ulm university universität ulm

On Transform–domain Decoding of Gabidulin Codes

Wenhui Li, Vladimir Sidorenko, Di Chen

Institute of Communications Engineering, Ulm University

WCC, Bergen, April 19, 2013

Abstract

- For a Gabidulin code, we propose a transform–domain algorithm correcting both errors and erasures.
- The transform–domain approach allows to simplify derivations, proofs, and decoding algorithms.
- We generalize this algorithm for interleaved Gabidulin codes.

Outline

Outline

Gabidulin codes

Gabidulin code $\mathcal{G}(q^m; n, k)$ is a linear (n, k) code of length n and dimension k over the field $\mathbb{F} = \mathbb{F}_{q^m}$, $n \le m$.

Codewords in vector form: $c = \begin{pmatrix} c_1 & \dots & c_n \end{pmatrix}, \quad c_i \in \mathbb{F}_{q^m}$

Codewords in matrix form: $C = \begin{pmatrix} c_{11} & \dots & c_{1n} \\ \vdots & \vdots & \vdots \\ c_{m1} & \dots & c_{mn} \end{pmatrix}, \quad c_{ij} \in \mathbb{F}_q$

Rank metric

For $a, b, c \in \mathbb{F}_{q^m}^n$

rank norm: $\operatorname{rank}_q c \triangleq \operatorname{rank} C$

rank distance: $d(a,b) \triangleq \operatorname{rank}_q(a-b)$

For Gabidulin code $\mathcal{G}(q^m; n, k)$

Code distance $d = n - k + 1$ achieves the Singleton type bound

Channel: $e = r - c, \quad \tau = \operatorname{rank}_q e$

If $d(r,c) = \tau < d/2$ then the error vector e will be corrected by a BMD decoder with complexity $\mathcal{O}(m^2)$ operations in $\mathbb{F}_{q^m}$

- "Standard" decoders: Gabidulin 1985, Roth 1991, Paramonov–Tretjakov 1991, Richter–Plass 2004
- Other decoders: Loidreau 2005, Wachter-Zeh et al. 2012

Rank metric

For $a, b, c \in \mathbb{F}_{q^m}^n$

rank norm: $\operatorname{rank}_q c \triangleq \operatorname{rank} C$

rank distance: $d(a, b) \triangleq \operatorname{rank}_q(a - b)$

For Gabidulin code $\mathcal{G}(q^m; n, k)$

Code distance $d = n - k + 1$ achieves the Singleton type bound

Channel: $e = r - c, \quad \tau = \operatorname{rank}_q e$

If $d(r, c) = \tau < d/2$ then the error vector e will be corrected by a BMD decoder with complexity $\mathcal{O}(m^2)$ operations in $\mathbb{F}_{q^m}$

- “Standard” decoders: Gabidulin 1985, Roth 1991, Paramonov–Tretjakov 1991, Richter–Plass 2004
- Other decoders: Loidreau 2005, Wachter-Zeh et al. 2012

Motivation

Lifting construction for Network coding (Kötter–Kschischang 2008)

Codeword of the subspace code:

$$V = (I_{m\times m}, C_{m\times n}) = \left(\begin{array}{ccc|ccc} 1 & & & c_{11} & \dots & c_{1n} \\ & \ddots & & \vdots & \vdots & \vdots \\ & & 1 & c_{m1} & \dots & c_{mn} \end{array}\right),$$

where $C \in \mathcal{G}(q^m; n, k)$, $m \geq n$.

To increase efficiency let us use *interleaving* of several Gabidulin codes

$$V = \left(I_{m\times m} | C^{(1)}, C^{(2)}, \dots, C^{(L)}\right), \quad C^{(i)} \in \mathcal{G}(q^m; n, k)$$

Motivation

Lifting construction for Network coding (Kötter–Kschischang 2008)

Codeword of the subspace code:

$$V = (I_{m\times m}, C_{m\times n}) = \left(\begin{array}{ccc|ccc} 1 & & & c_{11} & \dots & c_{1n} \\ & \ddots & & \vdots & \vdots & \vdots \\ & & 1 & c_{m1} & \dots & c_{mn} \end{array}\right),$$

where $C \in \mathcal{G}(q^m; n, k)$, $m \geq n$.

