Collaborative Decoding of Interleaved Reed-Solomon Codes Over Galois Rings

Marc A. Armand

Dept of Electrical & Computer Engineering
National University of Singapore

1 Background

- Jointly decoding codewords of a Reed-Solomon (RS) code arranged in parallel, or *collaborative* decoding of *interleaved* RS codes, first proposed by:
  - V. Y. Krachkovsky and Y. X. Lee, "Decoding for interleaved Reed-Solomon schemes," *IEEE Trans. Magn.*, vol. 33, pp. 2740–2743, Sep. 1997.
- Notable related works that have appeared in the literature include:
  - D. Bleichenbacher, A. Kiayas and M. Yung, "Decoding of interleaved Reed-Solomon codes over noisy data," *Lect. Notes Computer Sci.*, vol. 2719, pp. 97–108, Jan. 2003.
  - A. Brown, L. Minder and A. Shokrollahi, "Improved decoding of interleaved AG codes," *Lect. Notes Computer Sci.*, vol. 3796, pp. 37–46, 2005.
  - 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, Jul. 2009.

- Approach of Bleichenbacher et. al. may be viewed as a generalization of the Welch-Berlekamp approach which Brown et. al. further extended to decode interleaved AG codes.
- Approach of Schmidt et. al. is based on multisequence shift register synthesis (MSRS) and has its roots in the work by Krachkovsky & Lee.
- Given an interleaved code $\mathcal{RS}(\ell; n, k; \mathbb{F}_q)$ comprising ℓ parallel copies of an (n, k) RS code over $\mathbb{F}_q$ where $q := 2^m$, the MSRS approach enables the correction of up to

$$t_m := \left\lfloor \frac{\ell}{\ell + 1}(n - k) \right\rfloor$$

(column) errors, which may be viewed as elements of $\mathbb{F}_{q^\ell}$.

- If the errors are uniformly distributed on $\mathbb{F}_{q^\ell} \setminus \{0\}$, probability of decoding failure, given that t errors have occurred, is

$$\leq \left(\frac{q^\ell - (1/q)}{q^\ell - 1} \right)^t \frac{q^{-(\ell+1)(t_m - t)}}{q-1} \tag{1}$$

where $t \leq t_m$ but greater than the guaranteed decoding radius,

$$t_g := \lfloor (n-k)/2 \rfloor.$$

Probability of decoding failure, given that t_m errors have occurred, is therefore at most $\mathcal{O}(1/q)$.

- Probability of decoding error, given that t errors have occurred, $t_g < t \leq t_m$, is

$$\leq \frac{\sum_{w=n-k+1}^{t+t_m} A_w \sum_{j=0}^{\min\{t,t_m\}} U(q^\ell, t, w, j)}{\binom{n}{t}(q^\ell - 1)^t} \tag{2}$$

where A_w is the number of codewords of weight w, and

$$U(q^\ell, t, w, j) := \sum_{i=\lceil \frac{t+w-j}{2} \rceil}^{t+w-j} \binom{w}{i} \binom{i}{j-t-w+2i} \binom{n-w}{t-i} \cdot (q^\ell - 2)^{j-t-w+2i} (q^\ell - 1)^{t-i}.$$

A_w is obtained by viewing $\mathcal{RS}(\ell; n, k; \mathbb{F}_q)$ as an (n, k) MDS code over $\mathbb{F}_{q^\ell}$, for which, the weight distribution is well known.

2 This Work

- We consider q^ℓ-ary interleaved codes formed from RS codes over an alphabet of cardinality q^2, i.e., the Galois ring

$$R := \mathrm{GR}(4,\, m) \cong \mathbb{Z}_4[y]/\langle \Phi \rangle$$

  where Φ is a basic irreducible polynomial in $\mathbb{Z}_4[y]$ of degree m.

- Motivation stems from the question: "Can a q^ℓ-ary interleaved code formed from $\ell/2$ parallel copies of an (n, k) RS code over R offer any advantage over its field counterpart formed from ℓ parallel copies of an (n, k) RS code over $\mathbb{F}_q$?"

