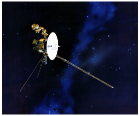
Reed–Solomon Codes over Fields of Characteristic Zero

Carmen Sippel, Cornelia Ott, Sven Puchinger, Martin Bossert

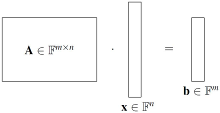
ISIT 2019, Paris

July 10, 2019

Motivation



We know Reed–Solomon Codes over



$$\mathbb{F}_q$$

$$\mathbb{C}$$

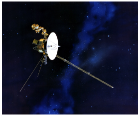
- Elements are represented with a fixed number of bits
- Operations cost a constant number of bit operations

- Floating point operations are used
- Problem: Rounding errors

Aim

Reed–Solomon Codes over arbitrary fields with exact calculations during Encoding and Decoding.

Motivation



We know Reed–Solomon Codes over

$$\mathbf{A} \in \mathbb{F}^{m \times n} \cdot \mathbf{x} \in \mathbb{F}^{n} = \mathbf{b} \in \mathbb{F}^{m}$$

$\mathbb{F}_q$

- Elements are represented with a fixed number of bits
- Operations cost a constant number of bit operations

$\mathbb{C}$

- Floating point operations are used
- Problem: Rounding errors

Aim

Reed–Solomon Codes over arbitrary fields with exact calculations during Encoding and Decoding.

GRS Codes over arbitrary Fields

Definition: Generalization of Definition 5.1.1 in [Rot06]

Let K be a field and k, $n \in \mathbb{N}$ such that $k \leq n$. Choose $\alpha_1, \ldots, \alpha_n \in K\backslash\{0\}$ to be distinct and $v_1, \ldots, v_n \in K \setminus \{0\}$. We define the *generalized Reed–Solomon Code* $\mathcal{C}_{\mathrm{GRS}} \subseteq K^n$ with parity check matrix

$$\boldsymbol{H}_{\text{Vandermonde}} = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \vdots & \vdots & \ldots & \vdots \\ \alpha_1^{n-k-1} & \alpha_2^{n-k-1} & \ldots & \alpha_n^{n-k-1} \end{pmatrix} \begin{pmatrix} v_1 & & & \\ & v_2 & & \\ & & \ddots & \\ & & & v_n \end{pmatrix}.$$

GRS Codes over arbitrary Fields

Generator Matrix

A generator matrix is of the form

$$\boldsymbol{G}_{\text{Vandermonde}} = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \vdots & \vdots & \dots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \dots & \alpha_n^{k-1} \end{pmatrix} \begin{pmatrix} v'_1 & & & \\ & v'_2 & & \\ & & \ddots & \\ & & & v'_n \end{pmatrix},$$

where the $v'_i \in K \setminus \{0\}$, given by the following linear system of equations:

$$\sum_{i=1}^{n} \alpha_i^r v_i v'_i = 0 \quad \forall\, r = 0, \dots, n-2\,.$$

Coefficient Growth

over Fields of Characteristic Zero

If the underlying field is of characteristic zero the coefficients during Encoding and Decoding will grow.

Example: Euclidean Algorithm

$$f_0, f_1 \in \mathbb{F}_{1789}[x] \qquad\qquad g_0, g_1 \in \mathbb{Q}[t]$$

$$f_0(x) = x^{10} - 3 \qquad\qquad g_0(t) = t^{10} - 3$$
$$f_1(x) = 3x^9 - 2 \qquad\qquad g_1(t) = 3t^9 - 2$$

Coefficient Growth

over Fields of Characteristic Zero

Example: Euclidean Algorithm - Step 1

$$(x^{10} - 3)/(3x^9 - 2)$$
$$= 1193x$$

Remainder: $597x + 1786$

$$(t^{10} - 3)/(3t^9 - 2)$$
$$= \frac{1}{3}t$$

Remainder: $\frac{2}{3}t - 3$

Coefficient Growth

over Fields of Characteristic Zero

Example: Euclidean Algorithm - Step 2

$$(3x^9 - 2)/(597x + 1786)$$
$$= 899x^8 + 1362x^7 + 762x^6$$
$$+ 1640x^5 + 224x^4 + 1008x^3$$
$$+ 958x^2 + 733x + 615$$