To increase efficiency let us use *interleaving* of several Gabidulin codes

$$V = \left(I_{m\times m} | C^{(1)}, C^{(2)}, \dots, C^{(L)}\right), \quad C^{(i)} \in \mathcal{G}(q^m; n, k)$$

Interleaved Gabidulin code $\mathcal{IG}$

In matrix form:

$$C = \left(C^{(1)}, C^{(2)}, \ldots, C^{(L)}\right), \quad C^{(i)} \in \mathcal{G}(q^m; n, k)$$

In vector form:

$$c = \left(c^{(1)}, c^{(2)}, \ldots, c^{(L)}\right), \quad c^{(i)} \in \mathcal{G}(q^m; n, k)$$

$\mathcal{IG}$ code is an (Ln, Lk) linear code over $\mathbb{F}_{q^m}$ with rank distance

$$d = n - k + 1$$

For $m = n$, $\mathcal{IG}$ is an MRD code.
Errors and erasures correction is necessary for network coding.

Known results

Loidreau and Overbeck (2006) considered another variant of interleaved Gabidulin code, where a codeword is

$$c = \begin{pmatrix} c^{(1)} \\ c^{(2)} \\ \vdots \\ c^{(L)} \end{pmatrix}, \quad c^{(i)} \in \mathcal{G}(q^m; n, k)$$

They suggested an algebraic decoder correcting errors only

- with complexity $\mathcal{O}(Lm^3) = \mathcal{O}(m^3)$ operations in $\mathbb{F}_{q^m}$
- which corrects error vectors e if $\operatorname{rank}_q e \leq \frac{L}{L+1}(d-1)$
- with probability of failure $P_f < 4q^{-m}$

Known results

In [SJB], a time domain algorithm for $\mathcal{IG}$ codes having complexity $\mathcal{O}(m^2)$ operations in $\mathbb{F}_{q^m}$ was suggested.

Standard approach:

1. solve the key equation to find "positions" of errors,
2. find error values.

To correct (errors only) by a single Gabidulin code Silva and Kschischang [SK] suggested an elegant solution for the second decoding step using a transform–domain approach.

[SJB] V. Sidorenko, L. Jiang, M. Bossert, "Skew-Feedback Shift-Register Synthesis and Decoding Interleaved Gabidulin Codes," *IEEE Trans. Inform. Theory*, vol. IT-57, pp. 621–632, Febr. 2011.

[SK] D. Silva and F. R. Kschischang, "Fast encoding and decoding of Gabidulin codes," in *Proc. IEEE Int. Symp. Inform. Theory*, Seoul, Korea, Jul. 2009, pp. 2858-2862

Our contribution

- For a single Gabidulin code we propose a transform–domain decoding algorithm. The algorithm is extended for $\mathcal{IG}$ codes. Time complexity of the algorithms is $\mathcal{O}(m^2)$ operations in the field $\mathbb{F}_{q^m}$.
- It corrects all error words of rank τ if

$$t \leq \tau_{\max} \triangleq \frac{L}{L+1}(d-1),$$

- where probability $P_f(\tau)$ of decoding failure is

$$P_f(\tau) \leq 3.5q^{-m\{(L+1)(\tau_{\max}-\tau)+1\}} < \frac{4}{q^m}.$$

Outline

Skew polynomials and linearized polynomials

Consider $\mathbb{F} = \mathbb{F}_{q^m}$, where q is power of a prime, with the Frobenius automorphism $\theta(a) = a^q$, $\theta^i(a) = \theta(\theta^{i-1}(a))$.
Define a ring structure on the set of skew polynomials $a(x)$

$$\mathbb{F}[x;\theta] = \{a(x) = a_n x^n + \cdots + a_1 x + a_0 \mid a_i \in \mathbb{F} \text{ and } n \in \mathbb{N}\}.$$

The addition in $\mathbb{F}[x;\theta]$ is usual. The multiplication is defined by the basic rule

$$xa = \theta(a)x$$

and extended to all elements of $\mathbb{F}[x;\theta]$ by associativity and distributivity.
Denote the corresponding linearized q-polynomial by $a_{(q)}(x)$, where

$$a_{(q)}(x) = \sum_{j=0}^{n} a_j \theta^j(x) = a_n x^{q^n} + \cdots + a_1 x^{q^1} + x.$$

θ-transform

Let us fix $n \leq m$ linearly independent over $\mathbb{F}_q$ elements $h_1, \ldots, h_n \in \mathbb{F}_{q^m}$ and define the following $n \times n$ transform matrix Φ over $\mathbb{F}_{q^m}$

$$\Phi = \begin{pmatrix} h_1 & h_2 & \ldots & h_n \\ \theta(h_1) & \theta(h_2) & \ldots & \theta(h_n) \\ \vdots & \vdots & \vdots & \vdots \\ \theta^{n-1}(h_1) & \theta^{n-1}(h_2) & \ldots & \theta^{n-1}(h_n) \end{pmatrix}.$$

The Moore matrix Φ is nonsingular and has the inverse matrix Φ^{-1}.

