ulm university universität ulm

On Reformulated Multi–Sequence Problems

Alexander Zeh and Wenhui Li

TAIT, University of Ulm, Germany and
INRIA Saclay-Île de France, France

September 9, 2010

Twelfth International Workshop on Algebraic and Combinatorial Coding Theory (ACCT 2010), Akademgorodok, Novosibirsk, RUSSIA

Motivation (i) - Various Applications

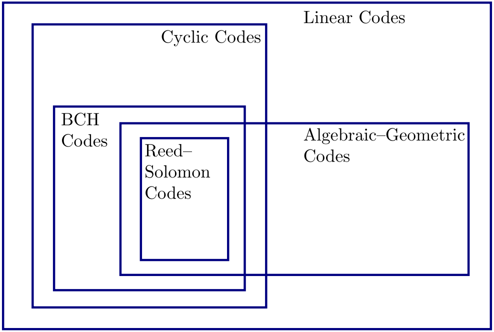
Irving Reed and Gustave Solomon discovered in 1960 codes.

1. Algebraic Structure:
   - (I)DFT or
   - Interpolation
2. Useful Properties:
   - MDS and Burst-Error,...

RS Codes in applications

1. Storage Systems:
   - CD, DVD, Blue-Ray, RAID-Systems
2. Communication Systems:
   - DSL, WiMax, DVB

Motivation (ii) - RS as Intersection



Definition Reed–Solomon code

Let $\mathcal{L}$ be the set $\{\alpha_1, \dots, \alpha_n\}$ over $\mathbb{F}_q$.

$$\mathcal{RS}(n,k) = \{\mathbf{c} = f(\mathcal{L}) : f(x) \in \mathbb{F}_k[x]\}$$

Outline

Plan

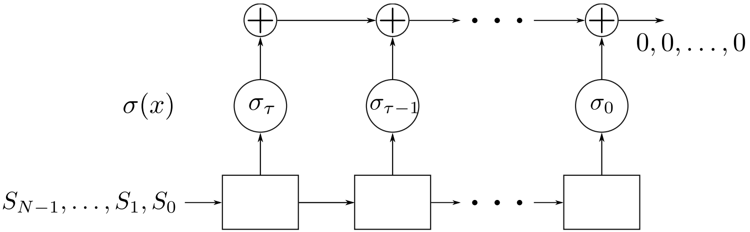
Single–Sequence Shift–Register Synthesis

Single–Sequence Shift–Register Problem

Let a sequence $\mathbf{S} = (S_0, S_1, \dots, S_{N-1})$ of length N over $\mathbb{F}$ be given. Then we search the connection polynomial $\sigma(x) = \sigma_0 + \sigma_1 x + \dots + \sigma_{\ell-1} x^{\ell-1} + x^{\ell}$ with the smallest degree ℓ such that:

$$S_i + \sigma_{\ell-1} \cdot S_{i-1} + \dots + \sigma_0 \cdot S_{i-\ell} = 0$$

for all $i = \ell, \ell+1, \dots, N-1$.



Algorithms for Single–Sequence

Conventional syndrome–based half–minimum distance decoding for an $\mathcal{RS}(n,k)$ code with $\tau_0 = \lfloor (n-k)/2 \rfloor$.

Berlekamp–Massey Algorithm

$$\sum_{i=0}^{\tau} \sigma_i S_{i+j} = 0, \tag{1}$$

for all $j = \tau, \tau+1, \dots, n-k-1$.

Extended Euclidean Algorithm gcd($S(x)$,x^{n-k})

$$f_i(x)S(x) + g_i(x)x^{n-k} = r_i(x), \tag{2}$$

till $i = k$, where $\deg r_k(x) < f_k(x)$, and $\deg r_{k-1}(x) \geq f_{k-1}(x)$, then $f_k(x) = \sigma(x)$.

Plan

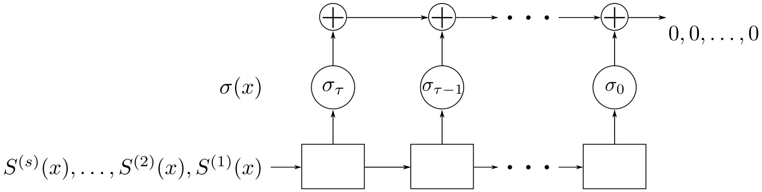
Multi–Sequence Shift–Register Synthesis

Multi–Sequence Varying Length

Let s sequences $\mathbf{S}^{(h)} = (S_0^{(h)}, S_1^{(h)}, \dots, S_{N_h-1}^{(h)})$ of different lengths $N_0, N_1, \dots, N_{s-1}$ be defined over $\mathbb{F}$. Then we search the connection polynomial $\sigma(x) = \sigma_0 + \sigma_1 x + \cdots + \sigma_{\ell-1} x^{\ell-1} + x^{\ell}$ with the smallest degree ℓ such that:

$$S_i^{(h)} + \sigma_{\ell-1} \cdot S_{i-1}^{(h)} + \cdots + \sigma_0 \cdot S_{i-\ell}^{(h)} = 0 \quad (3)$$

for all $i = \ell, \ell+1, \dots, N_h - 1$ and for all $h = 0, \dots, s-1$.