Remainder: 54

$$(3t^9 - 2)/(\frac{2}{3}t - 3)$$
$$= \frac{9}{2}t^8 + \frac{81}{4}t^7 + \frac{729}{8}t^6 + \frac{6561}{16}t^5$$
$$+ \frac{59049}{32}t^4 + \frac{531441}{64}t^3$$
$$+ \frac{4782969}{128}t^2 + \frac{43046721}{256}t$$
$$+ \frac{387420489}{512}$$

Remainder: $\frac{1162260443}{512}$

Coefficient Growth

over Fields of Characteristic Zero

Example: Euclidean Algorithm - Step 3

$$(597x + 1786)/54$$
$$= 508x + 1292$$

Remainder: 0

$$(\frac{2}{3}t - 3)/\frac{1162260443}{512}$$
$$= \frac{1024}{3486781329}t - \frac{1536}{1162260443}$$

Remainder: 0

Question:

Is it possible to derive bounds for the growth of the coefficients during Encoding and Decoding?

$\rightarrow$ Solution with the help of already known results from computer algebra.

Coefficient Growth

over Fields of Characteristic Zero

Example: Euclidean Algorithm - Step 3

$$(597x + 1786)/54$$
$$= 508x + 1292$$

Remainder: 0

$$(\frac{2}{3}t - 3)/\frac{1162260443}{512}$$
$$= \frac{1024}{3486781329}t - \frac{1536}{1162260443}$$

Remainder: 0

Question:

Is it possible to derive bounds for the growth of the coefficients during Encoding and Decoding?

$\rightarrow$ Solution with the help of already known results from computer algebra.

Coefficient Growth

over Fields of Characteristic Zero

Example: Euclidean Algorithm - Step 3

$$(597x + 1786)/54$$
$$= 508x + 1292$$

Remainder: 0

$$(\frac{2}{3}t - 3)/\frac{1162260443}{512}$$
$$= \frac{1024}{3486781329}t - \frac{1536}{1162260443}$$

Remainder: 0

Question:

Is it possible to derive bounds for the growth of the coefficients during Encoding and Decoding?

$\rightarrow$ Solution with the help of already known results from computer algebra.

The bit width - a Measure of Coefficient Growth

We define the *bit width* $\lambda(a)$: (Generalization of [vzGG13] p. 142)

- $a \in \mathbb{Z}$:

$$\lambda(a) := \begin{cases} \lfloor \log_2(|a|) \rfloor + 1, & \text{if } a \neq 0 \\ 0, & \text{if } a = 0 \end{cases}$$

- $a = \frac{b}{c} \in \mathbb{Q}$ with $b, c \in \mathbb{Z}$, $c \neq 0$, and $\gcd(b,c) = 1$:

$$\lambda(a) := \max\{\lambda(b), \lambda(c)\}.$$

- $a(x) = \sum_{i=0}^{r} \frac{a_i}{b} \cdot x^i \in \mathbb{Q}[x]$ with $a_i \in \mathbb{Z}$ and $b \in \mathbb{N} \setminus \{0\}$ such that $\gcd(a_0, \ldots, a_r, b) = 1$:

$$\lambda(a(x)) := \max\{\lambda(a_0), \ldots, \lambda(a_r), \lambda(b)\}.$$

- NEW: $\boldsymbol{A} = (a_{ij}) \in \mathbb{Q}^{k \times r}$:

$$\lambda(\boldsymbol{A}) = \max\{\lambda(a_{ij}) \,:\, i = 1, \ldots, k \text{ and } j = 1, \ldots, r\}.$$

The bit width - a Measure of Coefficient Growth

We define the *bit width* $\lambda(a)$: (Generalization of [vzGG13] p. 142)

- $a \in \mathbb{Z}$:

$$\lambda(a) := \begin{cases} \lfloor \log_2(|a|) \rfloor + 1, & \text{if } a \neq 0 \\ 0, & \text{if } a = 0 \end{cases}$$