Gabidulin code

Definition

A Gabidulin code $\mathcal{G}$ is a linear (n, k) code of length n and dimension k over the field $\mathbb{F}_{q^m}$, $n \leq m$, with parity check matrix

$$H = \begin{pmatrix} h_1 & h_2 & \dots & h_n \\ \theta(h_1) & \theta(h_2) & \dots & \theta(h_n) \\ \vdots & \vdots & \vdots & \vdots \\ \theta^{n-k-1}(h_1) & \theta^{n-k-1}(h_2) & \dots & \theta^{n-k-1}(h_n) \end{pmatrix}$$

consisting of the first $n-k$ rows of the matrix Φ.

Outline

Errors and erasures

Channel with errors only: $r = c + e$, $\quad \operatorname{rank}_q e = \tau$, then

$$e = aB,$$

where $\quad a \in \mathbb{F}_{q^m}^{\tau}, B \in \mathbb{F}_q^{\tau \times n}, \operatorname{rank}_q a = \operatorname{rank}_q B = \tau.$

Channel with errors and erasures

$$e = e_{\mathsf{C}} + e_{\mathsf{F}} + e_{\mathsf{R}},$$

$$e = aB = a_{\mathsf{C}} B_{\mathsf{C}} + a_{\mathsf{F}} B_{\mathsf{F}} + a_{\mathsf{R}} B_{\mathsf{R}},$$

where blue symbols are known and

$$a_{\mathsf{C}} \in \mathbb{F}_{q^m}^{\varkappa}, B_{\mathsf{C}} \in \mathbb{F}_q^{\varkappa \times n}, \quad \operatorname{rank} a_{\mathsf{C}} = \operatorname{rank} B_{\mathsf{C}} = \varkappa,$$

$$a_{\mathsf{F}} \in \mathbb{F}_{q^m}^{\varepsilon}, B_{\mathsf{F}} \in \mathbb{F}_q^{\varepsilon \times n}, \quad \operatorname{rank} a_{\mathsf{F}} = \operatorname{rank} B_{\mathsf{F}} = \varepsilon,$$

$$a_{\mathsf{R}} \in \mathbb{F}_{q^m}^{\rho}, B_{\mathsf{R}} \in \mathbb{F}_q^{\rho \times n}, \quad \operatorname{rank} a_{\mathsf{R}} = \operatorname{rank} B_{\mathsf{R}} = \rho.$$

Errors and erasures polynomials

Define row erasure skew polynomial $\sigma_R(x)$
$\sigma_{R(q)}(a_{R,i}) = 0, i = 1, \ldots, \rho,$ then $\sigma_{R(q)}(x) = \text{minpoly}(a_R)$
Define full error skew polynomial $\sigma_F(x)$

$$\sigma_{F(q)}\left(\sigma_{R(q)}(a_{F,i})\right) = 0, i = 1, \ldots, \varepsilon.$$

Denote

$$\sigma_{FR}(x) = \sigma_F(x)\sigma_R(x)$$

Define

$$f = (f_1, \ldots, f_{\varkappa}) = B_C h^T,$$

and column erasure polynomial

$$\lambda_{C(q)}(x) = \text{minpoly}(f)$$

Given a skew polynomial $\lambda(x)$ of degree $\varkappa$, we define a reciprocal skew polynomial $\overline{\lambda}(x)$ having coefficients $\overline{\lambda}_i = \theta^{i-\varkappa}(\lambda_{\varkappa-i})$ for $i = 0, ..., \varkappa$.

Modified syndrome

The syndrome vector:

$$s = (s_1, \ldots, s_{d-1}) = rH^T = eH^T.$$

The syndrome polynomial:

$$s(x) = \sum_{i=1}^{n-k} s_i x^{i-1}.$$

The modified syndrome polynomial $s_{RC}(x)$, incorporates known information about row and column erasures:

$$s_{RC}(x) = \sigma_R(x) s(x) \overline{\lambda}_C(x).$$

Key equation for a single Gabidulin code

Theorem (Silva-Kschischang-Kötter)

The following equation holds

$$\sigma_F(x)s_{RC}(x) \equiv \omega(x) \mod x^{n-k}, \tag{1}$$

where $\deg \omega(x) < \tau$ *and the error evaluator polynomial* $\omega(x)$ *is defined by the first* τ *components of the modified syndrome* $s_{RC}(x)$.