Interleaved Reed–Solomon Codes

The set of code locator's: $\mathcal{L}$,

$$f(\mathcal{L}) = (f(\alpha_i), \ldots, f(\alpha_n))$$

A Reed–Solomon code $\mathcal{RS}(n,k)$ over a field $\mathbb{F}$ with $n < q$ is given by

$$\mathcal{RS}(n,k) = \{\mathbf{c} = f(\mathcal{L}) : f(x) \in \mathbb{F}_k[x]\},$$

An s–times interleaved RS code is given by:

Virtual Extension to an IRS-code

$$\begin{pmatrix} \mathbf{c}^{<1>} \\ \mathbf{c}^{<2>} \\ \vdots \\ \mathbf{c}^{<s>} \end{pmatrix} = \begin{pmatrix} f^{(1)}(\mathcal{L}) & : f^{(1)}(x) & \in \mathbb{F}_{k_1}[x] \\ f^{(2)}(\mathcal{L}) & : f^{(2)}(x) & \in \mathbb{F}_{k_2}[x] \\ \vdots & & \\ f^{(s)}(\mathcal{L}) & : f^{(s)}(x) & \in \mathbb{F}_{k_s}[x] \end{pmatrix},$$

where $\tau_{IRS} < \left\lfloor \frac{s}{s+1}(n - \frac{1}{s}\sum_{i=1}^{s} k_i) \right\rfloor$ for burst–errors.

Virtual Extension to an IRS Scheme

The set of code locator's: $\mathcal{L}$,

$$f(\mathcal{L}) = (f(\alpha_i), \dots, f(\alpha_n))$$

A Reed–Solomon code $\mathcal{RS}(n,k)$ over a field $\mathbb{F}$ with $n < q$ is given by

$$\mathcal{RS}(n,k) = \{\mathbf{c} = f(\mathcal{L}) : f(x) \in \mathbb{F}_k[x]\},$$

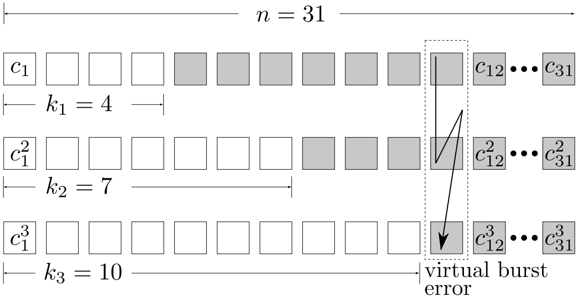
The virtual extension is given by:

Virtual Extension to an IRS-code

$$\begin{pmatrix} \mathbf{c}^{<1>} \\ \mathbf{c}^{<2>} \\ \vdots \\ \mathbf{c}^{<s>} \end{pmatrix} = \begin{pmatrix} f(\mathcal{L}) & : f(x) & \in \mathbb{F}_k[x] \\ f^2(\mathcal{L}) & : f^2(x) & \in \mathbb{F}_{2(k-1)+1}[x] \\ \vdots & & \\ f^s(\mathcal{L}) & : f^s(x) & \in \mathbb{F}_{s(k-1)+1}[x] \end{pmatrix}.$$

Decoding by the Virtual Extension (i)

Example: A $\mathcal{VIRS}(31,4,3)$ code:



Raise received word element per element to i-th power, $i = 1, \dots, s$:

$$\mathbf{r}^{[\mathbf{i}]} = \left(r_1^i, r_2^i, \dots, r_n^i\right) = \left((c_1+e_1)^i, \dots, (c_n+e_n)^i\right) = \mathbf{c}^{[\mathbf{i}]} + \mathbf{e}^{[\mathbf{i}]}.$$

Virtual Extension to an IRS Scheme (ii)

$\rightarrow$ Results in a multi–sequence shift–register problem of varying length for the common error–locator polynomial with s sequences:

$$S^{(t)}(x) \equiv \frac{R(x)^t}{G(x)} \mod x^{n-t(k-1)-1},$$

where $R(x)$ is s.t. $R(\alpha_i) = r_i$ and $G(x) = \prod_{i=1}^{n} (x - \alpha_i)$.
Here we have a unique solution as long as:

$$\tau \leq \left\lfloor \frac{s}{s+1}(n - \frac{1}{2}(s+1)(k-1) - 1) \right\rfloor.$$

$\Rightarrow$ Up to $\tau \approx 1 - \sqrt{2R}$ for low–rate RS codes.