  We will show that when ℓ is large, the former interleaved code can be as good as its counterpart over $\mathbb{F}_{q^\ell}$, in terms of the word error probabilities of their respective collaborative decoders, while incurring lower decoding complexity.

3 The Codes

- Throughout, let $\ell \geq 4$ and even.
- Let C be an $(n,\, k)$ RS code over R whose generator polynomial is $\prod_{i=1}^{n-k}(X - \xi^i)$ and parity-check matrix is

$$\begin{bmatrix} 1 & \xi & \xi^2 & \dots & \xi^{n-1} \\ 1 & \xi^2 & \xi^4 & \dots & \xi^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \xi^{n-k} & \xi^{2(n-k)} & \dots & \xi^{(n-1)(n-k)} \end{bmatrix}$$

  where $\xi \in R$ is a primitive nth root of unity such that $\overline{\xi} := \xi \bmod 2$ is a primitive nth root of unity in the residue field $R/2R$ of R, i.e., $\mathbb{F}_q$.
- Since n divides $q-1$, we take $n := q-1$ in which case $\overline{\xi}$ is a primitive element of $\mathbb{F}_q$.

- C is a MDS code over R (in the usual sense), i.e., its minimum distance is $n-k+1$.
- $\mathcal{RS}(\ell/2; n, k; R)$ will denote a q^ℓ-ary interleaved RS code comprising $\ell/2$ parallel copies of C.

4 The Decoding Problem & Its Solution

- Suppose a codeword $\mathbf{C}$ of $\mathcal{RS}(\ell/2; n, k; R)$ is transmitted and received as

$$\mathbf{R} = \mathbf{C} + \mathbf{E}.$$

- Let $\mathbf{E}_j := (\ e_j^{(1)}\ e_j^{(2)}\ \ldots\ e_j^{(\ell/2)}\ )^T$ be the jth column of $\mathbf{E}$, $\mathrm{Supp}(\mathbf{E}) := \{j : \mathbf{E}_j \neq \mathbf{0}\}$ and $t := |\mathrm{Supp}(\mathbf{E})|$.

  As in earlier works, we will assume that all (column) errors are equally likely.

- For $1 \leq l \leq \ell/2$, let $\mathbf{s}^{(l)}$ denote the lth syndrome, i.e.,

$$\mathbf{s}^{(l)} := s_0^{(l)}, s_{-1}^{(l)}, \ldots, s_{-n+k+1}^{(l)}$$

  where $s_i^{(l)} := \sum_{j \in \mathrm{Supp}(\mathbf{E})} e_j^{(l)} \xi^{-ji}$.

- Objective is to find a monic polynomial $\sigma := \sum_{j=0}^{t} \sigma_j X^j \in R[X]$ which simultaneously annihilates $\mathbf{s}^{(1)}, \mathbf{s}^{(2)}, \ldots, \mathbf{s}^{(\ell/2)}$, i.e., σ satisfies

$$\sum_{j=0}^{t-1} \sigma_j s_{i-j}^{(l)} = -s_{i-t}^{(l)} \ , \ \ -n+k+t+1 \leq i \leq 0, \ \ 1 \leq l \leq \ell/2. \tag{3}$$

- Straightforward to show that

$$\Gamma^{(l)} \equiv X\omega^{(l)}/\sigma \bmod X^{-n+k} \ , \ \ 1 \leq l \leq \ell/2$$

where

$$\begin{aligned} \Gamma^{(l)} &:= \sum_{j=-n+k+1}^{0} s_j^{(l)} X^j \\ \sigma &:= \prod_{j \in \mathrm{Supp}(\mathbf{E})} (X - \xi^j) \\ \omega^{(l)} &:= \sum_{j \in \mathrm{Supp}(\mathbf{E})} e_j^{(l)} \xi^j \prod_{i \in \mathrm{Supp}(\mathbf{E}), i \neq j} (X - \xi^i). \end{aligned}$$

- Due to the presence of zero divisors in R, the error locator polynomial actually has a slightly more general form.

