Fifteenth International Workshop on Algebraic and Combinatorial Coding Theory
June 18-24, 2016, Albena, Bulgaria *pp. 35–40*

On Syndrome Decoding of Punctured Reed-Solomon and Gabidulin Codes [1]

Hannes Bartz hannes.bartz@tum.de
Vladimir Sidorenko vladimir.sidorenko@tum.de
Institute for Communications Engineering
Technical University of Munich, D-80290 Munich, Germany

Abstract. Being evaluation codes, punctured Reed-Solomon (RS) and Gabidulin (G) codes over the field $\mathbb{F}_{q^m}$ *with locators from the subfield* $\mathbb{F}_q$ can be represented as interleaving of m correspondent codes over the subfield $\mathbb{F}_q$ or can be considered as virtual interleaving of m correspondent codes over the field $\mathbb{F}_{q^m}$. Using a probabilistic unique syndrome decoder, m-interleaved or virtually interleaved codes can be decoded up to *the same* radius $\frac{m}{m+1}(d-1)$, where d is the code distance in Hamming metric for RS codes and in rank metric for G codes. We show that the correspondent decoders over the subfield $\mathbb{F}_q$ and the field $\mathbb{F}_{q^m}$ are equivalent and conclude that in practice one should use a decoder over the subfield since it has less complexity.

1 Introduction

Reed-Solomon (RS) [1] and Gabidulin (G) [2] codes belong to the family of *evaluation* codes and are widely used for error correction in many applications. An evaluation code over the finite field $\mathbb{F}_{q^m}$ is constructed by evaluating all polynomials with coefficients from $\mathbb{F}_{q^m}$ of restricted degree at a set of code locators. By choosing the code locators from the subfield $\mathbb{F}_q$ we obtain a *punctured* evaluation code over $\mathbb{F}_{q^m}$ which can be equivalently interpreted as an *m-interleaved code* $\mathcal{I}$ over the subfield $\mathbb{F}_q$ [3].

It is known that m-interleaved RS and G codes over $\mathbb{F}_q$ with distance d can correct with high probability up to $\frac{m}{m+1}(d-1)$ errors in the corresponding metric [4,5]. In [6,7] it was shown that the same decoding radius can be achieved by computing element-wise q-powers of the received word at the decoder. This results in a received word V of a *virtually m-interleaved code* $\mathcal{V}$ over the large field $\mathbb{F}_{q^m}$. Virtual interleaving with usual powers was originally proposed in [8] and was modified to q-powers in [6]. For both decoding schemes either a syndrome- or interpolation-based decoder can be used.

In this paper we analyze and compare probabilistic unique syndrome-based decoding algorithms for interleaved and virtually interleaved RS and G codes.

[1] H. Bartz was supported by the German Ministry of Education and Research in the framework of an Alexander von Humboldt-Professorship. V. Sidorenko is on leave from the Institute for Information Transmission Problems, Russian Academy of Sciences.

We show that the syndrome-based decoder of the code $\mathcal{I}$ over the subfield $\mathbb{F}_q$ is *equivalent* to the respective decoder of $\mathcal{V}$ in the field $\mathbb{F}_{q^m}$. This means, that for the same input the decoders return the same output and shows, that the decoding failure probability is the same for both decoders. It allows us to choose the decoder with the lowest computational complexity, i.e., the respective decoder over the subfield $\mathbb{F}_q$. The extended version of the paper with proofs is available online at http://goo.gl/NL78P5.

2 Preliminaries

Let $\mathbb{F}_h$ be a finite field, where h is a power of a prime. Let $\mathbb{F}_q$ and $\mathbb{F}_{q^m}$ be extensions of $\mathbb{F}_h$. By the column vector $\underline{a} = \left(a^{(0)}a^{(1)}\dots a^{(m-1)}\right)^T \subset \mathbb{F}_q^m$ we denote the expansion of an element $a \in \mathbb{F}_{q^m}$ w.r.t. a fixed basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Given a vector $\mathbf{a}$ of length n over $\mathbb{F}_{q^m}$, we introduce the $m \times n$ expansion matrix over $\mathbb{F}_q$ as $\underline{\mathbf{a}} = (\underline{a_0}, \dots, \underline{a_{n-1}})$.