- $a = \frac{b}{c} \in \mathbb{Q}$ with $b, c \in \mathbb{Z}$, $c \neq 0$, and $\gcd(b, c) = 1$:

$$\lambda(a) := \max\{\lambda(b), \lambda(c)\}.$$

- $a(x) = \sum_{i=0}^{r} \frac{a_i}{b} \cdot x^i \in \mathbb{Q}[x]$ with $a_i \in \mathbb{Z}$ and $b \in \mathbb{N} \setminus \{0\}$ such that $\gcd(a_0, \ldots, a_r, b) = 1$:

$$\lambda(a(x)) := \max\{\lambda(a_0), \ldots, \lambda(a_r), \lambda(b)\}.$$

- NEW: $\boldsymbol{A} = (a_{ij}) \in \mathbb{Q}^{k \times r}$:

$$\lambda(\boldsymbol{A}) = \max\{\lambda(a_{ij}) \; : \; i = 1, \ldots, k \text{ and } j = 1, \ldots, r\}.$$

The bit width - a Measure of Coefficient Growth

We define the *bit width* $\lambda(a)$: (Generalization of [vzGG13] p. 142)

- $a \in \mathbb{Z}$:
$$\lambda(a) := \begin{cases} \lfloor \log_2(|a|) \rfloor + 1, & \text{if } a \neq 0 \\ 0, & \text{if } a = 0 \end{cases}$$
- $a = \frac{b}{c} \in \mathbb{Q}$ with $b, c \in \mathbb{Z}$, $c \neq 0$, and $\gcd(b, c) = 1$:
$$\lambda(a) := \max\{\lambda(b), \lambda(c)\}.$$
- $a(x) = \sum_{i=0}^{r} \frac{a_i}{b} \cdot x^i \in \mathbb{Q}[x]$ with $a_i \in \mathbb{Z}$ and $b \in \mathbb{N} \setminus \{0\}$ such that $\gcd(a_0, \ldots, a_r, b) = 1$:
$$\lambda(a(x)) := \max\{\lambda(a_0), \ldots, \lambda(a_r), \lambda(b)\}.$$
- NEW: $\boldsymbol{A} = (a_{ij}) \in \mathbb{Q}^{k \times r}$:
$$\lambda(\boldsymbol{A}) = \max\{\lambda(a_{ij}) \ : \ i = 1, \ldots, k \text{ and } j = 1, \ldots, r\}.$$

The bit width - a Measure of Coefficient Growth

We define the *bit width* $\lambda(a)$: (Generalization of [vzGG13] p. 142)

- $a \in \mathbb{Z}$:

$$\lambda(a) := \begin{cases} \lfloor \log_2(|a|) \rfloor + 1, & \text{if } a \neq 0 \\ 0, & \text{if } a = 0 \end{cases}$$

- $a = \frac{b}{c} \in \mathbb{Q}$ with $b, c \in \mathbb{Z}$, $c \neq 0$, and $\gcd(b, c) = 1$:

$$\lambda(a) := \max\{\lambda(b), \lambda(c)\}.$$

- $a(x) = \sum_{i=0}^{r} \frac{a_i}{b} \cdot x^i \in \mathbb{Q}[x]$ with $a_i \in \mathbb{Z}$ and $b \in \mathbb{N} \setminus \{0\}$ such that $\gcd(a_0, \ldots, a_r, b) = 1$:

$$\lambda(a(x)) := \max\{\lambda(a_0), \ldots, \lambda(a_r), \lambda(b)\}.$$

- NEW: $\boldsymbol{A} = (a_{ij}) \in \mathbb{Q}^{k \times r}$:

$$\lambda(\boldsymbol{A}) = \max\{\lambda(a_{ij}) \; : \; i = 1, \ldots, k \text{ and } j = 1, \ldots, r\}.$$