  Theorem 4.1 *If* $z_j \in R$ *s.t.* $z_j \mathbf{E}_j = \mathbf{0}$ *for all* $j \in \mathrm{Supp}(\mathbf{E})$, *then* $\prod_{j \in \mathrm{Supp}(\mathbf{E})}(X - \xi^j - z_j) \in \mathrm{Ann}[\mathbf{s}]$.

  $\mathrm{Ann}[\mathbf{s}]$ is the set of monic polynomials in $R[X]$ of degree at most t which simultaneously annihilate $\mathbf{s}^{(1)}, \mathbf{s}^{(2)}, \ldots, \mathbf{s}^{(\ell/2)}$.

- Following paper gives an algorithm for finding $\mu \in \mathrm{Ann}[\mathbf{s}]$ of minimal degree.
  - M. A. Armand, "Multisequence shift register synthesis over commutative rings with identity with applications to decoding cyclic codes over integer residue rings," *IEEE Trans. Inf. Theory*, vol. 50, no. 1, pp. 220–229, Jan. 2004.

- Since $\deg \mu \leq \deg \sigma = t$, μ may not be an error locator polynomial. If it is, then by Theorem 4.1, we can find the (column) error locations over $\mathbb{F}_q$.

- Our analog to the MSRS decoding approach by Schmidt et. al., for $\mathcal{RS}(\ell/2; n, k; R)$.

Algorithm 4.2

i. Given $\mathbf{R}$*, compute* $\mathbf{s}^{(1)}, \mathbf{s}^{(2)}, \ldots, \mathbf{s}^{(\ell/2)}$.

ii. Compute $\mu \in \mathrm{Ann}[\mathbf{s}]$ *of minimal degree.*

iii. For $j = 0, 1, \ldots, n-1$*, if* $\overline{\mu}(\overline{\xi^j}) = 0$ *over* $\mathbb{F}_q$*, then* $\mathrm{Supp}(\widehat{\mathbf{E}}) \leftarrow j$ *where* $\overline{\mu} := \mu \bmod 2$.

iv. If $|\mathrm{Supp}(\widehat{\mathbf{E}})| = \deg \mu$*, then*

a) set $\sigma := \prod_{j \in \mathrm{Supp}(\widehat{\mathbf{E}})}(X - \xi^j)$ *and* $\omega^{(l)} := \sum_{i=1}^{\deg \sigma} \sum_{j=-i+1}^{0} \sigma_i s_j^{(l)} X^{i+j-1}$,

b) for $1 \leq l \leq \ell/2$*, set* $e_j^{(l)} := \omega^{(l)}(\xi^j)/(\xi^j \sigma'(\xi^j))$ *if* $j \in \mathrm{Supp}(\widehat{\mathbf{E}})$ *and* $e_j^{(l)} := 0$ *otherwise,*

c) output $\mathbf{R} - \widehat{\mathbf{E}}$*;*

else, declare decoding failure.

5 Decoding Radius

- Guaranteed decoding radius of Algorithm 4.2 is also

$$t_g = \lfloor (n-k)/2 \rfloor .$$

Not obvious and requires the following two results. Note that when at most t_g (column) errors have occurred, $\deg \sigma$ is $\leq t_g$ — a fact required in the hypothesis of both results.

Lemma 5.1 *Let* $f \in \mathrm{Ann}[\mathbf{s}]$ *with* $\deg f \leq t_g$. *Then* $f(\xi^j) e_j^{(l)} \xi^{2j} \sigma'(\xi^j) = 0$ *for* $j \in \mathrm{Supp}(\mathbf{E})$ *and* $1 \leq l \leq \ell/2$ *where* σ' *is the formal derivative of* σ.