By $\mathbb{F}_{q^m}[x]$ we denote the ring of all polynomials $g(x) = \sum_{i=0}^{d} g_i x^i$ over $\mathbb{F}_{q^m}$ and $\mathbb{F}_{q^m}[x]_{<k}$ is the set of all polynomial from $\mathbb{F}_{q^m}[x]$ with degree less than k.

A nonzero polynomial of the form $p(x) = \sum_{i=0}^{d} p_i x^{[i]}$, where $[i]$ denotes the i Frobenius power $[i] = h^i$, with $p_i \in \mathbb{F}_{q^m}$, $p_d \neq 0$, is called an *h-linearized polynomial* of h-degree $\deg_h(p(x)) = d$. By $\mathbb{L}_{q^m}[x]$ we denote the ring of all h-linearized polynomials over $\mathbb{F}_{q^m}$ and $\mathbb{L}_{q^m}[x]_{<k}$ denotes the set of all polynomials from $\mathbb{L}_{q^m}[x]$ with h-degree less than k.

RS and G codes belong to a class of *evaluation codes*, which are defined as follows.

Evaluation code. Assume $0 < k \leq n$ and $m \geq 1$ are integers. Given an n-vector of code locators $\boldsymbol{\alpha} = (\alpha_0\, \alpha_1 \dots \alpha_{n-1})$ over $\mathbb{F}_{q^m}$ and a set $\mathcal{P}(m)$ of polynomials $f(x)$ over $\mathbb{F}_{q^m}$, where $\mathcal{P}(m) = \mathbb{F}_{q^m}[x]_{<k}$ or $\mathcal{P}(m) = \mathbb{L}_{q^m}[x]_{<k}$. We define $f(\boldsymbol{\alpha}) = (f(\alpha_0)\, f(\alpha_1) \dots f(\alpha_{n-1}))$. The evaluation code $\mathcal{C}_{ev}$ is the set of all n-words

$$\mathcal{C}_{ev}(n, k, \boldsymbol{\alpha}, \mathcal{P}(m)) = \{f(\boldsymbol{\alpha}) \mid f \in \mathcal{P}(m)\} \tag{1}$$

obtained by evaluating all polynomials f from $\mathcal{P}(m)$ at the locators $\boldsymbol{\alpha}$. RS and G codes can be defined as follows.

Reed-Solomon code. If the locators α_i are pairwise different and $\mathcal{P}(m) = \mathbb{F}_{q^m}[x]_{<k}$, then the code $\mathcal{C}_{ev}$ is an $[n, k]$ linear *Reed-Solomon* code over $\mathbb{F}_{q^m}$ with code distance $d = n - k + 1$ [1] in Hamming metric.

Gabidulin code. Assume that the locators α_i are $\mathbb{F}_h$-linearly independent. Let $\mathcal{P}(m) = \mathbb{L}_{q^m}[x]_{<k}$, then $\mathcal{C}_{ev}$ is an $[n, k]$ linear *Gabidulin* code over $\mathbb{F}_{q^m}$ with code distance $d = n - k + 1$ [2] in rank metric. The rank distance between two n-words $\mathbf{v}, \mathbf{w}$ over $\mathbb{F}_{q^m}$ is defined as $\mathrm{rk}(\underline{\mathbf{v}} - \underline{\mathbf{w}})$ over $\mathbb{F}_h$.

In general, RS and G codes with locators from the field $\mathbb{F}_{q^m}$ can correct errors of weight up to $(d-1)/2$ in the correspondent metric. It is known [3] that it is possible to correct with high probability more errors if we puncture the

codes and take locators from the subfield $\mathbb{F}_q$ only. Now we introduce (proper) punctured codes.

