On Syndrome Decoding of Punctured Reed-Solomon and Gabidulin Codes

Hannes Bartz[1], Vladimir Sidorenko[1,2]

[1]Institute for Communications Engineering
Technical University of Munich (TUM)
Munich, Germany

[2]Institute for Information Transmission Problems
Russian Academy of Sciences
Moscow, Russia

15th Int. Workshop on Algebraic and Combinatorial Coding Theory (ACCT)

Albena, Bulgaria

June 19, 2016

Punctured Codes

Example: Linear $[N, k, d]$ code $\mathcal{C}$ of length N and dimension k

c_0	c_1	c_2	c_3	c_4	c_5	c_6	$\cdots$	c_{N-1}	c_N

Puncturing: remove $1 \leq r \leq d-1$ codeword symbols

$$\Downarrow$$

Punctured code $\widetilde{\mathcal{C}}$ of length $n = N - r$ and dimension k

$\tilde{c}_0$	$\tilde{c}_1$	$\tilde{c}_2$	$\tilde{c}_3$	$\tilde{c}_4$	$\cdots$	$\tilde{c}_{n-2}$	$\tilde{c}_{n-1}$

Motivation: Punctured *Reed-Solomon* and *Gabidulin* codes can be decoded up to the Singleton [1, 2, 3] Bound [4]

[1] R. C. Singleton, "Maximum distance q-nary codes", 1964
[2] D. Joshi, "A note on upper bounds for minimum distance codes", 1958
[3] Komamiya, Y., "Application of logical mathematics to information theory", 1953
[4] V. Sidorenko, G. Schmidt, and M. Bossert, "Decoding Punctured Reed-Solomon Codes up to the Singleton Bound", 2008

Punctured Codes

Example: Linear $[N, k, d]$ code $\mathcal{C}$ of length N and dimension k

Puncturing: remove $1 \leq r \leq d-1$ codeword symbols

$$\Downarrow$$

Punctured code $\widetilde{\mathcal{C}}$ of length $n = N - r$ and dimension k

Motivation: Punctured *Reed-Solomon* and *Gabidulin* codes can be decoded up to the Singleton [1, 2, 3] Bound [4]

[1] R. C. Singleton, "Maximum distance q-nary codes", 1964
[2] D. Joshi, "A note on upper bounds for minimum distance codes", 1958
[3] Komamiya, Y., "Application of logical mathematics to information theory", 1953
[4] V. Sidorenko, G. Schmidt, and M. Bossert, "Decoding Punctured Reed-Solomon Codes up to the Singleton Bound", 2008

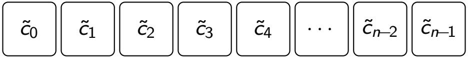
Punctured Codes

Example: Linear $[N, k, d]$ code $\mathcal{C}$ of length N and dimension k

Puncturing: remove $1 \leq r \leq d - 1$ codeword symbols

$$\Downarrow$$

Punctured code $\widetilde{\mathcal{C}}$ of length $n = N - r$ and dimension k



Motivation: Punctured *Reed-Solomon* and *Gabidulin* codes can be decoded up to the Singleton [1, 2, 3] Bound [4]

[1] R. C. Singleton, "Maximum distance q-nary codes", 1964

[2] D. Joshi, "A note on upper bounds for minimum distance codes", 1958

[3] Komamiya, Y., "Application of logical mathematics to information theory", 1953

[4] V. Sidorenko, G. Schmidt, and M. Bossert, "Decoding Punctured Reed-Solomon Codes up to the Singleton Bound", 2008

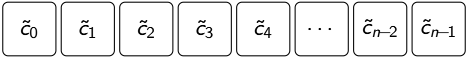
Punctured Codes

Example: Linear $[N, k, d]$ code $\mathcal{C}$ of length N and dimension k

Puncturing: remove $1 \leq r \leq d-1$ codeword symbols

$$\Downarrow$$

Punctured code $\widetilde{\mathcal{C}}$ of length $n = N - r$ and dimension k



Motivation: Punctured *Reed-Solomon* and *Gabidulin* codes can be decoded up to the Singleton [1, 2, 3] Bound [4]

[1] R. C. Singleton, "Maximum distance q-nary codes", 1964

[2] D. Joshi, "A note on upper bounds for minimum distance codes", 1958

[3] Komamiya, Y., "Application of logical mathematics to information theory", 1953

[4] V. Sidorenko, G. Schmidt, and M. Bossert, "Decoding Punctured Reed-Solomon Codes up to the Singleton Bound", 2008

Outline

Some Definitions

- $\mathbb{F}_q$: *finite field*, $\mathbb{F}_{q^m}$ *extension field* of degree m
- $\boldsymbol{\beta} = \{\beta_0, \beta_1, \ldots, \beta_{m-1}\}$: An ordered basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$
- Any element a from $\mathbb{F}_{q^m}$ can be represented w.r.t $\boldsymbol{\beta}$ by a *coordinate vector* $\underline{a} = \left(a^{(0)}, \ldots, a^{(m-1)}\right)^T$ over $\mathbb{F}_q$ s.th. $a = \sum_{i=0}^{m-1} a^{(i)}\beta_i$.
- Polynomial $p(x)$ of degree d

$$p(x) = \sum_{i=0}^{d} p_i x^i, p_d \neq 0.$$

- $\mathbb{F}_Q[x]$: ring of polynomials with coefficients from $\mathbb{F}_Q$
- $\mathbb{F}_Q[x]_{<k}$: set of all polynomials from $\mathbb{F}_Q[x]$ with *degree less than k*
- For any $b \in \mathbb{F}_q$ and integer i we have: $b^{q^i} = b$
- If $\boldsymbol{\beta}$ is a *normal* basis then $\underline{a^q} = \left(a^{(m-1)}, a^{(0)}, \ldots, a^{(m-2)}\right)^T$

Properly Punctured Reed-Solomon (RS) Codes

Definition (Properly Punctured RS Codes)

Let $\boldsymbol{\alpha} = (\alpha_0, \ldots, \alpha_{n-1})$ be a set of n distinct code locators from $\mathbb{F}_q$. A properly punctured Reed-Solomon $\mathcal{C}_{RS}$ code of length n and dimension k over $\mathbb{F}_{q^m}$ is defined as

$$\left\{ f(\boldsymbol{\alpha}) \stackrel{\text{def}}{=} (f(\alpha_0), f(\alpha_1), \ldots, f(\alpha_{n-1})) : f(x) \in \mathbb{F}_{q^m}[x]_{<k} \right\}. \quad (1)$$

RS code of length $N = q^m - 1$ with $\xi_i \in \mathbb{F}_{q^m}$ and $\alpha_i \in \mathbb{F}_q$

$f(\xi_0)$	$f(\xi_1)$	$f(\xi_2)$	$f(\xi_3)$	$f(\xi_4)$	$f(\xi_5)$	$f(\xi_6)$	$\cdots$	$f(\xi_{N-1})$

Properly Punctured RS code of length $n = q - 1$

$f(\alpha_0)$	$f(\alpha_1)$	$f(\alpha_2)$	$f(\alpha_3)$	$\cdots$	$f(\alpha_{n-1})$

Properly Punctured Reed-Solomon (RS) Codes

Definition (Properly Punctured RS Codes)

Let $\boldsymbol{\alpha} = (\alpha_0, \ldots, \alpha_{n-1})$ be a set of n distinct code locators from $\mathbb{F}_q$. A properly punctured Reed-Solomon $\mathcal{C}_{RS}$ code of length n and dimension k over $\mathbb{F}_{q^m}$ is defined as

$$\left\{ f(\boldsymbol{\alpha}) \stackrel{\text{def}}{=} (f(\alpha_0), f(\alpha_1), \ldots, f(\alpha_{n-1})) : f(x) \in \mathbb{F}_{q^m}[x]_{<k} \right\}. \tag{1}$$

RS code of length $N = q^m - 1$ with $\xi_i \in \mathbb{F}_{q^m}$ and $\alpha_i \in \mathbb{F}_q$

$f(\xi_0)$	$f(\xi_1)$	$f(\xi_2)$	$f(\xi_3)$	$f(\xi_4)$	$f(\xi_5)$	$f(\xi_6)$	$\cdots$	$f(\xi_{N-1})$

Properly Punctured RS code of length $n = q - 1$

$f(\alpha_0)$	$f(\alpha_1)$	$f(\alpha_2)$	$f(\alpha_3)$	$\cdots$	$f(\alpha_{n-1})$

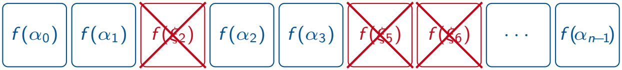
Properly Punctured Reed-Solomon (RS) Codes

Definition (Properly Punctured RS Codes)

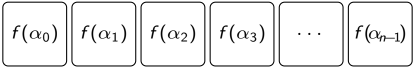
Let $\boldsymbol{\alpha} = (\alpha_0, \ldots, \alpha_{n-1})$ be a set of n distinct code locators from $\mathbb{F}_q$. A properly punctured Reed-Solomon $\mathcal{C}_{RS}$ code of length n and dimension k over $\mathbb{F}_{q^m}$ is defined as

$$\left\{ f(\boldsymbol{\alpha}) \stackrel{\text{def}}{=} (f(\alpha_0), f(\alpha_1), \ldots, f(\alpha_{n-1})) : f(x) \in \mathbb{F}_{q^m}[x]_{<k} \right\}. \tag{1}$$