The bit width - a Measure of Coefficient Growth

Examples

(i) $\lambda(127) = \lfloor \log_2(|127|) \rfloor + 1 = 7$

(ii) $\lambda(\frac{3}{64}) = \max\{ \underbrace{\lambda(3)}_{\lfloor \log_2(|3|) \rfloor + 1}, \underbrace{\lambda(64)}_{\lfloor \log_2(|64|) \rfloor + 1} \} = \max\{1, 7\} = 7$

(iii)
$$\begin{aligned} \lambda(2x^3 + \tfrac{2}{5}x^2 + \tfrac{1}{8}) &= \lambda(\tfrac{80x^3+16x^2+5}{40}) \\ &= \max\{\lambda(80), \lambda(16), \lambda(5), \lambda(40)\} \\ &= \lambda(80) = \lfloor \log_2(|80|) \rfloor + 1 = 7 \end{aligned}$$

The bit width - a Measure of Coefficient Growth

Examples

(i) $\lambda(127) = \lfloor \log_2(|127|) \rfloor + 1 = 7$

(ii) $\lambda(\frac{3}{64}) = \max\{ \underbrace{\lambda(3)}_{\lfloor \log_2(|3|) \rfloor + 1}, \underbrace{\lambda(64)}_{\lfloor \log_2(|64|) \rfloor + 1} \} = \max\{1, 7\} = 7$

(iii) $\lambda(2x^3 + \frac{2}{5}x^2 + \frac{1}{8}) = \lambda(\frac{80x^3+16x^2+5}{40})$

$= \max\{\lambda(80), \lambda(16), \lambda(5), \lambda(40)\}$

$= \lambda(80) = \lfloor \log_2(|80|) \rfloor + 1 = 7$

The bit width - a Measure of Coefficient Growth

Examples

(i) $\lambda(127) = \lfloor \log_2(|127|) \rfloor + 1 = 7$

(ii) $\lambda(\frac{3}{64}) = \max\{ \underbrace{\lambda(3)}_{\lfloor \log_2(|3|) \rfloor + 1}, \underbrace{\lambda(64)}_{\lfloor \log_2(|64|) \rfloor + 1} \} = \max\{1, 7\} = 7$

(iii)
$$\begin{aligned} \lambda(2x^3 + \tfrac{2}{5}x^2 + \tfrac{1}{8}) &= \lambda(\tfrac{80x^3+16x^2+5}{40}) \\ &= \max\{\lambda(80), \lambda(16), \lambda(5), \lambda(40)\} \\ &= \lambda(80) = \lfloor \log_2(|80|) \rfloor + 1 = 7 \end{aligned}$$

Coefficient Growth in Encoding

over the Rational Numbers

Bound for the bit width of the codeword

Let $\boldsymbol{c}$ be an RS codeword generated by encoding $\boldsymbol{u} \in \mathbb{Q}^k$ with generator matrix $\boldsymbol{G} \in \mathbb{Q}^{k \times n}$. Then

$$\lambda(\boldsymbol{c}) \leq k(\lambda(\boldsymbol{u}) + \lambda(\boldsymbol{G}) + 1).$$

Generator Matrix in systematic form [RS85, Theorem 1]

$\mathcal{C}_{\mathrm{GRS}}$ has a systematic generator matrix of the form $\boldsymbol{G}_{\mathsf{sys}} = (\boldsymbol{I}_{k \times k} \mid \boldsymbol{A})$, where $\boldsymbol{A} = \left(\frac{c_i d_j}{a_i - b_j}\right)$ is a Cauchy matrix with a_i, b_j, c_i, d_j dependent on α_i and $v_i' \quad \forall i = 1, \ldots, k, \quad j = 1, \ldots, n-k.$

Coefficient Growth in Encoding

over the Rational Numbers

Bound for the bit width of the codeword

Let $\boldsymbol{c}$ be an RS codeword generated by encoding $\boldsymbol{u} \in \mathbb{Q}^k$ with generator matrix $\boldsymbol{G} \in \mathbb{Q}^{k \times n}$. Then

$$\lambda(\boldsymbol{c}) \leq k(\lambda(\boldsymbol{u}) + \lambda(\boldsymbol{G}) + 1).$$