Punctured evaluation code. The evaluation code (1) over $\mathbb{F}_{q^m}$ is called *proper punctured* if all locators α_i belong to the subfield $\mathbb{F}_q$. Later on we consider proper punctured codes only and call them simply "punctured". This gives us definitions of *punctured RS and punctured G codes* as well.

Interleaved codes over small field $\mathbb{F}_q$ (Scheme I). Let us show that a punctured evaluation code over the large field $\mathbb{F}_{q^m}$ with locators $\alpha_i \in \mathbb{F}_q$ is equivalent to interleaving of m evaluation codes over the subfield $\mathbb{F}_q$ [3]. Let $f(x) = \sum_i f_i x^i$ be a polynomial from $\mathcal{P}(m)$. By representing each coefficient f_i by $\underline{f_i}$ we can write one polynomial $f(x) \in \mathcal{P}(m)$ as m polynomials $f^{(j)}(x) = \sum_i f_i^{(j)} x^i \in \mathcal{P}(1)$, $\forall j \in [0, m-1]$. Now every codeword of the punctured evaluation code (1) can be written over the small field $\mathbb{F}_q$ as $\mathbf{c} = f(\boldsymbol{\alpha}) \Rightarrow$

$$\begin{pmatrix} f^{(0)}(\boldsymbol{\alpha}) \\ \vdots \\ f^{(m-1)}(\boldsymbol{\alpha}) \end{pmatrix} = \begin{pmatrix} f^{(0)}(\alpha_0) & \cdots & f^{(0)}(\alpha_{n-1}) \\ \vdots & \vdots & \vdots \\ f^{(m-1)}(\alpha_0) & \cdots & f^{(m-1)}(\alpha_{n-1}) \end{pmatrix} \stackrel{\text{def}}{=} I. \tag{2}$$

Since $f^{(j)}(x) \in \mathcal{P}(1)$ for all j, every row in the $m \times n$ matrix I over $\mathbb{F}_q$ in (2) is a codeword of $\mathcal{C}_{ev}(n, k, \boldsymbol{\alpha}, \mathcal{P}(1))$. Hence I is obtained by interleaving of m codewords from $\mathcal{C}_{ev}(n, k, \boldsymbol{\alpha}, \mathcal{P}(1))$. This means that every codeword $f(\boldsymbol{\alpha}) \in \mathbb{F}_{q^m}^n$ of the code $\mathcal{C}_{ev}(n, k, \boldsymbol{\alpha}, \mathcal{P}(m))$ can be written as interleaving I of m codewords from $\mathcal{C}_{ev}(n, k, \boldsymbol{\alpha}, \mathcal{P}(1))$.

Virtual interleaving over the field $\mathbb{F}_{q^m}$ (Scheme V). Consider a codeword $\mathbf{c} = (c_0\, c_1 \ldots\, c_{n-1}) = f(\boldsymbol{\alpha})$ of a punctured evaluation code $\mathcal{C}_{ev}(n, k, \boldsymbol{\alpha}, \mathcal{P}(m))$ with locators $\alpha_i \in \mathbb{F}_q$ and compute the element-wise q-powers $\mathbf{c}^{q^j} = (c_0^{q^j}\, c_1^{q^j} \ldots\, c_{n-1}^{q^j})$. For $f(x) = \sum_i f_i x^i \in \mathcal{P}(m)$ denote a bijective map $f \to f^{q^j}$ where $f^{q^j}(x) = \sum_i f_i^{q^j} x^i \in \mathcal{P}(m)$. Since $c_i = f(\alpha_i)$ where $\alpha_i \in \mathbb{F}_q$ for all $i \in [0, n-1]$ and $f \in \mathcal{P}(m)$, we have $c_i^{q^j} = (f(\alpha_i))^{q^j} = f^{q^j}(\alpha_i)$. Hence $\mathbf{c}^{q^j} \in \mathcal{C}_{ev}(n, k, \boldsymbol{\alpha}, \mathcal{P}(m))$ and from one codeword $\mathbf{c}$ we can virtually create m codewords $\mathbf{c}^{q^j}$ for $j \in [0, m-1]$. These m codewords form an $m \times n$ matrix V over the big field $\mathbb{F}_{q^m}$ of the virtually m-interleaved code $\mathbf{c} = f(\boldsymbol{\alpha}) \Rightarrow$