Given the modified syndrome $s_{RC}(x)$, a solution $\sigma_F(x)$ of (1) can be found by a skew shift-register synthesis algorithm or by the Euclid's algorithm with complexity $\mathcal{O}(m^2)$.

Transformed error vector

The transformed error vector and polynomial

$$\tilde{e} = e\Phi^T$$

and the transformed error polynomial

$$\tilde{e}(x) = \sum_{i=1}^{n} \tilde{e}_i x^{i-1}.$$

Theorem (Error vector)

The transformed error polynomial $\tilde{e}(x)$ satisfies the following equation

$$\sigma_{FR}(x)\widetilde{e}_(x)\overline{\lambda}_C(x) \equiv \omega(x) \mod x^n, \qquad (2)$$

where the polynomial $\omega(x)$ is defined by (1).

Finding error vector

Known: $\sigma_R(x)$, $\overline{\lambda}_C(x)$, $s_{RC}(x)$, $\sigma_F(x)$

1. The error evaluator polynomial:

$$\omega(x) = \sigma_F(x) s_{RC}(x) \mod x^{n-k}$$

2. Compute $\sigma_{FR}(x) = \sigma_F(x)\sigma_R(x)$

   By Theorem(Error vector):

$$\sigma_{FR}(x)\widetilde{e}_(x)\overline{\lambda}_C(x) \equiv \omega(x) \mod x^n$$

3. Compute $s_C(x) = \sigma_{FR}(x) \backslash w(x)|_0^{n-1}$
4. The transformed error word: $\tilde{e}(x) = s_C(x)/\overline{\lambda}_C(x)|_0^{n-1}$
5. The error word: $e = \tilde{e}\left(\Phi^{-1}\right)^T$

Algorithm 1. Decoding of a single Gabidulin code

input: Received word $r \in \mathbb{F}_{q^m}^n$, vector a_R of row erasures , matrix B_C of column erasures

begin

- Row erasure polynomial: $\sigma_{R(q)}(x) = \text{minpoly}(a_R)$
- Column erasure polynomial: $f = B_C h^T$, $\lambda_{C(q)}(x) = \text{minpoly}(f)$
- Syndrome: $s = rH^T$
- Modified syndrome: $s_{RC}(x) = \sigma_R(x)s(x)\overline{\lambda}_C(x)$
- Find $\sigma_F(x)$ by solving the key equation (1) using the Berlekamp–Massey type algorithm in [SJB]; in case of non single solution output decoding failure
- The error evaluator polynomial $\omega(x) = \sigma_F(x)s_{RC}(x) \mod x^{n-k}$
- $\sigma_{FR}(x) = \sigma_F(x)\sigma_R(x)$
- The transformed error word $\tilde{e}(x) = \sigma_{FR}(x) \backslash w(x) / \overline{\lambda}_C(x)|_0^{n-1}$
- The error word $e = \tilde{e}\left(\Phi^{-1}\right)^T$

end

output: The codeword $c = r - e$ or decoding failure

Comparison with time-domain algorithms

In time-domain algorithms, instead of Lines 8–12 one should do the following more complicated steps:

- One polynomial multiplication to find $\sigma_{FR}(x)$,
- Solve a system of linear equations (41) in [SKK] to find $\beta = (\beta_1, \ldots, \beta_{\varkappa})$,
- Compute $\sigma_{C(q)}(x) =$minpoly(β),
- Compute $\sigma(x) = \sigma_C(x)\sigma_F(x)\sigma_R(x)$,
- Find a basis for the root space of $\sigma_{(q)}(x)$,
- Solve a system of linear equations (36) in [SKK] to find error locators,
- Compute error locations,
- Compute the error word.

Decoding of a single Gabidulin code

Theorem

Algorithm 1 corrects ε full errors, ρ row erasures and $\varkappa$ column erasures as long as

$$2\varepsilon + \rho + \varkappa \leq n - k = d - 1.$$

Time complexity of Algorithm 1 is $\mathcal{O}(m^2)$ operations in $\mathbb{F}_{q^m}$.