Plan

The GS Algorithm for Decoding RS Codes (i)

INPUT :

- Parameters n, k, ℓ, τ, s and $\{(\alpha_i, r_i)\}_{i=1}^{n}$ where $\alpha_i, r_i \in F$

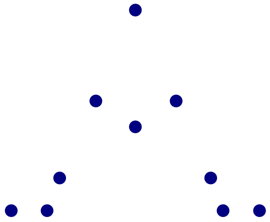
STEP 1 (Find a $Q(x,y)$ which fulfills):

- $\deg_{1,k-1} Q(x,y) < s(n-\tau)$
- $Q^{[a,b]}(\alpha_i, r_i) = 0, \quad \forall\, a+b < s$

STEP 2 (Factorization):

- Factorize the bivariate polynomial $Q(x,y)$ into irreducible factors
- Output all polynomials $f(x)$ such that $(y - f(x)) | Q(x,y)$ and $f(\alpha_i) = r_i$ for at least τ of i from $\{1, \dots, n\}$

Example: $\mathcal{RS}(10,2)$ with $\tau = 6$ for a multiplicity $s = 2$



Adopted from Venkatesan Guruswami: **Algorithmic Results in List Decoding**, Now Publishers Inc, January 2007.

The GS Algorithm for Decoding RS Codes (ii)

INPUT :

- Parameters n, k, ℓ, τ, s and $\{(\alpha_i, r_i)\}_{i=1}^{n}$ where $\alpha_i, r_i \in F$

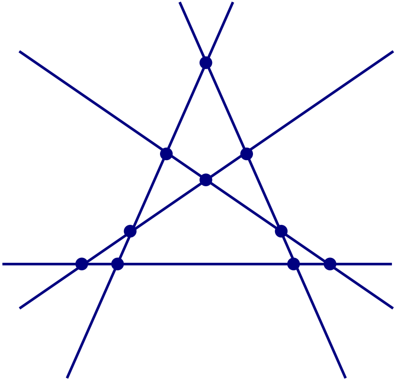
STEP 1 (Find a $Q(x, y)$ which fulfills):

- $\deg_{1,k-1} Q(x, y) < s(n - \tau)$
- $Q^{[a,b]}(\alpha_i, r_i) = 0, \quad \forall\, a + b < s$

STEP 2 (Factorization):

- Factorize the bivariate polynomial $Q(x, y)$ into irreducible factors
- Output all polynomials $f(x)$ such that $(y - f(x)) | Q(x, y)$ and $f(\alpha_i) = r_i$ for at least τ of i from $\{1, \dots, n\}$

Example: $\mathcal{RS}(10, 2)$ with $\tau = 6$ for a multiplicity $s = 2$



Adopted from Venkatesan Guruswami: **Algorithmic Results in List Decoding**, Now Publishers Inc, January 2007.

Univariate Reformulation of Sudan's Algo (i)

Roth–Ruckenstein [IEEE-IT, 2000] reformulation of the Sudan interpolation problem, where:

$$(\ell+1)(n-\tau) - \binom{\ell+1}{2}(k-1) > n$$

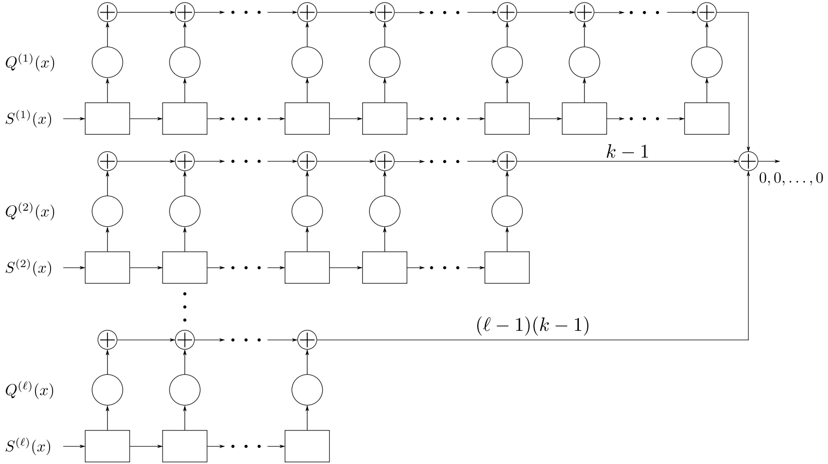
Multi–Level problem of varying lengths

Let ℓ sequences $\mathbf{S}^{(h)} = S_0^{(h)}, S_1^{(h)}, \dots, S_{N_h-1}^{(h)}$ $\forall h = 1, \dots, \ell$ of different lengths $N_h + \tau - 1$ over $\mathbb{F}$ be given. We search ℓ connection polynomials
$Q^{(h)}(x) = Q_0^{(h)} + Q_1^{(h)} x + \dots + Q_{N_h-1}^{(h)} x^{N_h-1}$ such that

$$\sum_{h=1}^{\ell} \sum_{j=0}^{N_h-1} Q_j^{(h)} \cdot S_{i+j}^{(h)} = 0,$$

holds for all $i = 0, \dots, \tau-1$.

Univariate Reformulation of Sudan's Algo (ii)



Plan

Comparison of two decoding schemes

Properties of the two schemes (IRS vs. Sudan)

We have two decoding schemes for RS codes with:

- $\approx$ decoding radius τ.
- Equivalent syndrome definition $S^{(t)}(x)$ for $t = 1, \dots, \ell$.
- Different decoding approaches: Multi–Sequence vs. Multi–Level.

$\rightarrow$ Compare them on same algorithmic basis.

Reformulation

Varying Length to Equal Length

From the s sequences $\mathbf{S}^{(0)}, \mathbf{S}^{(1)}, \ldots, \mathbf{S}^{(s-1)}$ of varying–length problem with different lengths we define

$$\widetilde{s} = s + \sum_{i=0}^{s-1} (N_i - N_{min})$$

sequences $\widetilde{\mathbf{S}}^{(h,j)}$ with the same length $N_{min} = min_i N_i$ in the following manner:

$$\begin{aligned} \widetilde{\mathbf{S}}^{(h,j)} &= (S_j^{(h)}, S_{j+1}^{(h)}, \ldots, S_{j+N_{min}-1}^{(h)}) \\ &= (\widetilde{S}_0^{(h,j)}, \widetilde{S}_1^{(h,j)}, \ldots, \widetilde{S}_{N_{min}-1}^{(h,j)}) \end{aligned}$$

for all $h = 0, \ldots, s-1$ and $j = 0, \ldots, N_h - N_{min}$.

Reformulation — General Case

Works as long $\deg \sigma(x) < N_{min}$ (in the case of the virtual extension).

Input: Sequences $\mathbf{S}^{(0)}, \mathbf{S}^{(1)}, \dots, \mathbf{S}^{(s-1)}$ of length $N_0 \geq N_1 \geq \dots \geq N_{s-1}$

Output: Shortest Shift–Register $\sigma(x)$ of degree ℓ generating $\mathbf{S}^{(0)}, \mathbf{S}^{(1)}, \dots, \mathbf{S}^{(s-1)}$

Initialize:

Arbitrary Shift–Register $\sigma(x)$ of degree N_{s-1};

Integers $\begin{pmatrix} N \\ \kappa \end{pmatrix} \leftarrow \begin{pmatrix} N_{s-1} \\ 0 \end{pmatrix}$;

while $(N == N_{s-1-\kappa})$ **do**

- $\sigma(x) \leftarrow \texttt{Shift}(\mathbf{S}^{(0)}, \mathbf{S}^{(1)}, \dots, \mathbf{S}^{(s-1-\kappa)})$;
- $N \leftarrow \deg \sigma(x)$;
- $\kappa \leftarrow \kappa + 1$;

Complexity and Multi–Level

Increased Complexity

Let $\widetilde{s}$ be the number of shifted sequences of length N_{min}, then clearly the complexity is:

$$\mathcal{O}\left(\widetilde{s} N_{min}^2\right),$$

for the case, where $\deg \sigma(x) < N_{min}$.

Similar approach for the Multi–Level problem, where

- ℓ polynomials $Q^{(t)}(x), t = 1..\ell$ are concatenated to one
- General approach was given.

Plan

Conclusion and Outlook

Conclusion

- Two decoding schemes, capable of decoding RS codes beyond $\tau_0 = (n-k)/2$ were investigated.
- The two decoding problems were reformulated into a multi–sequence shift–register problem of equal length.

Outlook

- Combination of two presented decoding approaches corresponds to the reformulated Guruswami–Sudan interpolation problem.

Thank You!