$$\begin{pmatrix} f^{q^0}(\boldsymbol{\alpha}) \\ \vdots \\ f^{q^{m-1}}(\boldsymbol{\alpha}) \end{pmatrix} = \begin{pmatrix} f^{q^0}(\alpha_0) & \cdots & f^{q^0}(\alpha_{n-1}) \\ \vdots & \vdots & \vdots \\ f^{q^{m-1}}(\alpha_0) & \cdots & f^{q^{m-1}}(\alpha_{n-1}) \end{pmatrix} \stackrel{\text{def}}{=} V. \tag{3}$$

Notice that in the case of virtual interleaving V, we still transmit just one codeword $\mathbf{c} = f(\boldsymbol{\alpha})$ of the original punctured code and receive one word $\mathbf{y}$ corrupted by errors. One can think that the rest $m-1$ codewords $\mathbf{c}^{q^j}$ were virtually transmitted as well. The correspondent $m-1$ received words can be computed at the receiver as $\mathbf{y}^{q^j}$. For the Hamming metric t errors in the received word $\mathbf{y}$ will induce t erroneous columns in the virtually received matrix

V. If the received word $\mathbf{y}$ is corrupted by an error of rank t then matrix V will be corrupted by an error of rank t as well.

What can we gain using I or V interleaving? It is known [4,5] that decoding of an s-interleaved code with distance d can be done up to the radius $\frac{m}{m+1}(d-1)$ with high probability. Hence we can increase the decoding radius almost twice if we use probabilistic decoders I or V instead of decoding the original punctured code up to radius $(d-1)/2$. Any known syndrome-based decoder for interleaved codes can be applied to get this gain. However, the complexity of operations increases with the field size. This is a disadvantage of Scheme V. Can we gain something using Scheme V instead of I? For example, if a syndrome decoder is used with Scheme I it will fail with probability at most (field size)$^{-1} = 1/q$. Does it mean that the failure probability of Scheme V over the large field $\mathbb{F}_{q^m}$ is smaller than the one of Scheme I as it is claimed in [7]? In the next section we will describe decoders for I and V matrices, analyse and compare them.

3 Syndrome Decoding of Punctured Reed-Solomon and Gabidulin Codes

Consider a proper punctured evaluation code $\mathcal{C}_{ev}(n, k, \boldsymbol{\alpha}, \mathcal{P}(m))$ which is a RS or G code over the field $\mathbb{F}_{q^m}$ with locators α_i from the subfield $\mathbb{F}_q$. Since $\alpha_i \in \mathbb{F}_q$ a parity check matrix $\mathbf{H}$ of the code is also over the subfield $\mathbb{F}_q$. Let a codeword $\mathbf{c} \in \mathcal{C}_{ev}$ be transmitted and an n-word $\mathbf{y}$ over $\mathbb{F}_{q^m}$ be received. Then the error vector in the channel is $\mathbf{e} = \mathbf{y} - \mathbf{c}$ and the number of errors t is the Hamming weight of the error $\mathbf{e}$ in case of RS code and $t = \mathrm{rk}(\underline{\mathbf{e}})$ for G code. Given received word $\mathbf{y}$, the unique decoder should output a codeword or declare a failure.