Theorem 5.2 *Let* μ *be a polynomial of minimal degree in* $\mathrm{Ann}[\mathbf{s}]$ *such that* $\deg \mu \leq t_g$. *Then* $\overline{\mu} = \prod_{j \in \mathrm{Supp}(\mathbf{E})} (X - \overline{\xi^j})$ *where* $\overline{\mu} := \mu \bmod 2$.

Lemma 5.1 is needed to prove Theorem 5.2.

- By Theorem 5.2, if there are at most t_g errors, σ and the polynomial μ computed in step ii. of Algorithm 4.2, will always coincide modulo 2.

  Thus, Algorithm 4.2 will always decode correctly whenever $|\mathrm{Supp}(\mathbf{E})| \leq t_g$.

- Next, recall from Cramer's Rule that if $\mathbf{A} \in R^{N \times N}$ with $\det(\mathbf{A})$ a unit of R, then for any $\mathbf{B} \in R^{N \times 1}$,

$$\mathbf{AX} = \mathbf{B}$$

  has a unique solution $\mathbf{X} \in R^{N \times 1}$.

- Thus, if in the system of equations in (3), we equate the #Constraints, $(n-k-t)\ell/2$, to the #Unknowns, t, there is a possibility that the solution is unique.

  Rearranging $(n-k-t)\ell/2 = t$ yields

  $$t = \tau := \left\lfloor \frac{(\ell/2)}{(\ell/2)+1}(n-k) \right\rfloor .$$

  Algorithm 4.2 will be able to correct t errors where $t_g < t \leq \tau$, with certain probability.

- Observe that as $\ell \to \infty$,

  $$\tau/n \to 1 - \mathcal{R}$$

  where $\mathcal{R} = k/n$, i.e., the rate of the code. (Compare this to the fraction of correctable errors for classical decoding, $(1-\mathcal{R})/2$, and Guruswami-Sudan list decoding, $1-\sqrt{\mathcal{R}}$.)

- When will τ coincide with the maximum decoding radius t_m of the MSRS approach of Schmidt et. al.?

  Theorem 5.3 gives refined conditions for $\tau = t_m$.

  Theorem 5.3 *For* $\ell \leq \lfloor (n - 3 + \sqrt{n^2 - 6n + 1})/2 \rfloor$, $\tau = t_m$ *for certain code rates exceeding*

$$1 - \frac{\ell + 3 + (2/\ell)}{n} \, .$$

6 Decoding Error & Decoding Failure Probabilities

- The derivation of the upperbound on the probability of decoding error for the field case by Schmidt et. al., (i.e., (2)), is independent of the algebraic structure of the code alphabet.

  Thus, Algorithm 4.2's probability of decoding error, given that t errors have occurred, $t_g < t \leq \tau$, is

$$\leq \frac{\sum_{w=n-k+1}^{t+\tau} A_w \sum_{j=0}^{\min\{t,\tau\}} U(q^\ell, t, w, j)}{\binom{n}{t}(q^\ell - 1)^t} \tag{4}$$

  Clearly, (4) coincides with (2) when $\tau = t_m$.

  A_w can similarly be obtained by viewing $\mathcal{RS}(\ell/2; n, k; R)$ as a q^ℓ-ary MDS code and noting that the derivation of the weight distribution of an MDS code over $\mathbb{F}_{q^\ell}$ is based on combinatorial arguments independent of the algebraic structure of the code alphabet.

- An upperbound on Algorithm 4.2's probability of decoding failure is given by

Theorem 6.1 *An upper bound on the probability of decoding failure, given t errors have occurred, $t_g < t \leq \tau$, is*

$$\sum_{w=1}^{t}\sum_{i=0}^{w}\sum_{j=0}^{w-i}\frac{t!(q^{\ell/2}-1)^j(q^2-q)^i(q-1)^{w-i}}{(t-w)!(w-i-j)!i!j!(q^{\ell}-1)^w} \cdot \frac{q^{(3w-i-3j-2n+2k+2t-\min\{w-i-j,w-j-n+k+t\})\ell/2}}{(q^2-q)\mathcal{I}(i)+(q-1)(1-\mathcal{I}(i))}$$

where

$$\mathcal{I}(i) := \begin{cases} 1 \ : \ i > 0 \\ 0 \ : \ \textit{otherwise.} \end{cases}$$