RS code of length $N = q^m - 1$ with $\xi_i \in \mathbb{F}_{q^m}$ and $\alpha_i \in \mathbb{F}_q$



Properly Punctured RS code of length $n = q - 1$



Interleaved Reed-Solomon Codes (Scheme I)

By representing each coefficient f_i by $\underline{f_i}$ we can write *one* polynomial

$$f(x) = \sum_{i=0}^{k-1} f_i x^i \quad \in \mathbb{F}_{q^m}[x]_{<k}$$

as *m* polynomials $\forall j \in [0, m-1]$

$$f^{(j)}(x) = \sum_{i=0}^{k-1} f_i^{(j)} x^i \quad \in \mathbb{F}_q[x]_{<k}.$$

Thus each codeword $\mathbf{c} = f(\alpha)$ from $\mathcal{C}_{RS}$ can be written as interleaving of *m codewords* of an RS code *over* $\mathbb{F}_q$ [4]:

$$\mathbf{c} = f(\alpha) = \begin{pmatrix} f^{(0)}(\alpha) \\ f^{(1)}(\alpha) \\ \vdots \\ f^{(m-1)}(\alpha) \end{pmatrix} = \begin{pmatrix} f^{(0)}(\alpha_0) & \cdots & f^{(0)}(\alpha_{n-1}) \\ f^{(1)}(\alpha_0) & \cdots & f^{(1)}(\alpha_{n-1}) \\ \vdots & \vdots & \vdots \\ f^{(m-1)}(\alpha_0) & \cdots & f^{(m-1)}(\alpha_{n-1}) \end{pmatrix} = \mathbf{I}. \quad (2)$$

[4] V. Sidorenko, G. Schmidt, and M. Bossert, "Decoding Punctured Reed-Solomon Codes up to the Singleton Bound", 2008

Interleaved Reed-Solomon Codes (Scheme I)

By representing each coefficient f_i by $\underline{f_i}$ we can write *one* polynomial

$$f(x) = \sum_{i=0}^{k-1} f_i x^i \quad \in \mathbb{F}_{q^m}[x]_{<k}$$

as *m* polynomials $\forall j \in [0, m-1]$

$$f^{(j)}(x) = \sum_{i=0}^{k-1} f_i^{(j)} x^i \quad \in \mathbb{F}_q[x]_{<k}.$$

Thus each codeword $\mathbf{c} = f(\boldsymbol{\alpha})$ from $\mathcal{C}_{RS}$ can be written as interleaving of *m codewords* of an RS code *over* $\mathbb{F}_q$ [4]:

$$\mathbf{c} = f(\boldsymbol{\alpha}) = \begin{pmatrix} f^{(0)}(\boldsymbol{\alpha}) \\ f^{(1)}(\boldsymbol{\alpha}) \\ \vdots \\ f^{(m-1)}(\boldsymbol{\alpha}) \end{pmatrix} = \begin{pmatrix} f^{(0)}(\alpha_0) & \cdots & f^{(0)}(\alpha_{n-1}) \\ f^{(1)}(\alpha_0) & \cdots & f^{(1)}(\alpha_{n-1}) \\ \vdots & \vdots & \vdots \\ f^{(m-1)}(\alpha_0) & \cdots & f^{(m-1)}(\alpha_{n-1}) \end{pmatrix} = \mathbf{I}. \qquad (2)$$

[4] V. Sidorenko, G. Schmidt, and M. Bossert, "Decoding Punctured Reed-Solomon Codes up to the Singleton Bound", 2008

Virtual Interleaved Reed-Solomon Codes (Scheme V)

Consider a codeword $\mathbf{c} = (c_0 \, c_1 \dots \, c_{n-1})$ from $\mathcal{C}_{RS}$ and compute for $j = 0, \dots, m-1$ the *element-wise q-powers*

$$\mathbf{c}^{q^j} \stackrel{\text{def}}{=} (c_0^{q^j} \, c_1^{q^j} \, \dots \, c_{n-1}^{q^j}).$$

Since $c_i = f(\alpha_i)$ where $\alpha_i \in \mathbb{F}_q$ for all $i \in [0, n-1]$ and $f(x) \in \mathbb{F}_{q^m}[x]_{<k}$, we have

$$c_i^{q^j} = (f(\alpha_i))^{q^j} = f^{q^j}(\alpha_i) \qquad \Longrightarrow \qquad \mathbf{c}^{q^j} \in \mathcal{C}_{RS}.$$

From *one* codeword $\mathbf{c}$ we can virtually create $1 \leq s \leq m$ *codewords* over $\mathbb{F}_{q^m}$ [5, 6]:

$$\mathbf{V} = \begin{pmatrix} f(\boldsymbol{\alpha}) \\ f^{q^1}(\boldsymbol{\alpha}) \\ \vdots \\ f^{q^{s-1}}(\boldsymbol{\alpha}) \end{pmatrix} = \begin{pmatrix} f(\alpha_0) & \cdots & f(\alpha_{n-1}) \\ f^{q^1}(\alpha_0) & \cdots & f^{q^1}(\alpha_{n-1}) \\ \vdots & \vdots & \vdots \\ f^{q^{s-1}}(\alpha_0) & \cdots & f^{q^{s-1}}(\alpha_{n-1}) \end{pmatrix} \tag{3}$$

[5] V. Guruswami and C. Xing, "List Decoding RS, Algebraic-Geometric, and Gabidulin Subcodes up to the Singleton Bound", 2012
[6] L.-Z. Shen, F. wei Fu, and X. Guang, "Unique Decoding of Certain Reed-Solomon Codes", 2015

Virtual Interleaved Reed-Solomon Codes (Scheme V)

Consider a codeword $\mathbf{c} = (c_0\, c_1 \ldots c_{n-1})$ from $\mathcal{C}_{RS}$ and compute for $j = 0, \ldots, m-1$ the *element-wise q-powers*

$$\mathbf{c}^{q^j} \stackrel{\text{def}}{=} (c_0^{q^j}\, c_1^{q^j} \ldots c_{n-1}^{q^j}).$$

Since $c_i = f(\alpha_i)$ where $\alpha_i \in \mathbb{F}_q$ for all $i \in [0, n-1]$ and $f(x) \in \mathbb{F}_{q^m}[x]_{<k}$, we have

$$c_i^{q^j} = (f(\alpha_i))^{q^j} = f^{q^j}(\alpha_i) \qquad \Longrightarrow \qquad \mathbf{c}^{q^j} \in \mathcal{C}_{RS}.$$

From *one* codeword $\mathbf{c}$ we can virtually create $1 \leq s \leq m$ *codewords* over $\mathbb{F}_{q^m}$ [5, 6]:

$$\mathbf{V} = \begin{pmatrix} f(\boldsymbol{\alpha}) \\ f^{q^1}(\boldsymbol{\alpha}) \\ \vdots \\ f^{q^{s-1}}(\boldsymbol{\alpha}) \end{pmatrix} = \begin{pmatrix} f(\alpha_0) & \cdots & f(\alpha_{n-1}) \\ f^{q^1}(\alpha_0) & \cdots & f^{q^1}(\alpha_{n-1}) \\ \vdots & \vdots & \vdots \\ f^{q^{s-1}}(\alpha_0) & \cdots & f^{q^{s-1}}(\alpha_{n-1}) \end{pmatrix} \tag{3}$$

[5] V. Guruswami and C. Xing, "List Decoding RS, Algebraic-Geometric, and Gabidulin Subcodes up to the Singleton Bound", 2012

[6] L.-Z. Shen, F. wei Fu, and X. Guang, "Unique Decoding of Certain Reed-Solomon Codes", 2015

Virtual Interleaved Reed-Solomon Codes (Scheme V)

Consider a codeword $\mathbf{c} = (c_0\, c_1 \ldots c_{n-1})$ from $\mathcal{C}_{RS}$ and compute for $j = 0, \ldots, m-1$ the *element-wise q-powers*

$$\mathbf{c}^{q^j} \overset{\text{def}}{=} (c_0^{q^j}\, c_1^{q^j} \ldots c_{n-1}^{q^j}).$$

Since $c_i = f(\alpha_i)$ where $\alpha_i \in \mathbb{F}_q$ for all $i \in [0, n-1]$ and $f(x) \in \mathbb{F}_{q^m}[x]_{<k}$, we have

$$c_i^{q^j} = (f(\alpha_i))^{q^j} = f^{q^j}(\alpha_i) \qquad \Longrightarrow \qquad \mathbf{c}^{q^j} \in \mathcal{C}_{RS}.$$