Generator Matrix in systematic form [RS85, Theorem 1]

$\mathcal{C}_{\mathrm{GRS}}$ has a systematic generator matrix of the form
$\boldsymbol{G}_{\mathsf{sys}} = (\boldsymbol{I}_{k \times k} \mid \boldsymbol{A})$, where $\boldsymbol{A} = \left(\frac{c_i d_j}{a_i - b_j}\right)$ is a Cauchy matrix with a_i, b_j, c_i, d_j dependent on α_i and
$v_i' \quad \forall i = 1, \ldots, k, \quad j = 1, \ldots, n-k.$

Coefficient Growth in Encoding

over the Rational Numbers

Bound for the bit width of the codeword

Let $\boldsymbol{c}$ be an RS codeword generated by encoding $\boldsymbol{u} \in \mathbb{Q}^k$ with generator matrix $\boldsymbol{G} \in \mathbb{Q}^{k \times n}$. Then

$$\lambda(\boldsymbol{c}) \leq k(\lambda(\boldsymbol{u}) + \lambda(\boldsymbol{G}) + 1).$$

Generator Matrix in systematic form [RS85, Theorem 1]

$\mathcal{C}_{\mathrm{GRS}}$ has a systematic generator matrix of the form
$\boldsymbol{G}_{\mathsf{sys}} = (\boldsymbol{I}_{k \times k} \mid \boldsymbol{A})$, where $\boldsymbol{A} = \left(\frac{c_i d_j}{a_i - b_j}\right)$ is a Cauchy matrix with
a_i, b_j, c_i, d_j dependent on α_i and
$v_i' \quad \forall i = 1, \ldots, k, \quad j = 1, \ldots, n-k.$
$\rightarrow \lambda(\boldsymbol{G})$ small

Coefficient Growth in Encoding

over the Rational Numbers

Bound for the bit width of the codeword

Let $\boldsymbol{c}$ be an RS codeword generated by encoding $\boldsymbol{u} \in \mathbb{Q}^k$ with generator matrix $\boldsymbol{G} \in \mathbb{Q}^{k \times n}$. Then

$$\lambda(\boldsymbol{c}) \leq k(\lambda(\boldsymbol{u}) + \lambda(\boldsymbol{G}) + 1).$$

Generator Matrix in systematic form [RS85, Theorem 1]

$\mathcal{C}_{\mathrm{GRS}}$ has a systematic generator matrix of the form $\boldsymbol{G}_{\mathsf{sys}} = (\boldsymbol{I}_{k \times k} \mid \boldsymbol{A})$, where $\boldsymbol{A} = \left(\frac{c_i d_j}{a_i - b_j}\right)$ is a Cauchy matrix with a_i, b_j, c_i, d_j dependent on α_i and $v_i' \quad \forall i = 1, \ldots, k, \quad j = 1, \ldots, n-k.$

$\rightarrow \lambda(\boldsymbol{G})$ small

Coefficient Growth in Encoding

over the Rational Numbers

Comparison of systematic and non-systematic Encoding

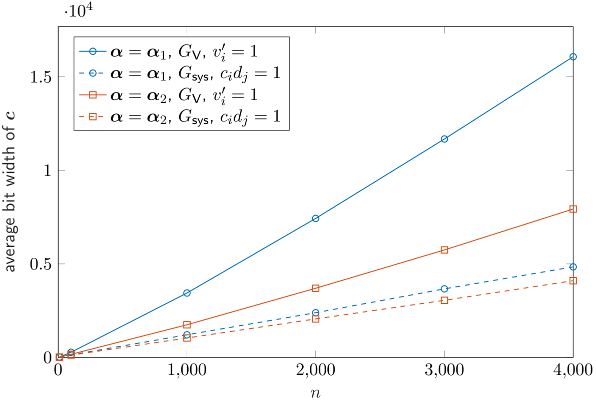
For a special choice of $\boldsymbol{v}'$ we get $\lambda(\boldsymbol{G}_{\mathsf{sys}}) < \lambda(\boldsymbol{G}_{\mathsf{Vandermonde}})$

