

We analyze the success probability of decoding to a specific codeword (i.e., the analog of Lemma 2) for guessing jointly the row and the column space of the error.

**Lemma 4.** *Let $\boldsymbol{r} \in \mathbb{F}_{q^m}^n$ be defined as in Section 2.2, where neither parts of the error row space nor column space are known, i.e., $\gamma = \rho = 0$ and $t = w$. The probability that an error-erasure decoder using a random*

– *$\delta_r$-dimensional guess of the error row space and a*
– *$\delta_c$-dimensional guess of the error column space,*

*where $\delta_r + \delta_c =: \delta \in [2\xi, n-k]$, outputs $\boldsymbol{mG}_{\mathrm{Gab}}$ is upper-bounded by*

$$\frac{\sum_{i=\lceil \xi + \frac{\delta}{2} \rceil}^{\min\{\delta, w\}} \sum_{\substack{0 \le w_r, w_c \le i \\ w_r + w_c = i}} \begin{bmatrix} n-w \\ \delta_r - w_r \end{bmatrix}_q \begin{bmatrix} w \\ w_r \end{bmatrix}_q q^{(w-w_r)(\delta_r - w_r)} \begin{bmatrix} m-w \\ \delta_c - w_c \end{bmatrix}_q \begin{bmatrix} w \\ w_c \end{bmatrix}_q q^{(w-w_c)(\delta_c - w_c)}}{\begin{bmatrix} n \\ \delta_r \end{bmatrix}_q \begin{bmatrix} m \\ \delta_c \end{bmatrix}_q}$$

*Proof.* The statement follows by the same arguments as Lemma 2, where we computed the probability that the row space of a random vector space of dimension $\delta$ instersects with the $w$-dimensional row space of the error in $i$ dimensions (where $i$ must be sufficiently large to apply the error erasure decoder successfully). Here, we want that a random guess of $\delta_r$- and $\delta_c$-dimensional vector spaces intersect with the row and column space of the error in exactly $w_r$ and $w_c$ dimensions, respectively. We sum up over all choices of $w_r$ and $w_c$ that sum up to an $i$ that is sufficiently large to successfully apply the error erasure decoder. This is an optimistic argument since guessing correctly $w_r$ dimensions of the row and $w_c$ dimensions of the column space of the error might not reduce the rank of the error by $w_r + w_c$. However, this gives an upper bound on the success probability.

Example 2 shows that guessing row and column space jointly is not advantageous for some specific parameters.

*Example 2.* Consider the example $q = 2$, $m = n = 24$, $k = 16$, $w = 6$. Guessing only the row space of the error with $\delta = 4$ succeeds with probability $1.66 \cdot 10^{-22}$ and joint guessing with $\delta_r = \delta_c = 2$ succeeds with probability $1.93 \cdot 10^{-22}$. Hence, it is advantageous to guess only the row space (or due to $m = n$ only the column space). For a larger example with $m = n = 64$, $k = 16$, and $w = 19$, the two probabilities are almost the same, $\approx 5.27 \cdot 10^{-82}$ (for $\delta = 32$ and $\delta_r = \delta_c = 16$).