7 Example #1

- Computed upperbounds on probability of decoding failure for $\mathcal{RS}(8; 255, 237; \mathrm{GR}(4, 8))$ and $\mathcal{RS}(16; 255, 237; \mathbb{F}_{256})$ using Theorem 6.1 and (1), respectively.

t	$\mathcal{RS}(8; 255, 237; \mathrm{GR}(4, 8))$	$\mathcal{RS}(16; 255, 237; \mathbb{F}_{256})$
10	3.536×10^{-133}	8.974×10^{-249}
11	1.670×10^{-111}	7.817×10^{-208}
12	7.885×10^{-90}	6.810×10^{-167}
13	3.724×10^{-68}	5.932×10^{-126}
14	1.758×10^{-46}	5.168×10^{-85}
15	8.304×10^{-25}	4.502×10^{-44}
16	3.937×10^{-3}	3.922×10^{-3}

- For these codes, $\tau = t_m = 16$. Therefore, the upperbounds on the probability of decoding error given by (2) and (4) are identical (and hence not shown).
- Observe that the probability of decoding failure is larger in the ring case for the various values of t considered other than $t = t_m$.

  On the other hand, decoding $\mathcal{RS}(8; 255, 237; \mathrm{GR}(4, 8))$ is more computationally intensive, primarily because an R-multiplication is more complex than an $\mathbb{F}_q$-multiplication.

  So, Galois ring interleaved codes have no advantage over their finite field counterparts, or do they?

8 Decoding When ℓ Is Large

- Recall the component code of $\mathcal{RS}(\ell/2; n, k; R)$, which is an $(n,\ k)$ RS code over R whose generator polynomial is $\prod_{i=1}^{n-k}(X - \xi^i)$.

  Its canonical image in $\mathbb{F}_q^n$ is an (n, k) RS code with generator polynomial $\prod_{i=1}^{n-k}(X - \overline{\xi^i})$.

- Consequently, suppose that with high probability, $\mathbf{E}$ does not contain any zero divisors of R so that

$$\mathrm{Supp}(\mathbf{E}) = \mathrm{Supp}(\overline{\mathbf{E}})$$

  where $\overline{\mathbf{E}} := \mathbf{E} \bmod 2$.

  Thus, to determine $\mathrm{Supp}(\mathbf{E})$, we can decode the canonical image $\mathcal{RS}(\ell/2; n, k; \mathbb{F}_q)$ of $\mathcal{RS}(\ell/2; n, k; R)$ in $\mathbb{F}_{q^{\ell/2}}^n$.

  The following modification of Algorithm 4.2 does just that.

Algorithm 8.1

i. Given $\mathbf{R}$*, compute the* $\ell/2$ *syndrome sequences.*

ii. Compute a monic polynomial $\mu \in \mathbb{F}_q[X]$ *of minimal degree that simultaneously annihilates* $\overline{\mathbf{s}^{(1)}}, \overline{\mathbf{s}^{(2)}}, \ldots, \overline{\mathbf{s}^{(\ell/2)}}$.

iii. For $j = 0, \ldots, n-1$*, if* $\mu(\overline{\xi^j}) = 0$*, then* $\mathrm{Supp}(\widehat{\overline{\mathbf{E}}}) \leftarrow j$.

iv. If $|\mathrm{Supp}(\widehat{\overline{\mathbf{E}}})| = \deg \mu$*, then*

a) set $\sigma := \prod_{j \in \mathrm{Supp}(\widehat{\overline{\mathbf{E}}})}(X - \xi^j)$ *and* $\omega^{(l)} := \sum_{i=1}^{\deg \sigma} \sum_{j=-i+1}^{0} \sigma_i s_j^{(l)} X^{i+j-1}$,

b) for $1 \le l \le \ell/2$*, set* $e_j^{(l)} := \omega^{(l)}(\xi^j)/(\xi^j \sigma'(\xi^j))$ *if* $j \in \mathrm{Supp}(\widehat{\overline{\mathbf{E}}})$ *and* $e_j^{(l)} := 0$ *otherwise,*

c) output $\mathbf{R} - \widehat{\mathbf{E}}$*;*

else, declare decoding failure.