Upper Bounds for the bit width of the Generatormatix

	$\lambda(\boldsymbol{G}_{\mathsf{Vandermonde}})$	$\lambda(\boldsymbol{G}_{\mathsf{sys}})$
general	$(k-1)\lambda(\boldsymbol{\alpha}) + \lambda(\boldsymbol{v}')$	$2(2k-1)\lambda(\boldsymbol{\alpha}) + 2\lambda(\boldsymbol{v}') + 2k - 1$
$c_i d_j = 1$	$(k-1)(3\lambda(\boldsymbol{\alpha}) + 1)$	$2\lambda(\boldsymbol{\alpha}) + 1$

Coefficient Growth in Encoding

over the Rational Numbers



$\boldsymbol{\alpha}_1 := (1, 2, \dots, n)$
$\boldsymbol{\alpha}_2 := (-1, 1, -\frac{1}{2}, \frac{1}{2}, -2, 2, \frac{1}{3}, -\frac{1}{3}, \frac{2}{3}, \dots)$

We chose 1000 information words of bit width 100.

Rate: $k = \lfloor n/3 \rfloor$.

	$\lambda(\boldsymbol{G}_{\mathsf{Vandermonde}})$	$\lambda(\boldsymbol{G}_{\mathsf{sys}})$
general	$(k-1)\lambda(\boldsymbol{\alpha}) + \lambda(\boldsymbol{v}')$	$2(2k-1)\lambda(\boldsymbol{\alpha}) + 2\lambda(\boldsymbol{v}') + 2k - 1$
$c_i d_j = 1$	$(k-1)(3\lambda(\boldsymbol{\alpha}) + 1)$	$2\lambda(\boldsymbol{\alpha}) + 1$

Coefficient Growth in Decoding

over the Rational Numbers (Generalization of [Rot06] Chapter 6)

Algorithm 1: Decoding Algorithm for GRS Codes over $\mathbb{Q}$

Input: Received Word $\boldsymbol{r} = \boldsymbol{c} + \boldsymbol{e}$, where $\boldsymbol{c} \in \mathcal{C}_{\mathrm{GRS}}$ and $\mathrm{wt}_{\mathrm{H}}(\boldsymbol{e}) \leq \lfloor \frac{n-k}{2} \rfloor$.

Output: Codeword $\boldsymbol{c}$

$\boldsymbol{s} \leftarrow \boldsymbol{r}\boldsymbol{H}^{\top}_{\text{Vandermonde}}$

$S(x) \leftarrow \sum_{i=0}^{d-2} s_i x^i$

$\xi \leftarrow \mathrm{lcm}(\mathrm{den}(s_0), \ldots, \mathrm{den}(s_{d-2}))$

$(r_h, s_h, t_h) \leftarrow \mathrm{EEA}(\xi \cdot x^{d-1}, \xi \cdot S(x), \frac{d-1}{2})$ `// implementation of [vzGG13, Algorithm 6.57]`

$c \leftarrow 0^{\text{th}}$ coefficient of t_h

$(\Lambda(x), \Omega(x)) \leftarrow c^{-1} \cdot (t_h, \frac{r_h}{\xi})$

$\Lambda'(x) \leftarrow \sum_{i>0} i \Lambda_i x^{i-1}$

$e_i \leftarrow -\frac{\alpha_i}{v_i} \frac{\Omega(\alpha_i^{-1})}{\Lambda'(\alpha_i^{-1})}$ for $i = 1, \ldots, n$

return $\boldsymbol{c} = \boldsymbol{r} - \boldsymbol{e}$

Coefficient Growth in Decoding

over the Rational Numbers

Bit width of the Syndrome

Let $\boldsymbol{r} = \boldsymbol{c} + \boldsymbol{e}$ be a received word, $\boldsymbol{s} = \boldsymbol{r}\boldsymbol{H}_{\mathsf{Vandermonde}}^{\top}$ the syndrome and $\tau = \mathrm{wt_H}(\boldsymbol{e})$. For the bit width of $\boldsymbol{s}$ we get the following bound:

$$\lambda(\boldsymbol{s}) \leq \tau(\lambda(\boldsymbol{e}) + \lambda(\boldsymbol{H}_{\mathsf{Vandermonde}}) + 1).$$