From *one* codeword $\mathbf{c}$ we can virtually create $1 \leq s \leq m$ *codewords* over $\mathbb{F}_{q^m}$ [5, 6]:

$$\mathbf{V} = \begin{pmatrix} f^{q^0}(\boldsymbol{\alpha}) \\ f^{q^1}(\boldsymbol{\alpha}) \\ \vdots \\ f^{q^{s-1}}(\boldsymbol{\alpha}) \end{pmatrix} = \begin{pmatrix} f^{q^0}(\alpha_0) & \cdots & f^{q^0}(\alpha_{n-1}) \\ f^{q^1}(\alpha_0) & \cdots & f^{q^1}(\alpha_{n-1}) \\ \vdots & \vdots & \vdots \\ f^{q^{s-1}}(\alpha_0) & \cdots & f^{q^{s-1}}(\alpha_{n-1}) \end{pmatrix} \tag{3}$$

[5] V. Guruswami and C. Xing, "List Decoding RS, Algebraic-Geometric, and Gabidulin Subcodes up to the Singleton Bound", 2012
[6] L.-Z. Shen, F. wei Fu, and X. Guang, "Unique Decoding of Certain Reed-Solomon Codes", 2015

Virtual Interleaved Reed-Solomon Codes (Scheme V)

Consider a codeword $\mathbf{c} = (c_0\, c_1 \ldots c_{n-1})$ from $\mathcal{C}_{RS}$ and compute for $j = 0, \ldots, m-1$ the *element-wise q-powers*

$$\mathbf{c}^{q^j} \stackrel{\text{def}}{=} (c_0^{q^j}\, c_1^{q^j} \ldots c_{n-1}^{q^j}).$$

Since $c_i = f(\alpha_i)$ where $\alpha_i \in \mathbb{F}_q$ for all $i \in [0, n-1]$ and $f(x) \in \mathbb{F}_{q^m}[x]_{<k}$, we have

$$c_i^{q^j} = (f(\alpha_i))^{q^j} = f^{q^j}(\alpha_i) \qquad \Longrightarrow \qquad \mathbf{c}^{q^j} \in \mathcal{C}_{RS}.$$

From *one* codeword $\mathbf{c}$ we can virtually create $1 \leq s \leq m$ *codewords* over $\mathbb{F}_{q^m}$ [5, 6]:

$$\mathbf{V} = \begin{pmatrix} f^{q^0}(\boldsymbol{\alpha}) \\ f^{q^1}(\boldsymbol{\alpha}) \\ \vdots \\ f^{q^{s-1}}(\boldsymbol{\alpha}) \end{pmatrix} = \begin{pmatrix} f^{q^0}(\alpha_0) & \cdots & f^{q^0}(\alpha_{n-1}) \\ f^{q^1}(\alpha_0) & \cdots & f^{q^1}(\alpha_{n-1}) \\ \vdots & \vdots & \vdots \\ f^{q^{s-1}}(\alpha_0) & \cdots & f^{q^{s-1}}(\alpha_{n-1}) \end{pmatrix} \tag{3}$$

[5] V. Guruswami and C. Xing, "List Decoding RS, Algebraic-Geometric, and Gabidulin Subcodes up to the Singleton Bound", 2012
[6] L.-Z. Shen, F. wei Fu, and X. Guang, "Unique Decoding of Certain Reed-Solomon Codes", 2015

Scheme I vs. Scheme V

	Scheme I [7, 8]	Scheme V [5, 6]
Decoding radius	$t \leq \frac{m}{m+1}(n-k)$	$t \leq \frac{m}{m+1}(n-k)$
Failure probability	$\lvert\mathbb{F}_q\rvert^{-1}$	$\lvert\mathbb{F}_{q^m}\rvert^{-1}$? [6]
Comp. complexity	$\varkappa$ in $\mathbb{F}_q$	$\varkappa$ in $\mathbb{F}_{q^m}$

Standard [7]: $\varkappa = \mathcal{O}(mn^2)$, fast [9,10]: $\varkappa = \mathcal{O}(m^3 n \log(n))$

Question

What can we gain by using Scheme V instead of Scheme I?

[5] V. Guruswami and C. Xing, "List Decoding RS, Algebraic-Geometric, and Gabidulin Subcodes up to the Singleton Bound", 2012
[6] L.-Z. Shen, F. wei Fu, and X. Guang, "Unique Decoding of Certain Reed-Solomon Codes", 2015
[7] G. Schmidt, V. Sidorenko, M. Bossert, "Collaborative Decoding of Interleaved RS Codes and Concatenated Code Designs", 2009
[8] D. Bleichenbacher, A. Kiayias, and M. Yung, "Decoding Interleaved Reed–Solomon Codes over Noisy Channels", 2007
[9] V. Sidorenko, M. Bossert "Fast skew-feedback shift-register synthesis.", 2007
[10] S. Puchinger, S. Muelich, D. Moedinger, J. Nielsen, M. Bossert, "Decoding Interleaved Gabidulin Codes using Alekhnovich's Algorithm", ACCT 2016 $\Longrightarrow$ Wednesday 14:00h

Scheme I vs. Scheme V

	Scheme I [7, 8]	Scheme V [5, 6]
Decoding radius	$t \leq \frac{m}{m+1}(n-k)$	$t \leq \frac{m}{m+1}(n-k)$
Failure probability	$\lvert\mathbb{F}_q\rvert^{-1}$	$\lvert\mathbb{F}_{q^m}\rvert^{-1}$? [6]
Comp. complexity	$\varkappa$ in $\mathbb{F}_q$	$\varkappa$ in $\mathbb{F}_{q^m}$

Standard [7]: $\varkappa = \mathcal{O}(mn^2)$, fast [9,10]: $\varkappa = \mathcal{O}(m^3 n \log(n))$

Question

What can we gain by using Scheme V instead of Scheme I?

[5] V. Guruswami and C. Xing, "List Decoding RS, Algebraic-Geometric, and Gabidulin Subcodes up to the Singleton Bound", 2012
[6] L.-Z. Shen, F. wei Fu, and X. Guang, "Unique Decoding of Certain Reed-Solomon Codes", 2015
[7] G. Schmidt, V. Sidorenko, M. Bossert, "Collaborative Decoding of Interleaved RS Codes and Concatenated Code Designs", 2009
[8] D. Bleichenbacher, A. Kiayias, and M. Yung, "Decoding Interleaved Reed–Solomon Codes over Noisy Channels", 2007
[9] V. Sidorenko, M. Bossert "Fast skew-feedback shift-register synthesis.", 2007
[10] S. Puchinger, S. Muelich, D. Moedinger, J. Nielsen, M. Bossert, "Decoding Interleaved Gabidulin Codes using Alekhnovich's Algorithm", ACCT 2016 $\Longrightarrow$ Wednesday 14:00h

Syndrome Decoding of RS Codes

Let $\mathbf{H} \in \mathbb{F}_q^{n-k \times n}$ be a parity check matrix of $\mathcal{C}_{RS}$. Suppose we receive

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

with error vector $\mathbf{e}$ of Hamming weight t.

- Compute the *syndrome* $\mathbf{s} = \mathbf{y}\mathbf{H}^T$
- Solve the *key equation* for the error-locator polynomial $\sigma(x)$

$$s_i = -\sum_{j=1}^{t} \sigma_j s_{i-j}, \qquad i = [t, d-2], \ell = [0, m-1]. \tag{4}$$

$\Longrightarrow$ Find the *smallest t* such that (4) has a solution

- Using $\sigma(x)$ compute the error vector $\mathbf{e}$ and return codeword $\hat{\mathbf{c}} = \mathbf{y} - \mathbf{e}$

(4) is a *linear system* $\mathbf{A}\mathbf{x} = \mathbf{b}$ with $\mathbf{A}, \mathbf{b}$ over $\mathbb{F}_{q^m}$ and $\mathbf{x}$ over $\mathbb{F}_q$
Equivalently we can solve $\underline{\mathbf{A}}\mathbf{x} = \underline{\mathbf{b}}$ over the *subfield* $\mathbb{F}_q$

Syndrome Decoding of RS Codes

Let $\mathbf{H} \in \mathbb{F}_q^{n-k \times n}$ be a parity check matrix of $\mathcal{C}_{RS}$. Suppose we receive

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

with error vector $\mathbf{e}$ of Hamming weight t.

- Compute the *syndrome* $\mathbf{s} = \mathbf{y}\mathbf{H}^T$
- Solve the *key equation* for the error-locator polynomial $\sigma(x)$

$$s_i = -\sum_{j=1}^{t} \sigma_j s_{i-j}, \qquad i = [t, d-2], \ell = [0, m-1]. \tag{4}$$

$\implies$ Find the *smallest t* such that (4) has a solution

- Using $\sigma(x)$ compute the error vector $\mathbf{e}$ and return codeword $\hat{\mathbf{c}} = \mathbf{y} - \mathbf{e}$

(4) is a *linear system* $\mathbf{A}\mathbf{x} = \mathbf{b}$ with $\mathbf{A}, \mathbf{b}$ over $\mathbb{F}_{q^m}$ and $\mathbf{x}$ over $\mathbb{F}_q$
Equivalently we can solve $\underline{\mathbf{A}}\mathbf{x} = \underline{\mathbf{b}}$ over the *subfield* $\mathbb{F}_q$

Syndrome Decoding of RS Codes

Let $\mathbf{H} \in \mathbb{F}_q^{n-k \times n}$ be a parity check matrix of $\mathcal{C}_{RS}$. Suppose we receive

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

with error vector $\mathbf{e}$ of Hamming weight t.