A syndrome decoder first computes the syndrome vector $\mathbf{s} = \mathbf{y}\mathbf{H}^T \in \mathbb{F}_{q^m}^{n-k}$. If the syndrome $\mathbf{s} = \mathbf{0}$ then $\mathbf{y}$ is a codeword, otherwise for $\mathbf{s} \neq \mathbf{0}$ the following key equation (6) must be solved [9, 10]. Define the field automorphism θ as

$$\theta(a) \stackrel{\text{def}}{=} \begin{cases} a & \text{for RS codes} \\ a^h & \text{for G codes} \end{cases} \tag{4}$$

and the *reversed* syndromes for $i \in [0, d-2]$ as

$$\overline{s}_i \stackrel{\text{def}}{=} \begin{cases} s_i & \text{for RS codes} \\ \theta^{i-(d-2)}(s_{d-2-i}) & \text{for G codes} \end{cases} . \tag{5}$$

Key equation.

$$\overline{s}_i = -\sum_{j=1}^{t} \sigma_j \theta^j(\overline{s}_{i-j}), \quad i = [t, d-2]. \tag{6}$$

To solve the key equation means to find minimum integer $t > 0$ such that (6) has a solution $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_t)$. If the solution is not unique the decoder fails.

Otherwise it forms the error locator polynomial

$$\sigma(x) = \begin{cases} 1 + \sigma_1 x + \cdots + \sigma_t x^t & \in \mathbb{F}_{q^m}[x] \quad \text{for RS codes} \\ x + \sigma_1 x^h + \cdots + \sigma_t x^{h^t} & \in \mathbb{L}_{q^m}[x] \quad \text{for G codes} \end{cases} . \tag{7}$$

Having the error locator polynomial it is easy to find the error vector $\mathbf{e}$ using known approaches, e.g. in [9, 10], and to compute the codeword $\mathbf{c} = \mathbf{y} - \mathbf{e}$.

So, the main part of the decoder is solving the key equation, which can be done by solving the linear system of equations (6) with coefficients from $\mathbb{F}_{q^m}$ for $t = 1, 2, ...$ This can be done by standard linear algebra resulting in a decoding algorithm which always corrects up to $d/2$ errors, but we would like to correct more errors using a probabilistic decoder as follows.

Locators α_i of punctured codes belong to the subfield $\mathbb{F}_q$. Since the roots of an error locator polynomial belong to the subfield $\mathbb{F}_q$ of code locators, the coefficients of the error locator polynomial $\sigma(x)$ also belong to $\mathbb{F}_q$ and we should find unknowns σ_i in (6) from the subfield $\mathbb{F}_q$. This allows to write more equations and as a result to correct more errors using Schemes I or V as follows.

Key equation over subfield, Scheme I. We receive the vectort $\mathbf{y}$, i.e. the matrix $\underline{\mathbf{y}}$ with m interleaved words $\mathbf{y}^{(\ell)}$ over $\mathbb{F}_q$. The syndromes $\mathbf{s}^{(\ell)}$ can be computed as $\mathbf{s}^{(\ell)} = \mathbf{y}^{(\ell)}\mathbf{H}^T$ because $\mathbf{H}$ is over $\mathbb{F}_q$. Since error locators are common for interleaved words [5, 11], we can write the key equation (6) for each syndrome $\mathbf{s}^{(\ell)}$ with the common error locator $\sigma(x)$ and get the following system of equations *over the subfield* $\mathbb{F}_q$

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

Key equation for virtual interleaving, Scheme V. The syndromes $\mathbf{s}^{q^\ell}$, $\ell = [0, m-1]$, can be computed from m virtually received words $\mathbf{y}^{q^\ell}$ as $\mathbf{y}^{q^\ell}\mathbf{H}^T = \mathbf{s}^{q^\ell}$ since $\mathbf{H}$ is over $\mathbb{F}_q$. Virtual error vectors $\mathbf{y}^{q^\ell} - \mathbf{c}^{q^\ell} = \mathbf{e}^{q^\ell}$ have the same weight t and common error locations. Hence we can write the key equation (6) for each syndrome $\mathbf{s}^{q^\ell}$ with common error locator $\sigma(x)$ and get the following system of equations *over the field* $\mathbb{F}_{q^m}$

$$\overline{s}_i^{q^\ell} = -\sum_{j=1}^{t} \sigma_j \theta^j \left(\overline{s}_{i-j}^{q^\ell} \right), i = [t, d-2], \ell = [0, m-1]. \tag{9}$$