Outline

Assume a transmitted codeword

$$c = \begin{pmatrix} c^{(1)} & \dots & c^{(L)} \end{pmatrix} \in \mathbb{F}_{q^m}^{Ln}$$

and a received word word

$$r = \begin{pmatrix} r^{(1)} & \dots & r^{(L)} \end{pmatrix} \in \mathbb{F}_{q^m}^{Ln.}$$

The error word is

$$e = \begin{pmatrix} e^{(1)} & \dots & e^{(L)} \end{pmatrix} \in \mathbb{F}_{q^m}^{Ln},$$

where $e = r - c$. Denote $\operatorname{rank} e = \tau$, then the error word is

$$e = aB = a \begin{pmatrix} B^{(1)} & \dots & B^{(L)} \end{pmatrix}, \quad \text{where } a \in \mathbb{F}_{q^m}^{\tau},\ B \in \mathbb{F}_q^{\tau \times Ln},$$

where for every component code we have the following error vector

$$e^{(\ell)} = aB^{(\ell)} = a_{\mathsf{C}} B_{\mathsf{C}}^{(\ell)} + a_{\mathsf{F}} B_{\mathsf{F}}^{(\ell)} + a_{\mathsf{R}} B_{\mathsf{R}}^{(\ell)}.$$

Vector a is common for all interleaved codes. This allows to get more equations for the common error span polynomial $\sigma_F(x)$.

Theorem (Key equation for interleaved Gabidulin codes)

The following equation holds for $\ell = 1, \ldots, L$

$$\sigma_F(x) s_{RC}^{(\ell)}(x) \equiv \omega^{(\ell)}(x) \mod x^{n-k}, \tag{3}$$

where $\deg \omega^{(\ell)}(x) < \tau$ *and the error evaluator polynomial* $\omega^{(\ell)}(x)$ *is defined by the first* τ *components of the modified syndrome* $s_{RC}^{(\ell)}(x)$.

Theorem (Error vector)

The transformed error polynomials $\tilde{e}^{(\ell)}(x)$ *satisfies the following equations*

$$\sigma_{FR}(x) \widetilde{e}^{(\ell)}(x) \overline{\lambda}_C^{(\ell)}(x) \equiv \omega^{(\ell)}(x) \mod x^n,$$

where the polynomials $\omega^{(\ell)}(x)$ *are defined by (3).*

Algorithm 2. Decoding of interleaved codes

input: Received word $r = (r^{(1)}, \dots, r^{(L)}) \in \mathbb{F}_{q^m}^{Ln}$, a_R, $B_C^{(\ell)}$, $\ell = 1, \dots, L$ Row erasure polynomial: $\sigma_{R(q)}(x) =$ minpoly(a_R)

for $\ell = 1, \dots, L$ **do**

  Column erasure polynomials: $f^{(\ell)} = B_C^{(\ell)} h^T$, $\lambda_{C(q)}^{(\ell)}(x) =$ minpoly$(f^{(\ell)})$

  Syndromes: $s^{(\ell)} = r^{(\ell)} H^T$

  Modified syndromes: $s_{RC}^{(\ell)}(x) = \sigma_R(x) s^{(\ell)}(x) \overline{\lambda}_C^{(\ell)}(x)$

Find $\sigma_F(x)$ by solving the key equation (3) using the Berlekamp–Massey type algorithm in [SJB]; in case of non single solution output decoding failure

for $\ell = 1, \dots, L$ **do**

  The error evaluator polynomial: $\omega^{(\ell)}(x) = \sigma_F(x) s_{RC}^{(\ell)}(x) \mod x^{n-k}$

  $\sigma_{FR}(x) = \sigma_F(x) \sigma_R(x)$

  The transformed error word: $\tilde{e}^{(\ell)}(x) = \sigma_{FR}(x) \backslash w^{(\ell)}(x) / \overline{\lambda}_C^{(\ell)}(x)|_0^{n-1}$