- Compute the *syndrome* $\mathbf{s} = \mathbf{y}\mathbf{H}^T$
- Solve the *key equation* for the error-locator polynomial $\sigma(x)$

$$s_i = -\sum_{j=1}^{t} \sigma_j s_{i-j}, \qquad i = [t, d-2], \ell = [0, m-1]. \tag{4}$$

$\Longrightarrow$ Find the *smallest t* such that (4) has a solution

- Using $\sigma(x)$ compute the error vector $\mathbf{e}$ and return codeword $\hat{\mathbf{c}} = \mathbf{y} - \mathbf{e}$

(4) is a *linear system* $\mathbf{A}\mathbf{x} = \mathbf{b}$ with $\mathbf{A}, \mathbf{b}$ over $\mathbb{F}_{q^m}$ and $\mathbf{x}$ over $\mathbb{F}_q$
Equivalently we can solve $\underline{\mathbf{A}}\mathbf{x} = \underline{\mathbf{b}}$ over the *subfield* $\mathbb{F}_q$

Syndrome Decoding of RS Codes

Let $\mathbf{H} \in \mathbb{F}_q^{n-k \times n}$ be a parity check matrix of $\mathcal{C}_{RS}$. Suppose we receive

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

with error vector $\mathbf{e}$ of Hamming weight t.

- Compute the *syndrome* $\mathbf{s} = \mathbf{y}\mathbf{H}^T$
- Solve the *key equation* for the error-locator polynomial $\sigma(x)$

$$s_i = -\sum_{j=1}^{t} \sigma_j s_{i-j}, \qquad i = [t, d-2], \ell = [0, m-1]. \tag{4}$$

$\Longrightarrow$ Find the *smallest t* such that (4) has a solution

- Using $\sigma(x)$ compute the error vector $\mathbf{e}$ and return codeword $\hat{\mathbf{c}} = \mathbf{y} - \mathbf{e}$

(4) is a *linear system* $\mathbf{A}\mathbf{x} = \mathbf{b}$ with $\mathbf{A}, \mathbf{b}$ over $\mathbb{F}_{q^m}$ and $\mathbf{x}$ over $\mathbb{F}_q$
Equivalently we can solve $\underline{\mathbf{A}}\mathbf{x} = \underline{\mathbf{b}}$ over the *subfield* $\mathbb{F}_q$

Syndrome Decoding of RS Codes

Let $\mathbf{H} \in \mathbb{F}_q^{n-k \times n}$ be a parity check matrix of $\mathcal{C}_{RS}$. Suppose we receive

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

with error vector $\mathbf{e}$ of Hamming weight t.

- Compute the *syndrome* $\mathbf{s} = \mathbf{y}\mathbf{H}^T$
- Solve the *key equation* for the error-locator polynomial $\sigma(x)$

$$s_i = -\sum_{j=1}^{t} \sigma_j s_{i-j}, \qquad i = [t, d-2], \ell = [0, m-1]. \tag{4}$$

$\implies$ Find the *smallest t* such that (4) has a solution

- Using $\sigma(x)$ compute the error vector $\mathbf{e}$ and return codeword $\hat{\mathbf{c}} = \mathbf{y} - \mathbf{e}$

(4) is a *linear system* $\mathbf{A}\mathbf{x} = \mathbf{b}$ with $\mathbf{A}, \mathbf{b}$ over $\mathbb{F}_{q^m}$ and $\mathbf{x}$ over $\mathbb{F}_q$
Equivalently we can solve $\underline{\mathbf{A}}\mathbf{x} = \underline{\mathbf{b}}$ over the *subfield* $\mathbb{F}_q$

Solving the Key Equation - Scheme I [7]

- Compute *one syndrome* $\mathbf{s} = \mathbf{y}\mathbf{H}^T \in \mathbb{F}_{q^m}^{d-1}$ i.e., $\underline{\mathbf{s}} = \underline{\mathbf{y}}\mathbf{H}^T$
- We get *m syndromes* $\mathbf{s}^{(\ell)} = \mathbf{y}^{(\ell)}\mathbf{H}^T$ for all $\ell = 0, \dots, m-1$
- Solve the *m key equations* over $\mathbb{F}_q$ for *the same* error-locator polynomial $\sigma(x) \in \mathbb{F}_q[x]$

$$s_i^{(\ell)} = -\sum_{j=1}^{t} \sigma_j s_{i-j}^{(\ell)}, i = [t, d-2], \ell = [0, m-1]. \qquad (5)$$

- Output: Unique $\sigma(x)$ or "decoding failure"

(5) is a *linear* system $\underline{\mathbf{A}}\mathbf{x} = \underline{\mathbf{b}}$ over the *subfield* $\mathbb{F}_q$ or equivalently $\mathbf{A}\mathbf{x} = \mathbf{b}$ with $\mathbf{A}, \mathbf{b}$ over $\mathbb{F}_{q^m}$ and $\mathbf{x}$ over $\mathbb{F}_q$

[7] G. Schmidt, V. Sidorenko, M. Bossert, "Collaborative Decoding of Interleaved RS Codes and Concatenated Code Designs", 2009

Solving the Key Equation - Scheme I [7]

- Compute *one syndrome* $\mathbf{s} = \mathbf{y}\mathbf{H}^T \in \mathbb{F}_{q^m}^{d-1}$ i.e., $\underline{\mathbf{s}} = \underline{\mathbf{y}}\mathbf{H}^T$
- We get *m syndromes* $\mathbf{s}^{(\ell)} = \mathbf{y}^{(\ell)}\mathbf{H}^T$ for all $\ell = 0, \ldots, m-1$
- Solve the *m key equations* over $\mathbb{F}_q$ for *the same* error-locator polynomial $\sigma(x) \in \mathbb{F}_q[x]$

$$s_i^{(\ell)} = -\sum_{j=1}^{t} \sigma_j s_{i-j}^{(\ell)}, i = [t, d-2], \ell = [0, m-1]. \qquad (5)$$

- Output: Unique $\sigma(x)$ or "decoding failure"

(5) is a *linear* system $\underline{\mathbf{A}}\mathbf{x} = \underline{\mathbf{b}}$ over the *subfield* $\mathbb{F}_q$ or equivalently $\mathbf{A}\mathbf{x} = \mathbf{b}$ with $\mathbf{A}, \mathbf{b}$ over $\mathbb{F}_{q^m}$ and $\mathbf{x}$ over $\mathbb{F}_q$

[7] G. Schmidt, V. Sidorenko, M. Bossert, "Collaborative Decoding of Interleaved RS Codes and Concatenated Code Designs", 2009

Solving the Key Equation - Scheme I [7]

- Compute *one syndrome* $\mathbf{s} = \mathbf{y}\mathbf{H}^T \in \mathbb{F}_{q^m}^{d-1}$ i.e., $\underline{\mathbf{s}} = \underline{\mathbf{y}}\mathbf{H}^T$
- We get *m syndromes* $\mathbf{s}^{(\ell)} = \mathbf{y}^{(\ell)}\mathbf{H}^T$ for all $\ell = 0, \ldots, m-1$
- Solve the *m key equations* over $\mathbb{F}_q$ for *the same* error-locator polynomial $\sigma(x) \in \mathbb{F}_q[x]$

$$s_i^{(\ell)} = -\sum_{j=1}^{t} \sigma_j s_{i-j}^{(\ell)}, i = [t, d-2], \ell = [0, m-1]. \quad (5)$$

- Output: Unique $\sigma(x)$ or "decoding failure"

(5) is a *linear* system $\underline{\mathbf{A}}\mathbf{x} = \underline{\mathbf{b}}$ over the *subfield* $\mathbb{F}_q$ or equivalently $\mathbf{A}\mathbf{x} = \mathbf{b}$ with $\mathbf{A}, \mathbf{b}$ over $\mathbb{F}_{q^m}$ and $\mathbf{x}$ over $\mathbb{F}_q$

[7] G. Schmidt, V. Sidorenko, M. Bossert, "Collaborative Decoding of Interleaved RS Codes and Concatenated Code Designs", 2009

Solving the Key Equation - Scheme I [7]

- Compute *one syndrome* $\mathbf{s} = \mathbf{y}\mathbf{H}^T \in \mathbb{F}_{q^m}^{d-1}$ i.e., $\underline{\mathbf{s}} = \underline{\mathbf{y}}\mathbf{H}^T$
- We get *m syndromes* $\mathbf{s}^{(\ell)} = \mathbf{y}^{(\ell)}\mathbf{H}^T$ for all $\ell = 0, \dots, m-1$
- Solve the *m key equations* over $\mathbb{F}_q$ for *the same* error-locator polynomial $\sigma(x) \in \mathbb{F}_q[x]$

$$s_i^{(\ell)} = -\sum_{j=1}^{t} \sigma_j s_{i-j}^{(\ell)}, i = [t, d-2], \ell = [0, m-1]. \quad (5)$$

- Output: Unique $\sigma(x)$ or "decoding failure"