- Key modification is in step ii. where the objective is to compute a monic polynomial in $\mathbb{F}_q[X]$ of minimal degree that simultaneously annihilates (over $\mathbb{F}_q$), $\overline{\mathbf{s}^{(1)}}, \overline{\mathbf{s}^{(2)}}, \ldots, \overline{\mathbf{s}^{(\ell/2)}}$ where $\overline{\mathbf{s}^{(l)}} := \mathbf{s}^{(l)} \bmod 2$.

- Algorithm 8.1 has no guaranteed decoding radius, since it will not decode correctly if at least one of the (column) errors does not contain any units of R.

  Since all errors are assumed to be equally likely, the probability that an error does not contain any units of R, is

$$p_{\mathcal{K}} := \frac{\sum_{l=1}^{\ell/2} \binom{\ell/2}{l} (q-1)^l}{\sum_{l=1}^{\ell/2} \binom{\ell/2}{l} (q^2-1)^l} .$$

- Clearly, $p_{\mathcal{K}}$ decreases as ℓ increases, for a given q.

  Therefore, it only makes sense to use Algorithm 8.1 when ℓ is large.

9 Word Error Rates Under Modified Decoding Strategy

- Given t (column) errors, $t_g < t \leq \tau$, all of which not containing any zero divisors of R, probability of decoding failure is

$$\leq \overline{\mathbb{P}_f}(t) := \left(\frac{q^{\ell/2} - (1/q)}{q^{\ell/2} - 1}\right)^t \frac{q^{-((\ell/2)+1)(\tau-t)}}{q-1}$$

and probability of decoding error is

$$\leq \overline{\mathbb{P}_e}(t) := \frac{\sum_{w=n-k+1}^{t+\tau} A_w \sum_{j=0}^{\min\{t,\tau\}} U(q^{\ell/2}, t, w, j)}{\binom{n}{t}(q^{\ell/2}-1)^t}$$

where A_w is the number of codewords of weight w of a $q^{\ell/2}$-ary (n,k) MDS code, and

$$U(q^{\ell/2}, t, w, j) := \sum_{i=\lceil\frac{t+w-j}{2}\rceil}^{t+w-j} \binom{w}{i}\binom{i}{j-t-w+2i}\binom{n-w}{t-i} \cdot (q^{\ell/2}-2)^{j-t-w+2i}(q^{\ell/2}-1)^{t-i}.$$

- Given t errors have occurred, probability that at least one of the errors does not contain any units of R, is $P_{\mathcal{K}}(t) := \sum_{i=1}^{t} \binom{t}{i} (1-p_{\mathcal{K}})^{t-i} p_{\mathcal{K}}^{i}$.

  With that, the (overall) word error probability of Algorithm 8.1 is

$$\leq \overline{\mathcal{P}_w} := \sum_{t=1}^{n} \overline{\mathcal{P}_w}(t) \cdot \rho(t) \tag{5}$$

  where

$$\overline{\mathcal{P}_w}(t) := \begin{cases} P_{\mathcal{K}}(t) & : \ t \leq t_g \\ \min\left\{\left(\overline{\mathbb{P}_e}(t) + \overline{\mathbb{P}_f}(t)\right)(1-P_{\mathcal{K}}(t)) + P_{\mathcal{K}}(t),\ 1\right\} & : \ t_g < t \leq \tau \\ 1 & : \ t > \tau \end{cases}$$

  upperbounds the probability of word error given that t errors have occurred, and

$$\rho(t) := \binom{n}{t} (1-p)^{n-t} p^{t}$$

  is the probability of t errors occurring, where p is the probability of an error occurring.