Coefficient Growth in Decoding

over the Rational Numbers

Complexity of the Algorithm

- The complexity in bit operations is

$$O^{\sim}\Big(d^7\left[\lambda(\boldsymbol{e})+\lambda(\boldsymbol{H}_{\mathrm{GRS}})\right]^2+n^4[\lambda(\boldsymbol{c})+\lambda(\boldsymbol{e})+\lambda(\boldsymbol{H}_{\mathrm{GRS}})]\Big).$$

- If the error $\boldsymbol{e}$ has bit width at most t, codeword $\boldsymbol{c}$ at most t' and $\boldsymbol{\alpha}$ is chosen choosen such that $\lambda(\boldsymbol{\alpha}) \in O(\log(n))$ (e.g., $\boldsymbol{\alpha}_1$ or $\boldsymbol{\alpha}_2$) then Algorithm 1 can be implemented in

$$O^{\sim}(\max\{n^7t^2, n^9, n^4t'\})$$

bit operations.

Coefficient Growth in Decoding

over the Rational Numbers

Complexity of the Algorithm

- The complexity in bit operations is

$$O^{\sim}\Big(d^7\left[\lambda(\boldsymbol{e})+\lambda(\boldsymbol{H}_{\mathrm{GRS}})\right]^2+n^4[\lambda(\boldsymbol{c})+\lambda(\boldsymbol{e})+\lambda(\boldsymbol{H}_{\mathrm{GRS}})]\Big).$$

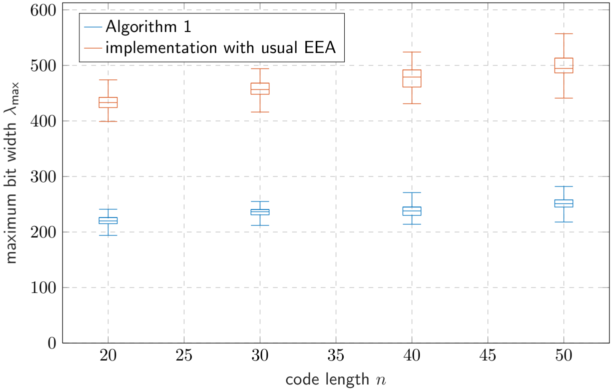
- If the error $\boldsymbol{e}$ has bit width at most t, codeword $\boldsymbol{c}$ at most t' and $\boldsymbol{\alpha}$ is chosen choosen such that $\lambda(\boldsymbol{\alpha}) \in O(\log(n))$ (e.g., $\boldsymbol{\alpha}_1$ or $\boldsymbol{\alpha}_2$) then Algorithm 1 can be implemented in

$$O^{\sim}\left(\max\{n^7t^2, n^9, n^4t'\}\right)$$

bit operations.

Coefficient Growth in Decoding

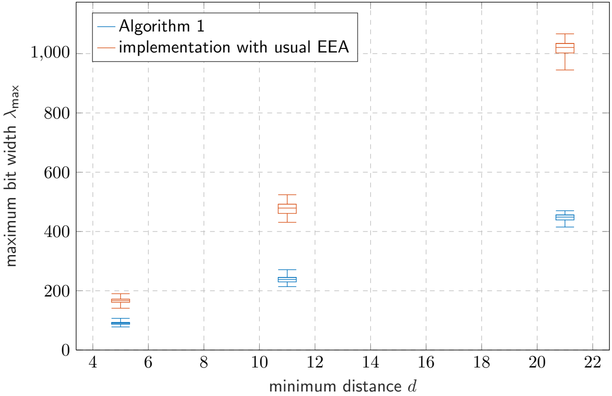
Comparison of the maximum bit width $\lambda_{\max}$ for Decoding using different Variants of the EEA