Lemma 1 *Given a vector* $\mathbf{s} \neq \mathbf{0}$ *over* $\mathbb{F}_{q^m}$ *and integer* $0 < t < d-1$*, a solution* $\boldsymbol{\sigma}_I$ *of (8) is unique if and only if (9) has a unique solution* $\boldsymbol{\sigma}_V$*. In this case* $\boldsymbol{\sigma}_I = \boldsymbol{\sigma}_V$ *is a vector over* $\mathbb{F}_q$*.*

This means that for fixed received word $\mathbf{y}$ both decoders I and V will find the same error locator polynomial in case when (8) and (9) have unique solution and output the same result, otherwise both decoders will fail. Hence *the decoders are equivalent* and we get the following theorem, where we assume that the errors $\mathbf{e}$ of weight t have equal probability to estimate failure probabilities.

Theorem 1 *For punctured RS and G codes unique probabilistic syndrome decoders of Schemes I and V are equivalent having decoding radius* $t_{max} = \frac{m}{m+1}(d-1)$*, 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. Decoding failure probability* $P_f(t) \leq \gamma q^{-(m+1)(t_{max}-t)-1}$*, where* t *is error weight,* $\gamma \leq 3.5$ *and* $\gamma \approx 1$ *for RS codes.*

Using fast operations, decoding can be further accelerated to sub-quadratic complexity. The obtained results are directly applied to correcting *errors and erasures*. Without establishing equivalence it is not easy to estimate the failure probability for Scheme V which can lead to incorrect conclusions [7].

References

[1] I. S. Reed, "A Class of Multiple-Error-Correcting Codes and the Decoding Scheme," *IRE Trans. Inf. Theory*, vol. 4, no. 4, pp. 38–49, Sep. 1954.

[2] E. M. Gabidulin, "Theory of Codes with Maximum Rank Distance," *Probl. Inf. Transm.*, vol. 21, no. 1, pp. 3–16, 1985.

[3] V. Sidorenko, G. Schmidt, and M. Bossert, "Decoding Punctured Reed-Solomon Codes up to the Singleton Bound," in *, 2008 7th Int. ITG Conf. on Source and Channel Coding (SCC)*, Jan 2008.

[4] D. Bleichenbacher, A. Kiayias, and M. Yung, "Decoding Interleaved Reed–Solomon Codes over Noisy Channels," *Theor. Comput. Sci.*, vol. 379, no. 3, pp. 348–360, Jul. 2007.

[5] G. Schmidt, V. R. Sidorenko, and M. Bossert, "Collaborative Decoding of Interleaved Reed–Solomon Codes and Concatenated Code Designs," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 2991–3012, 2009.

[6] V. Guruswami and C. Xing, "List Decoding Reed–Solomon, Algebraic-Geometric, and Gabidulin Subcodes up to the Singleton Bound," *Electronic Colloq. Comp. Complexity*, vol. 19, no. 146, 2012.

[7] L.-Z. Shen, F. wei Fu, and X. Guang, "Unique Decoding of Certain Reed-Solomon Codes," *IEICE Trans. on Fund. of Electr., Comm. and Comput. Sciences*, vol. E98-A, no. 12, pp. 2728–2732, Dec. 2015.

[8] G. Schmidt, V. R. Sidorenko, and M. Bossert, "Syndrome Decoding of Reed-Solomon Codes Beyond Half the Minimum Distance Based on Shift-Register Synthesis," *IEEE Trans. Inf. Theory*, vol. 56, no. 10, pp. 5245–5252, Oct. 2010.

[9] R. E. Blahut, *Theory and Practice of Error Control Codes*, 1st ed. Addison-Wesley, 1983.

[10] D. Silva, F. R. Kschischang, and R. Kötter, "A Rank-Metric Approach to Error Control in Random Network Coding," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 3951–3967, 2008.

[11] V. R. Sidorenko, L. Jiang, and M. Bossert, "Skew-Feedback Shift-Register Synthesis and Decoding Interleaved Gabidulin Codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 2, pp. 621–632, Feb. 2011.