  The error word: $e^{(\ell)} = \tilde{e}^{(\ell)} \left(\Phi^{-1}\right)^T$

$e = (e^{(1)}, \dots, e^{(L)})$

output: The codeword $c = r - e$ or decoding failure

Theorem

The fraction $P_f(\varepsilon)$ of full error vectors of $\operatorname{rank} e_F = \varepsilon$ *uncorrectable by Algorithm 2 in presence of ρ row erasures and $\varkappa_1, \ldots, \varkappa_L$ column erasures is upper bounded by*

$$P_f(\varepsilon) \leq 3.5q^{-m\{(L+1)(\varepsilon_{max}-\varepsilon)+1\}} < \frac{4}{q^m}$$

if

$$L \leq \varepsilon \leq \varepsilon_{max} \triangleq \frac{L}{L+1}(\overline{d}-1) \tag{4}$$

and

$$P_f(\varepsilon) = 0 \text{ for } \varepsilon < d_{min}/2, \tag{5}$$

$$\overline{d} = \frac{1}{L}\sum_{\ell=1}^{L} d-\rho-\varkappa^{(\ell)}, \quad d_{min} = \min_{\ell}\{d-\rho-\varkappa^{(\ell)}\}$$

are the average and minimum code distances respectively after erasings in interleaved (n, k) Gabidulin codes, $d = n-k+1$. Time complexity of the algorithm is $\mathcal{O}(Lm^2)$ operations in $\mathbb{F}_{q^m}$.

Discussion and future work

- Complexity: $\mathcal{O}(m^2)$ operations over $\mathbb{F}_{q^m}$ and $\mathcal{O}(Lm^2)$.
- Fast methods:
  - for multiplication of linearized polynomials were found in [SK] and [WAS].
  - Fast solution of the key equations – in [SB].
- We need:
  - a fast method for finding a minimal power linearized polynomial, given a basis of its roots, and
  - a fast method for division of skew polynomials.

[SK] D. Silva and F. R. Kschischang, "Fast encoding and decoding of Gabidulin codes," in *Proc. IEEE Int. Symp. Inform. Theory*, Seoul, Korea, Jul. 2009, pp. 2858-2862

[WAS] A. Wachter, V. Afanassiev, V. Sidorenko, "Fast Decoding of Gabidulin Codes," *Designs, Codes and Cryptography*, April, 2012.

[SB] V. Sidorenko, M. Bossert, "Fast skew-feedback shift-register synthesis", *Designs, Codes and Cryptography*, April, 2012, pp. 1-13.

Acknowledgement

The authors are thankful to

- Antonia Wachter-Zeh
- Erik Gabidulin,

for helpful discussions.

Thank you!

Acknowledgement

The authors are thankful to

- Antonia Wachter-Zeh
- Erik Gabidulin,

for helpful discussions.

Thank you!

Skew-feedback shift-registers

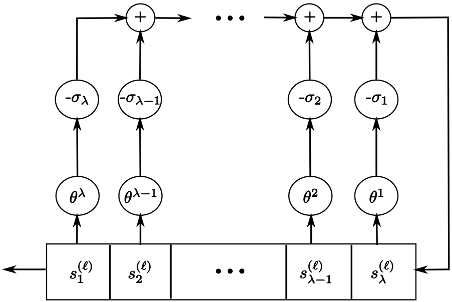

Figure: θ-skew-feedback shift-register (λ, σ)

- Given $\mathbb{F}$ and an automorphism θ. When $\theta = id$ (i.e., $\theta(a) = a$) we have a classical *linear*-feedback shift-register.
- For $\mathbb{F} = \mathbb{F}_{q^m}$ and the Frobenius automorphism $\theta(a) = a^q$ we have a *linearized*-feedback shift-register.

Linearized polynomials

- *Extention field:* $\mathbb{F}_{q^m}$,
- *Frobenius power:* For any integer i, $x^{[i]} \triangleq x^{q^i}$

Definition

A q-linearized polynomial (or q-polynomial) over $\mathbb{F}_Q$ is a polynomial of the form

$$f(x) = \sum_{i=0}^{t} f_i x^{[i]}, \quad f_i \in \mathbb{F}_Q,$$

Symbolic product

$$f(x) \otimes g(x) = f(g(x))$$

Algorithm 1. Decoding the Gabidulin code

input: Received word $r \in \mathbb{F}_{q^m}^n$

begin

Compute syndrome $s = rH^T$

Solve the key equation using the PTRP type algorithm, get $\sigma(x)$ and $t = \lambda$.

Find a basis $a_1, \ldots, a_t \in \mathbb{F}_{q^m}$ for the root space of $\sigma(x)$ get the vector $a = (a_1, \ldots, a_t)$.

Compute the matrix B using Gabidulin's algorithm.

Compute error word $e = aB$.

end

output: Codeword $c = r - e$.

Algorithm 1 corrects errors of rank up to $(d-1)/2$ with the total complexity $\mathcal{O}(n^2)$ operations in $\mathbb{F}_{q^m}$.