(5) is a *linear* system $\underline{\mathbf{A}}\mathbf{x} = \underline{\mathbf{b}}$ over the *subfield* $\mathbb{F}_q$ or equivalently $\mathbf{A}\mathbf{x} = \mathbf{b}$ with $\mathbf{A}, \mathbf{b}$ over $\mathbb{F}_{q^m}$ and $\mathbf{x}$ over $\mathbb{F}_q$

[7] G. Schmidt, V. Sidorenko, M. Bossert, "Collaborative Decoding of Interleaved RS Codes and Concatenated Code Designs", 2009

Solving the Key Equation - Scheme I [7]

- Compute *one syndrome* $\mathbf{s} = \mathbf{y}\mathbf{H}^T \in \mathbb{F}_{q^m}^{d-1}$ i.e., $\underline{\mathbf{s}} = \underline{\mathbf{y}}\mathbf{H}^T$
- We get *m syndromes* $\mathbf{s}^{(\ell)} = \mathbf{y}^{(\ell)}\mathbf{H}^T$ for all $\ell = 0, \ldots, m-1$
- Solve the *m key equations* over $\mathbb{F}_q$ for *the same* error-locator polynomial $\sigma(x) \in \mathbb{F}_q[x]$

$$s_i^{(\ell)} = -\sum_{j=1}^{t} \sigma_j s_{i-j}^{(\ell)}, i = [t, d-2], \ell = [0, m-1]. \qquad (5)$$

- Output: Unique $\sigma(x)$ or "decoding failure"

(5) is a *linear* system $\underline{\mathbf{A}}\mathbf{x} = \underline{\mathbf{b}}$ over the *subfield* $\mathbb{F}_q$ or equivalently $\mathbf{A}\mathbf{x} = \mathbf{b}$ with $\mathbf{A}, \mathbf{b}$ over $\mathbb{F}_{q^m}$ and $\mathbf{x}$ over $\mathbb{F}_q$

[7] G. Schmidt, V. Sidorenko, M. Bossert, "Collaborative Decoding of Interleaved RS Codes and Concatenated Code Designs", 2009

Solving the Key Equation - Scheme V [6]

- Compute *one syndrome* $\mathbf{s} = \mathbf{y}\mathbf{H}^T \in \mathbb{F}_{q^m}^{d-1}$
- Compute *virtual syndromes* $\mathbf{s}^{q^\ell} = \mathbf{y}^{q^\ell}\mathbf{H}^T$ for all $\ell = 0, \dots, m-1$
- Solve the *m key equations* over $\mathbb{F}_{q^m}$ for *the same* error-locator polynomial $\sigma(x) \in \mathbb{F}_q[x]$

$$s_i^{q^\ell} = -\sum_{j=1}^{t} \sigma_j s_{i-j}^{q^\ell}, i = [t, d-2], \ell = [0, m-1]. \quad (6)$$

- Corresponds to solving an *inhomogeneous linear system*

$$\begin{pmatrix} \mathbf{A}^{q^0} \\ \vdots \\ \mathbf{A}^{q^{m-1}} \end{pmatrix} \cdot \mathbf{x} = \begin{pmatrix} \mathbf{b}^{q^0} \\ \vdots \\ \mathbf{b}^{q^{m-1}} \end{pmatrix}$$

- The *first equation* is the same as for Scheme I
- We get *$m-1$ additional* equations in $\mathbb{F}_{q^m}$
  $\Longrightarrow$ Are the additional equations linearly independent?

[6] L.-Z. Shen, F. wei Fu, and X. Guang, "Unique Decoding of Certain Reed-Solomon Codes", 2015

Solving the Key Equation - Scheme V [6]

- Compute *one syndrome* $\mathbf{s} = \mathbf{y}\mathbf{H}^T \in \mathbb{F}_{q^m}^{d-1}$
- Compute *virtual syndromes* $\mathbf{s}^{q^\ell} = \mathbf{y}^{q^\ell}\mathbf{H}^T$ for all $\ell = 0, \ldots, m-1$
- Solve the *m key equations* over $\mathbb{F}_{q^m}$ for *the same* error-locator polynomial $\sigma(x) \in \mathbb{F}_q[x]$

$$s_i^{q^\ell} = -\sum_{j=1}^{t} \sigma_j s_{i-j}^{q^\ell}, i = [t, d-2], \ell = [0, m-1]. \tag{6}$$

- Corresponds to solving an *inhomogeneous linear system*

$$\begin{pmatrix} \mathbf{A}^{q^0} \\ \vdots \\ \mathbf{A}^{q^{m-1}} \end{pmatrix} \cdot \mathbf{x} = \begin{pmatrix} \mathbf{b}^{q^0} \\ \vdots \\ \mathbf{b}^{q^{m-1}} \end{pmatrix}$$

- The *first equation* is the same as for Scheme I
- We get *m − 1 additional* equations in $\mathbb{F}_{q^m}$
  $\Longrightarrow$ Are the additional equations linearly independent?

[6] L.-Z. Shen, F. wei Fu, and X. Guang, "Unique Decoding of Certain Reed-Solomon Codes", 2015

Solving the Key Equation - Scheme V [6]

- Compute *one syndrome* $\mathbf{s} = \mathbf{y}\mathbf{H}^T \in \mathbb{F}_{q^m}^{d-1}$
- Compute *virtual syndromes* $\mathbf{s}^{q^\ell} = \mathbf{y}^{q^\ell}\mathbf{H}^T$ for all $\ell = 0, \ldots, m-1$
- Solve the *m key equations* over $\mathbb{F}_{q^m}$ for *the same* error-locator polynomial $\sigma(x) \in \mathbb{F}_q[x]$

$$s_i^{q^\ell} = -\sum_{j=1}^{t} \sigma_j s_{i-j}^{q^\ell}, i = [t, d-2], \ell = [0, m-1]. \quad (6)$$

- Corresponds to solving an *inhomogeneous linear system*

$$\begin{pmatrix} \mathbf{A}^{q^0} \\ \vdots \\ \mathbf{A}^{q^{m-1}} \end{pmatrix} \cdot \mathbf{x} = \begin{pmatrix} \mathbf{b}^{q^0} \\ \vdots \\ \mathbf{b}^{q^{m-1}} \end{pmatrix}$$

- The *first equation* is the same as for Scheme I
- We get *$m-1$ additional* equations in $\mathbb{F}_{q^m}$
  $\Longrightarrow$ Are the additional equations linearly independent?

[6] L.-Z. Shen, F. wei Fu, and X. Guang, "Unique Decoding of Certain Reed-Solomon Codes", 2015

Solving the Key Equation - Scheme V [6]

- Compute *one syndrome* $\mathbf{s} = \mathbf{y}\mathbf{H}^T \in \mathbb{F}_{q^m}^{d-1}$
- Compute *virtual syndromes* $\mathbf{s}^{q^\ell} = \mathbf{y}^{q^\ell}\mathbf{H}^T$ for all $\ell = 0, \dots, m-1$
- Solve the *m key equations* over $\mathbb{F}_{q^m}$ for *the same* error-locator polynomial $\sigma(x) \in \mathbb{F}_q[x]$

$$s_i^{q^\ell} = -\sum_{j=1}^{t} \sigma_j s_{i-j}^{q^\ell}, i = [t, d-2], \ell = [0, m-1]. \qquad (6)$$

- Corresponds to solving an *inhomogeneous linear system*

$$\begin{pmatrix} \mathbf{A}^{q^0} \\ \vdots \\ \mathbf{A}^{q^{m-1}} \end{pmatrix} \cdot \mathbf{x} = \begin{pmatrix} \mathbf{b}^{q^0} \\ \vdots \\ \mathbf{b}^{q^{m-1}} \end{pmatrix}$$

- The *first equation* is the same as for Scheme I
- We get *$m-1$ additional* equations in $\mathbb{F}_{q^m}$

$\Longrightarrow$ Are the additional equations linearly independent?

[6] L.-Z. Shen, F. wei Fu, and X. Guang, "Unique Decoding of Certain Reed-Solomon Codes", 2015

Solving the Key Equation - Scheme V [6]

- Compute *one syndrome* $\mathbf{s} = \mathbf{y}\mathbf{H}^T \in \mathbb{F}_{q^m}^{d-1}$
- Compute *virtual syndromes* $\mathbf{s}^{q^\ell} = \mathbf{y}^{q^\ell}\mathbf{H}^T$ for all $\ell = 0, \dots, m-1$
- Solve the *m key equations* over $\mathbb{F}_{q^m}$ for *the same* error-locator polynomial $\sigma(x) \in \mathbb{F}_q[x]$

$$s_i^{q^\ell} = -\sum_{j=1}^{t} \sigma_j s_{i-j}^{q^\ell}, i = [t, d-2], \ell = [0, m-1]. \tag{6}$$

- Corresponds to solving an *inhomogeneous linear system*

$$\begin{pmatrix} \mathbf{A}^{q^0} \\ \vdots \\ \mathbf{A}^{q^{m-1}} \end{pmatrix} \cdot \mathbf{x} = \begin{pmatrix} \mathbf{b}^{q^0} \\ \vdots \\ \mathbf{b}^{q^{m-1}} \end{pmatrix}$$

- The *first equation* is the same as for Scheme I
- We get $m-1$ *additional* equations in $\mathbb{F}_{q^m}$
  $\Longrightarrow$ Are the additional equations linearly independent?