10 Example #2

- Using (5), we computed upperbounds on the word error probability of Algorithm 8.1 when used to decode $\mathcal{RS}(36; 255, 235; \mathrm{GR}(4, 8))$ for $p = 10^{-4}, 10^{-5}, 10^{-6}, 10^{-7}$.

  We also computed the corresponding upperbounds on the word error probability of the MSRS approach of Schmidt et. al. when used to decode $\mathcal{RS}(72; 255, 235; \mathbb{F}_{256})$.

p	$\mathcal{RS}(36; 255, 235; \mathrm{GR}(4, 8))$	$\mathcal{RS}(72; 255, 235; \mathbb{F}_{256})$
10^{-4}	1.092×10^{-50}	1.092×10^{-50}
10^{-5}	8.830×10^{-70}	8.830×10^{-70}
10^{-6}	8.667×10^{-89}	8.616×10^{-89}
10^{-7}	5.127×10^{-92}	8.594×10^{-108}

  Evidently, we have comparable word error rate performance for $p = 10^{-4}, 10^{-5}, 10^{-6}$.

11 Decoding Complexity

- Compare the computational cost of decoding $\mathcal{RS}(\ell/2; n, k; R)$ and $\mathcal{RS}(\ell; n, k; \mathbb{F}_q)$ using their respective collaborative decoders in terms of the number of multiplications needed.

  As there are R-multiplications and $\mathbb{F}_q$-multiplications involved, we count one R-multiplication as two $\mathbb{F}_q$-multiplications.

- The rationale follows from the fact that the critical path length (i.e., the longest path a signal has to travel during one clock cycle) of a standard-shift-register (SSR) serial R-multiplier need only be twice as long as that of a SSR serial $\mathbb{F}_q$-multiplier.

  – B. Abrahamsson, "Architectures for multiplication in Galois rings," Undergraduate thesis, Linköping University, Dept. of Electrical Engineering, Jun. 2004. Available online at http://www.ep.liu.se.

- This means that the clock frequency for the $\mathbb{F}_q$-multiplier can be twice as fast as that for the R-multiplier.

  With each multiplier needing m clock cycles to perform the calculations, the R-multiplier will therefore take twice as long as the $\mathbb{F}_q$-multiplier to produce a result.

- Straightforward counting procedure shows that Algorithm 8.1 requires at most

$$\ell(n-1)(n-k) + (\ell/2)(n-k)^2 + n(\tau-1) + ((\ell/2)+1)(\tau-1)\tau + 2\ell\tau^2$$

  $\mathbb{F}_q$-multiplications, while the MSRS approach by Schmidt et. al. requires at most

$$\ell(n-1)(n-k) + \ell(n-k)^2 + n(t_m-1) + (\ell/2)(t_m-1)t_m + 2\ell t_m^2$$

  $\mathbb{F}_q$-multiplications.

- Decoding $\mathcal{RS}(36; 255, 235; \mathrm{GR}(4, 8))$ and $\mathcal{RS}(72; 255, 235; \mathbb{F}_{256})$ require at most 449388 and 463446 $\mathbb{F}_{256}$-multiplications, respectively.

  Translates to a computational saving of 3.03% at the decoder if one chooses to use the former code instead of the latter.

- In general, given n, one can expect increasing computational savings as ℓ increases (resp., code rate decreases), while code rate (resp., ℓ) remains fixed.

12 Summary

- We have studied the merits of MSRS-based collaborative decoding of interleaved codes formed from RS codes over Galois rings, in terms of key performance indicators such as the decoding error and decoding failure probabilities.
- We have shown that when ℓ is large, a q^ℓ-ary interleaved code formed from $\ell/2$ parallel copies of an (n, k) RS code over R, can be as good as its field counterpart, formed from ℓ parallel copies of an (n, k) RS code over $\mathbb{F}_q$, in terms of the word error probabilities of their respective collaborative decoders, while incurring lower decoding complexity.