We chose $\lambda(\boldsymbol{e}) = 40$, $d = 11$
For each point 100 simulations were carried out

Coefficient Growth in Decoding

Comparison of the maximum bit width $\lambda_{\max}$ for Decoding using different Variants of the EEA



We chose $\lambda(\boldsymbol{e}) = 40$ and $n = 40$
For each point 100 simulations were carried out

Conclusion

- Properties of Reed–Solomon Codes over $\mathbb{F}_q$ also hold over arbitrary fields
- Over $\mathbb{Q}$ there exist bounds for the coefficient growth during encoding
- Over $\mathbb{Q}$ decoding up to half-the-minimum distance is possible in a polynomial number of bit operations

Conclusion

- Properties of Reed–Solomon Codes over $\mathbb{F}_q$ also hold over arbitrary fields
- Over $\mathbb{Q}$ there exist bounds for the coefficient growth during encoding
- Over $\mathbb{Q}$ decoding up to half-the-minimum distance is possible in a polynomial number of bit operations

Conclusion

- Properties of Reed–Solomon Codes over $\mathbb{F}_q$ also hold over arbitrary fields
- Over $\mathbb{Q}$ there exist bounds for the coefficient growth during encoding
- Over $\mathbb{Q}$ decoding up to half-the-minimum distance is possible in a polynomial number of bit operations

Future Work

- Extension of the results to more classes of number fields, for instance $\mathbb{Q}[\mathrm{i}]$.
- Consider other decoding algorithms, e.g. Berlekamp-Welch, Berlekamp-Massey or list decoding approaches
- Reduction of the computation modulo a prime by decomposing the number field into prime ideals such as in [ALR17]
- Determine the bit complexity of Decoding algorithms for Gabidulin codes over characteristic zero with the same methods.

Future Work

- Extension of the results to more classes of number fields, for instance $\mathbb{Q}[\mathrm{i}]$.
- Consider other decoding algorithms, e.g. Berlekamp-Welch, Berlekamp-Massey or list decoding approaches
- Reduction of the computation modulo a prime by decomposing the number field into prime ideals such as in [ALR17]
- Determine the bit complexity of Decoding algorithms for Gabidulin codes over characteristic zero with the same methods.

Future Work

- Extension of the results to more classes of number fields, for instance $\mathbb{Q}[\mathrm{i}]$.
- Consider other decoding algorithms, e.g. Berlekamp-Welch, Berlekamp-Massey or list decoding approaches
- Reduction of the computation modulo a prime by decomposing the number field into prime ideals such as in [ALR17]
- Determine the bit complexity of Decoding algorithms for Gabidulin codes over characteristic zero with the same methods.

Future Work

- Extension of the results to more classes of number fields, for instance $\mathbb{Q}[\mathrm{i}]$.
- Consider other decoding algorithms, e.g. Berlekamp-Welch, Berlekamp-Massey or list decoding approaches
- Reduction of the computation modulo a prime by decomposing the number field into prime ideals such as in [ALR17]
- Determine the bit complexity of Decoding algorithms for Gabidulin codes over characteristic zero with the same methods.

References

[ALR17] Daniel Augot, Pierre Loidreau, and Gwezheneg Robert.
Generalized Gabidulin Codes Over Fields of Any Characteristic.
Des. Codes Cryptogr., pages 1–42, 2017.

[Rot06] Ron M. Roth.
Introduction to Coding Theory.
Cambridge UP, 2006.

[RS85] Ron M Roth and Gadiel Seroussi.
On Generator Matrices of MDS Codes.
IEEE Trans. Inf. Theory, 31(6):826–830, November 1985.

[SOPB19] Carmen Sippel, Cornelia Ott, Sven Puchinger, and Martin Bossert.
Reed–Solomon Codes over Fields of Characteristic Zero, 2019.
Available at
https://nt.uni-ulm.de/sippelottpuchrs2019extended.

[vzGG13] Joachim von zur Gathen and Jürgen Gerhard.
Modern Computer Algebra.
Cambridge university press, 2013.