[6] L.-Z. Shen, F. wei Fu, and X. Guang, "Unique Decoding of Certain Reed-Solomon Codes", 2015

Solving the Key Equation - Scheme V [6]

- Compute *one syndrome* $\mathbf{s} = \mathbf{y}\mathbf{H}^T \in \mathbb{F}_{q^m}^{d-1}$
- Compute *virtual syndromes* $\mathbf{s}^{q^\ell} = \mathbf{y}^{q^\ell}\mathbf{H}^T$ for all $\ell = 0, \ldots, m-1$
- Solve the *m key equations* over $\mathbb{F}_{q^m}$ for *the same* error-locator polynomial $\sigma(x) \in \mathbb{F}_q[x]$

$$s_i^{q^\ell} = -\sum_{j=1}^{t} \sigma_j s_{i-j}^{q^\ell}, i = [t, d-2], \ell = [0, m-1]. \quad (6)$$

- Corresponds to solving an *inhomogeneous linear system*

$$\begin{pmatrix} \mathbf{A}^{q^0} \\ \vdots \\ \mathbf{A}^{q^{m-1}} \end{pmatrix} \cdot \mathbf{x} = \begin{pmatrix} \mathbf{b}^{q^0} \\ \vdots \\ \mathbf{b}^{q^{m-1}} \end{pmatrix}$$

- The *first equation* is the same as for Scheme I
- We get *$m-1$ additional* equations in $\mathbb{F}_{q^m}$
  $\Longrightarrow$ Are the additional equations linearly independent?

[6] L.-Z. Shen, F. wei Fu, and X. Guang, "Unique Decoding of Certain Reed-Solomon Codes", 2015

Solving the Key Equation for Scheme V - Example

$m = 3, \mathbf{A} \in \mathbb{F}_{q^m}^{1\times 3}$, normal basis $\boldsymbol{\beta}$: $\Rightarrow \underline{a_i^q} = \left(a_i^{(m-1)}, a_i^{(0)}, \dots, a_i^{(m-2)}\right)^T$

$\mathbb{F}_{q^m}$

$$\begin{pmatrix} a_0 & a_1 & a_2 \\ a_0^q & a_1^q & a_2^q \\ a_0^{q^2} & a_1^{q^2} & a_2^{q^2} \end{pmatrix} \cdot \mathbf{x} = \begin{pmatrix} b \\ b^q \\ b^{q^2} \end{pmatrix}$$

$\mathbb{F}_q$

$$\begin{pmatrix} a_0^{(0)} & a_1^{(0)} & a_2^{(0)} \\ a_0^{(1)} & a_1^{(1)} & a_2^{(1)} \\ a_0^{(2)} & a_1^{(2)} & a_2^{(2)} \\ a_0^{(2)} & a_1^{(2)} & a_2^{(2)} \\ a_0^{(0)} & a_1^{(0)} & a_2^{(0)} \\ a_0^{(1)} & a_1^{(1)} & a_2^{(1)} \\ a_0^{(1)} & a_1^{(1)} & a_2^{(1)} \\ a_0^{(2)} & a_1^{(2)} & a_2^{(2)} \\ a_0^{(0)} & a_1^{(0)} & a_2^{(0)} \end{pmatrix} \cdot \mathbf{x} = \begin{pmatrix} b^{(0)} \\ b^{(1)} \\ b^{(2)} \\ b^{(2)} \\ b^{(0)} \\ b^{(1)} \\ b^{(1)} \\ b^{(2)} \\ b^{(0)} \end{pmatrix}$$

Solving the Key Equation for Scheme V - Example

$m = 3, \mathbf{A} \in \mathbb{F}_{q^m}^{1\times 3}$, normal basis $\boldsymbol{\beta}$: $\Rightarrow \underline{a_i^q} = \left(a_i^{(m-1)}, a_i^{(0)}, \dots, a_i^{(m-2)}\right)^T$

$\mathbb{F}_{q^m}$

$$\begin{pmatrix} a_0 & a_1 & a_2 \\ a_0^q & a_1^q & a_2^q \\ a_0^{q^2} & a_1^{q^2} & a_2^{q^2} \end{pmatrix} \cdot \mathbf{x} = \begin{pmatrix} b \\ b^q \\ b^{q^2} \end{pmatrix}$$

$\mathbb{F}_q$

$$\begin{pmatrix} a_0^{(0)} & a_1^{(0)} & a_2^{(0)} \\ a_0^{(1)} & a_1^{(1)} & a_2^{(1)} \\ a_0^{(2)} & a_1^{(2)} & a_2^{(2)} \\ a_0^{(2)} & a_1^{(2)} & a_2^{(2)} \\ a_0^{(0)} & a_1^{(0)} & a_2^{(0)} \\ a_0^{(1)} & a_1^{(1)} & a_2^{(1)} \\ a_0^{(1)} & a_1^{(1)} & a_2^{(1)} \\ a_0^{(2)} & a_1^{(2)} & a_2^{(2)} \\ a_0^{(0)} & a_1^{(0)} & a_2^{(0)} \end{pmatrix} \cdot \mathbf{x} = \begin{pmatrix} b^{(0)} \\ b^{(1)} \\ b^{(2)} \\ b^{(2)} \\ b^{(0)} \\ b^{(1)} \\ b^{(1)} \\ b^{(2)} \\ b^{(0)} \end{pmatrix}$$

Solving the Key Equation for Scheme V - Example

$m = 3, \mathbf{A} \in \mathbb{F}_{q^m}^{1\times 3}$, normal basis $\boldsymbol{\beta}$: $\Rightarrow \underline{a_i^q} = \left(a_i^{(m-1)}, a_i^{(0)}, \dots, a_i^{(m-2)}\right)^T$

$\mathbb{F}_{q^m}$

$$\begin{pmatrix} a_0 & a_1 & a_2 \\ a_0^q & a_1^q & a_2^q \\ a_0^{q^2} & a_1^{q^2} & a_2^{q^2} \end{pmatrix} \cdot \mathbf{x} = \begin{pmatrix} b \\ b^q \\ b^{q^2} \end{pmatrix}$$

$\mathbb{F}_q$

$$\begin{pmatrix} a_0^{(0)} & a_1^{(0)} & a_2^{(0)} \\ a_0^{(1)} & a_1^{(1)} & a_2^{(1)} \\ a_0^{(2)} & a_1^{(2)} & a_2^{(2)} \\ a_0^{(2)} & a_1^{(2)} & a_2^{(2)} \\ a_0^{(0)} & a_1^{(0)} & a_2^{(0)} \\ a_0^{(1)} & a_1^{(1)} & a_2^{(1)} \\ a_0^{(1)} & a_1^{(1)} & a_2^{(1)} \\ a_0^{(2)} & a_1^{(2)} & a_2^{(2)} \\ a_0^{(0)} & a_1^{(0)} & a_2^{(0)} \end{pmatrix} \cdot \mathbf{x} = \begin{pmatrix} b^{(0)} \\ b^{(1)} \\ b^{(2)} \\ b^{(2)} \\ b^{(0)} \\ b^{(1)} \\ b^{(1)} \\ b^{(2)} \\ b^{(0)} \end{pmatrix}$$

Solving the Key Equation for Scheme V - Example

$m = 3, \mathbf{A} \in \mathbb{F}_{q^m}^{1\times 3}$, normal basis $\boldsymbol{\beta}$: $\Rightarrow \underline{a_i^q} = \left(a_i^{(m-1)}, a_i^{(0)}, \dots, a_i^{(m-2)}\right)^T$

$\mathbb{F}_{q^m}$

$$\begin{pmatrix} a_0 & a_1 & a_2 \\ a_0^q & a_1^q & a_2^q \\ a_0^{q^2} & a_1^{q^2} & a_2^{q^2} \end{pmatrix} \cdot \mathbf{x} = \begin{pmatrix} b \\ b^q \\ b^{q^2} \end{pmatrix}$$

$\mathbb{F}_q$

$$\begin{pmatrix} a_0^{(0)} & a_1^{(0)} & a_2^{(0)} \\ a_0^{(1)} & a_1^{(1)} & a_2^{(1)} \\ a_0^{(2)} & a_1^{(2)} & a_2^{(2)} \\ a_0^{(2)} & a_1^{(2)} & a_2^{(2)} \\ a_0^{(0)} & a_1^{(0)} & a_2^{(0)} \\ a_0^{(1)} & a_1^{(1)} & a_2^{(1)} \\ a_0^{(1)} & a_1^{(1)} & a_2^{(1)} \\ a_0^{(2)} & a_1^{(2)} & a_2^{(2)} \\ a_0^{(0)} & a_1^{(0)} & a_2^{(0)} \end{pmatrix} \cdot \mathbf{x} = \begin{pmatrix} b^{(0)} \\ b^{(1)} \\ b^{(2)} \\ b^{(2)} \\ b^{(0)} \\ b^{(1)} \\ b^{(1)} \\ b^{(2)} \\ b^{(0)} \end{pmatrix}$$

Solving the Key Equation for Scheme V - Example

$$m = 3, \mathbf{A} \in \mathbb{F}_{q^m}^{1\times 3}, \text{ normal basis } \boldsymbol{\beta} : \Rightarrow \underline{a_i^q} = \left(a_i^{(m-1)}, a_i^{(0)}, \dots, a_i^{(m-2)}\right)^T$$

$\mathbb{F}_{q^m}$

$$\begin{pmatrix} a_0 & a_1 & a_2 \\ a_0^q & a_1^q & a_2^q \\ a_0^{q^2} & a_1^{q^2} & a_2^{q^2} \end{pmatrix} \cdot \mathbf{x} = \begin{pmatrix} b \\ b^q \\ b^{q^2} \end{pmatrix}$$

$\mathbb{F}_q$

$$\begin{pmatrix} a_0^{(0)} & a_1^{(0)} & a_2^{(0)} \\ a_0^{(1)} & a_1^{(1)} & a_2^{(1)} \\ a_0^{(2)} & a_1^{(2)} & a_2^{(2)} \\ a_0^{(2)} & a_1^{(2)} & a_2^{(2)} \\ a_0^{(0)} & a_1^{(0)} & a_2^{(0)} \\ a_0^{(1)} & a_1^{(1)} & a_2^{(1)} \\ a_0^{(1)} & a_1^{(1)} & a_2^{(1)} \\ a_0^{(2)} & a_1^{(2)} & a_2^{(2)} \\ a_0^{(0)} & a_1^{(0)} & a_2^{(0)} \end{pmatrix} \cdot \mathbf{x} = \begin{pmatrix} b^{(0)} \\ b^{(1)} \\ b^{(2)} \\ b^{(2)} \\ b^{(0)} \\ b^{(1)} \\ b^{(1)} \\ b^{(2)} \\ b^{(0)} \end{pmatrix}$$

Solving the Key Equation for Scheme V - Example

$m = 3, \mathbf{A} \in \mathbb{F}_{q^m}^{1\times 3}$, normal basis $\boldsymbol{\beta}$: $\Rightarrow \underline{a_i^q} = \left(a_i^{(m-1)}, a_i^{(0)}, \dots, a_i^{(m-2)}\right)^T$

$\mathbb{F}_{q^m}$

$$\begin{pmatrix} a_0 & a_1 & a_2 \\ a_0^q & a_1^q & a_2^q \\ a_0^{q^2} & a_1^{q^2} & a_2^{q^2} \end{pmatrix} \cdot \mathbf{x} = \begin{pmatrix} b \\ b^q \\ b^{q^2} \end{pmatrix}$$

$\mathbb{F}_q$

$$\begin{pmatrix} a_0^{(0)} & a_1^{(0)} & a_2^{(0)} \\ a_0^{(1)} & a_1^{(1)} & a_2^{(1)} \\ a_0^{(2)} & a_1^{(2)} & a_2^{(2)} \\ a_0^{(2)} & a_1^{(2)} & a_2^{(2)} \\ a_0^{(0)} & a_1^{(0)} & a_2^{(0)} \\ a_0^{(1)} & a_1^{(1)} & a_2^{(1)} \\ a_0^{(1)} & a_1^{(1)} & a_2^{(1)} \\ a_0^{(2)} & a_1^{(2)} & a_2^{(2)} \\ a_0^{(0)} & a_1^{(0)} & a_2^{(0)} \end{pmatrix} \cdot \mathbf{x} = \begin{pmatrix} b^{(0)} \\ b^{(1)} \\ b^{(2)} \\ b^{(2)} \\ b^{(0)} \\ b^{(1)} \\ b^{(1)} \\ b^{(2)} \\ b^{(0)} \end{pmatrix}$$

Solving the Key Equation for Scheme V - Example

$m = 3, \mathbf{A} \in \mathbb{F}_{q^m}^{1\times 3}$, normal basis $\boldsymbol{\beta}$: $\Rightarrow \underline{a_i^q} = \left(a_i^{(m-1)}, a_i^{(0)}, \dots, a_i^{(m-2)}\right)^T$

$\mathbb{F}_{q^m}$

$$\begin{pmatrix} a_0 & a_1 & a_2 \\ a_0^q & a_1^q & a_2^q \\ a_0^{q^2} & a_1^{q^2} & a_2^{q^2} \end{pmatrix} \cdot \mathbf{x} = \begin{pmatrix} b \\ b^q \\ b^{q^2} \end{pmatrix}$$

$\mathbb{F}_q$

$$\begin{pmatrix} a_0^{(0)} & a_1^{(0)} & a_2^{(0)} \\ a_0^{(1)} & a_1^{(1)} & a_2^{(1)} \\ a_0^{(2)} & a_1^{(2)} & a_2^{(2)} \end{pmatrix} \cdot \mathbf{x} = \begin{pmatrix} b^{(0)} \\ b^{(1)} \\ b^{(2)} \end{pmatrix}$$

Solving the Key Equation for Scheme V - Example

$m = 3, \mathbf{A} \in \mathbb{F}_{q^m}^{1\times 3}$, normal basis $\boldsymbol{\beta}$: $\Rightarrow \underline{a_i^q} = \left(a_i^{(m-1)}, a_i^{(0)}, \dots, a_i^{(m-2)}\right)^T$

$\mathbb{F}_{q^m}$

$$\begin{pmatrix} a_0 & a_1 & a_2 \\ a_0^q & a_1^q & a_2^q \\ a_0^{q^2} & a_1^{q^2} & a_2^{q^2} \end{pmatrix} \cdot \mathbf{x} = \begin{pmatrix} b \\ b^q \\ b^{q^2} \end{pmatrix}$$

$\mathbb{F}_q$

$$\begin{pmatrix} a_0^{(0)} & a_1^{(0)} & a_2^{(0)} \\ a_0^{(1)} & a_1^{(1)} & a_2^{(1)} \\ a_0^{(2)} & a_1^{(2)} & a_2^{(2)} \end{pmatrix} \cdot \mathbf{x} = \begin{pmatrix} b^{(0)} \\ b^{(1)} \\ b^{(2)} \end{pmatrix}$$

Observations:

- The additional equations in $\mathbb{F}_q$ are $\mathbb{F}_q$-linearly dependent
- If there exists a *unique solution over* $\mathbb{F}_{q^m}$ then there exists a *unique solution over* $\mathbb{F}_q$ (and vice versa)
- The *probability* of getting a unique solution is *the same*
- The linear systems have the *same size* but they are over *different fields*

Solving the Key Equation for Scheme V - Example

$m = 3, \mathbf{A} \in \mathbb{F}_{q^m}^{1\times 3}$, normal basis $\boldsymbol{\beta}: \Rightarrow \underline{a_i^q} = \left(a_i^{(m-1)}, a_i^{(0)}, \dots, a_i^{(m-2)}\right)^T$

$\mathbb{F}_{q^m}$

$$\begin{pmatrix} a_0 & a_1 & a_2 \\ a_0^q & a_1^q & a_2^q \\ a_0^{q^2} & a_1^{q^2} & a_2^{q^2} \end{pmatrix} \cdot \mathbf{x} = \begin{pmatrix} b \\ b^q \\ b^{q^2} \end{pmatrix}$$

$\mathbb{F}_q$

$$\begin{pmatrix} a_0^{(0)} & a_1^{(0)} & a_2^{(0)} \\ a_0^{(1)} & a_1^{(1)} & a_2^{(1)} \\ a_0^{(2)} & a_1^{(2)} & a_2^{(2)} \end{pmatrix} \cdot \mathbf{x} = \begin{pmatrix} b^{(0)} \\ b^{(1)} \\ b^{(2)} \end{pmatrix}$$

Observations:

- The additional equations in $\mathbb{F}_q$ are $\mathbb{F}_q$-linearly dependent
- If there exists a *unique solution over* $\mathbb{F}_{q^m}$ then there exists a *unique solution over* $\mathbb{F}_q$ (and vice versa)
- The *probability* of getting a unique solution is *the same*
- The linear systems have the *same size* but they are over *different fields*

Solving the Key Equation for Scheme V - Example

$m = 3, \mathbf{A} \in \mathbb{F}_{q^m}^{1\times 3}$, normal basis $\boldsymbol{\beta} : \Rightarrow \underline{a_i^q} = \left(a_i^{(m-1)}, a_i^{(0)}, \ldots, a_i^{(m-2)}\right)^T$

$\mathbb{F}_{q^m}$

$$\begin{pmatrix} a_0 & a_1 & a_2 \\ a_0^q & a_1^q & a_2^q \\ a_0^{q^2} & a_1^{q^2} & a_2^{q^2} \end{pmatrix} \cdot \mathbf{x} = \begin{pmatrix} b \\ b^q \\ b^{q^2} \end{pmatrix}$$

$\mathbb{F}_q$

$$\begin{pmatrix} a_0^{(0)} & a_1^{(0)} & a_2^{(0)} \\ a_0^{(1)} & a_1^{(1)} & a_2^{(1)} \\ a_0^{(2)} & a_1^{(2)} & a_2^{(2)} \end{pmatrix} \cdot \mathbf{x} = \begin{pmatrix} b^{(0)} \\ b^{(1)} \\ b^{(2)} \end{pmatrix}$$

Observations:

- The additional equations in $\mathbb{F}_q$ are $\mathbb{F}_q$-linearly dependent
- If there exists a *unique solution over* $\mathbb{F}_{q^m}$ then there exists a *unique solution over* $\mathbb{F}_q$ (and vice versa)
- The *probability* of getting a unique solution is *the same*
- The linear systems have the *same size* but they are over *different fields*

Solving the Key Equation for Scheme V - Example

$$m = 3, \mathbf{A} \in \mathbb{F}_{q^m}^{1\times 3}, \text{ normal basis } \boldsymbol{\beta} : \Rightarrow \underline{a_i^q} = \left(a_i^{(m-1)}, a_i^{(0)}, \dots, a_i^{(m-2)}\right)^T$$

$\mathbb{F}_{q^m}$

$$\begin{pmatrix} a_0 & a_1 & a_2 \\ a_0^q & a_1^q & a_2^q \\ a_0^{q^2} & a_1^{q^2} & a_2^{q^2} \end{pmatrix} \cdot \mathbf{x} = \begin{pmatrix} b \\ b^q \\ b^{q^2} \end{pmatrix}$$

$\mathbb{F}_q$

$$\begin{pmatrix} a_0^{(0)} & a_1^{(0)} & a_2^{(0)} \\ a_0^{(1)} & a_1^{(1)} & a_2^{(1)} \\ a_0^{(2)} & a_1^{(2)} & a_2^{(2)} \end{pmatrix} \cdot \mathbf{x} = \begin{pmatrix} b^{(0)} \\ b^{(1)} \\ b^{(2)} \end{pmatrix}$$

Observations:

- The additional equations in $\mathbb{F}_q$ are $\mathbb{F}_q$-linearly dependent
- If there exists a *unique solution over* $\mathbb{F}_{q^m}$ then there exists a *unique solution over* $\mathbb{F}_q$ (and vice versa)
- The *probability* of getting a unique solution is *the same*
- The linear systems have the *same size* but they are over *different fields*

Syndrome Decoding of Punctured Gabidulin Codes

Field automorphism: $\theta(a) \stackrel{\text{def}}{=} a^h$ where q is a power of h

Reversed syndromes: $\bar{s}_i \stackrel{\text{def}}{=} \theta^{i-(d-2)}(s_{d-2-i})$ for $i \in [0, d-2]$

Key equation - Scheme I

$$\bar{s}_i^{(\ell)} = -\sum_{j=1}^{t} \sigma_j \theta^j \left(\bar{s}_{i-j}^{(\ell)}\right), i = [t, d-2], \ell = [0, m-1]. \qquad (7)$$

Key equation - Scheme V

$$\bar{s}_i^{q^\ell} = -\sum_{j=1}^{t} \sigma_j \theta^j \left(\bar{s}_{i-j}^{q^\ell}\right), i = [t, d-2], \ell = [0, m-1]. \qquad (8)$$

Syndrome Decoding: Scheme I vs. Scheme V

Theorem (Main Result)

For punctured RS and G codes the probabilistic unique syndrome decoders for Schemes I and V are equivalent having decoding radius

$$t_{max} = \frac{m}{m+1}(d-1),$$

decoding failure probability

$$P_f(t) \leq \gamma q^{-(m+1)(t_{max}-t)-1}$$

and decoding complexity $\mathcal{O}(mn^2)$ operations in the field $\mathbb{F}_q$ for Scheme I and in $\mathbb{F}_{q^m}$ for Scheme V, where $\gamma \leq 3.5$ and $\gamma \approx 1$ for RS codes.

- One multiplication in $\mathbb{F}_{q^m}$ costs $\approx m^2$ multiplications in $\mathbb{F}_q$
  $\Longrightarrow$ Scheme V: $\mathcal{O}(m^3 n^2)$, Scheme I: $\mathcal{O}(mn^2)$ in $\mathbb{F}_q$
- Use decoder with the lowest computational complexity
  $\Longrightarrow$ Scheme I

Syndrome Decoding: Scheme I vs. Scheme V

Theorem (Main Result)

For punctured RS and G codes the probabilistic unique syndrome decoders for Schemes I and V are equivalent having decoding radius

$$t_{max} = \frac{m}{m+1}(d-1),$$

decoding failure probability

$$P_f(t) \leq \gamma q^{-(m+1)(t_{max}-t)-1}$$

and decoding complexity $\mathcal{O}(mn^2)$ operations in the field $\mathbb{F}_q$ for Scheme I and in $\mathbb{F}_{q^m}$ for Scheme V, where $\gamma \leq 3.5$ and $\gamma \approx 1$ for RS codes.

- One multiplication in $\mathbb{F}_{q^m}$ costs $\approx m^2$ multiplications in $\mathbb{F}_q$
  $\Longrightarrow$ Scheme V: $\mathcal{O}(m^3 n^2)$, Scheme I: $\mathcal{O}(mn^2)$ in $\mathbb{F}_q$
- Use decoder with the lowest computational complexity
  $\Longrightarrow$ Scheme I

Syndrome Decoding: Scheme I vs. Scheme V

Theorem (Main Result)

For punctured RS and G codes the probabilistic unique syndrome decoders for Schemes I and V are equivalent having decoding radius

$$t_{max} = \frac{m}{m+1}(d-1),$$

decoding failure probability

$$P_f(t) \leq \gamma q^{-(m+1)(t_{max}-t)-1}$$

and decoding complexity $\mathcal{O}(mn^2)$ operations in the field $\mathbb{F}_q$ for Scheme I and in $\mathbb{F}_{q^m}$ for Scheme V, where $\gamma \leq 3.5$ and $\gamma \approx 1$ for RS codes.

- One multiplication in $\mathbb{F}_{q^m}$ costs $\approx m^2$ multiplications in $\mathbb{F}_q$
  $\Longrightarrow$ Scheme V: $\mathcal{O}(m^3 n^2)$, Scheme I: $\mathcal{O}(mn^2)$ in $\mathbb{F}_q$
- Use decoder with the lowest computational complexity
  $\Longrightarrow$ Scheme I

Conclusion

- *Analyzed* and *compared* syndrome decoding strategies for punctured RS and Gabidulin codes
- We showed that the *syndrome-based* decoding schemes over $\mathbb{F}_q$ are *equivalent* to the corresponding decoding schemes in the $\mathbb{F}_{q^m}$
- Allows to choose the decoder with the *lowest complexity*
  $\Rightarrow$ Decode punctured RS and G codes as m-interleaved codes over the subfield $\mathbb{F}_q$
- Similar results for *interpolation-based* decoding [11]

---

[11] H. Bartz, V. Sidorenko "On List-Decoding Schemes for Punctured Reed-Solomon, Gabidulin and Subspace Codes", accepted Redundancy 2016

Thank you! Questions?

{hannes.bartz, vladimir.sidorenko}@tum.de

A.1 Syndrome Decoding of Punctured Gabildulin Codes

Lemma

*The key equation (**??**) over $\mathbb{F}_{q^m}$ has a unique solution if and only if the key equation* (5)

$$\overline{s}_i^{(\ell)} = -\sum_{j=1}^{t} \sigma_j \theta^j \left(\overline{s}_{i-j}^{(\ell)} \right), i \in [t, d-2], \ell \in [0, m-1].$$

over $\mathbb{F}_q$ has a unique solution.

Proof.

Let $\sigma_0 = 1$. For $\ell = 0$ (**??**) can be expanded as

$$\overline{s}_i = -\sum_{j=1}^{t} \sigma_j \theta^j (\overline{s}_{i-j})$$

$$\iff \quad \sum_{l=0}^{m-1} \theta^{i-(d-2)}(\beta_l) \underbrace{\sum_{j=0}^{t} \sigma_j \theta^{i-(d-2)} \left(s_{d-2-i+j}^{(l)} \right)}_{a_{i,j}^{(l)} \in \mathbb{F}_q} = 0. \qquad (9)$$

Proof. (cont.)

Since $\beta_0, \ldots, \beta_{m-1}$ are $\mathbb{F}_q$-linearly independent the elements $\theta^{i-(d-2)}(\beta_0), \ldots, \theta^{i-(d-2)}(\beta_m)$ are also $\mathbb{F}_q$-linearly independent. Thus (9) has only the trivial solution (all coefficients $a_{i,j}^{(l)} = 0$), i.e.

$$\sum_{j=0}^{t} \sigma_j \theta^{i-(d-2)}\left(s_{d-2-i+j}^{(l)}\right) = 0$$
$$\iff \quad \sum_{j=0}^{t} \sigma_j \theta^{j}\left(\overline{s}_{i-j}^{(l)}\right) = 0 \qquad (10)$$

for all $l \in [0, m-1]$. Since $\sigma_0 = 1$ we can rewrite (10) as

$$\sum_{j=0}^{t} \sigma_j \theta^{j}\left(\overline{s}_{i-j}^{(l)}\right) = 0 \quad \iff \quad \overline{s}_{i}^{(l)} = -\sum_{j=1}^{t} \sigma_j \theta^{j}\left(\overline{s}_{i-j}^{(l)}\right) \qquad (11)$$

for all $i \in [t, d-2]$ and $l \in [0, m-1]$ which is the key equation (5) of Scheme I over $\mathbb{F}_q$. ∎