

# Sudan's key equation and syndrome extension

Iwan Duursma  
Université de Limoges

Augsburg, 2 August 1999

# Decoding of BCH Codes

# 1

## Partial realisation

Peterson 1960  
Zierler-Gorenstein 1961

Berlekamp 1968  
Massey 1969

Justesen et al. 1988  
Feng and Rao 1993

## Interpolation

\*

Welch-Berlekamp 1986

Sudan 1997

\* Wolf 1967: Decoding of BCH codes and Prony's method for curve fitting

\* Peterson-Weldon: "Mathematically the method is closely related to an interpolation problem "

\* McEliece

## Comparison

# 2

Partial realisation

Interpolation

syndromes

information symbols

control matrix

generator matrix

frequency domain

time domain

approximation

interpolation

differentials

functions

## The affine line

# 3

(codelength  $n = q$ , dimension  $k$ )

$$G = (\mathbf{g}_1, \dots, \mathbf{g}_k)^T, \quad H = (\mathbf{h}_1, \dots, \mathbf{h}_{n-k})^T$$

$$\bar{G} = (\mathbf{g}_1, \dots, \mathbf{g}_n)^T, \quad \bar{H} = (\mathbf{h}_1, \dots, \mathbf{h}_n)^T$$

$$\bar{G} = \bar{H} =$$

$$= \begin{pmatrix} 1 & 1 & \dots & 1 & \dots & 1 & 1 \\ x_0 & x_1 & & x_i & & x_{q-2} & 0 \\ \vdots & & & & & & \vdots \\ x_0^j & x_1^j & & x_i^j & & x_{q-2}^j & 0 \\ \vdots & & & & & & \vdots \\ x_0^{q-2} & x_1^{q-2} & & x_i^{q-2} & & x_{q-2}^{q-2} & 0 \\ 1 & 1 & \dots & 1 & \dots & 1 & 0 \end{pmatrix}$$

## Syndromes

# 4

For a vector  $\mathbf{y} = (y_0, y_1, \dots, y_{q-1})$

the vector of known syndromes

$$\mathbf{s} = \mathbf{H}\mathbf{y}^T = (S_0, \dots, S_{n-k-1})^T$$

and the vector of all syndromes

$$\bar{\mathbf{s}} = \bar{\mathbf{H}}\mathbf{y}^T = (S_0, \dots, S_{n-k-1}, \dots, S_{q-1})^T$$

$\bar{\mathbf{s}}$  is also called the Fourier transform of  $\mathbf{y}$

## The partial realisation problem

# 5

Parameters: Integers  $q, r, \tau$

(Berlekamp-Massey  $r = 2\tau$ )

Input: A finite sequence  $S_0, S_1, \dots, S_{r-1}$   
over a finite field of  $q$  elements

Output: All simple recurrence relations  
of length at most  $\tau + 1$  and  
of period length dividing  $q - 1$  that  
generate an infinite sequence  
 $S_0, S_1, \dots, S_{r-1}, \dots$

## The interpolation problem

# 6

Parameters: Integers  $q, k, \tau$

(Welch-Berlekamp  $q = k + 2\tau$ )

Input: A vector  $(y_0, y_1, \dots, y_{q-1})$   
over a finite field of  $q$  elements  
An ordering  $x_0, x_1, \dots, x_{q-1}$   
of the elements of the finite field

Output: All polynomials  $f(X)$  of degree  
at most  $k - 1$  for which  $f(x_i) \neq y_i$   
in at most  $\tau$  coordinates

## Example

# 7

$$q = 7, r = 4, k = 3, \tau = 2$$

$$S_0 = 0, S_1 = 4, S_2 = 4, S_3 = 4$$

has shortest recurrence relation

$$S_{i+2} - S_{i+1} = 0$$

$$(x_i) = (1, 2, 3, 4, 5, 6, 0)$$

$$(y_i) = (0, 0, 5, 5, 0, 4, 0)$$

has optimal quadratic interpolation

$$(x_i^2 + 3) = (-, 0, 5, 5, 0, 4, -)$$

## Berlekamp-Massey

# 8

Let

$$R(T) = \underbrace{S_0 + S_1T + \cdots + S_{r-1}T^{r-1}}_{\text{known syndromes}} + \cdots$$

Key equation

$$\sigma(T)R(T) \equiv \omega(T) \pmod{T^r}$$

$$\sigma(T) = 1 + \sigma_1T + \cdots + \sigma_eT^e$$

$$\deg(\omega) < \deg(\sigma) + \delta$$

Corresponding system of linear equations

$$\begin{pmatrix} S_0 & S_1 & \cdots & S_e \\ S_1 & S_2 & & S_{e+1} \\ \vdots & & & \vdots \\ S_{r-1-e} & \cdots & \cdots & S_{r-1} \end{pmatrix} \begin{pmatrix} \sigma_e \\ \sigma_{e-1} \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

## Welch-Berlekamp 1/2

# 9

### Key equation

$$h(x_i) y_i = g(x_i), \quad \forall i = 0, 1, \dots, q-1$$

$$h(X) = X^e + h_1 X^{e-1} + \dots + h_e$$

$$\deg(g) \leq \deg(h) + k - 1$$

Fourrier transform gives system of linear equations

$$\begin{pmatrix} S_e & S_{e-1} & \cdots & S_0 \\ S_{e+1} & S_e & & S_1 \\ \vdots & & & \vdots \\ S_{q-k-1} & \cdots & \cdots & S_{q-k-1-e} \end{pmatrix} \begin{pmatrix} 1 \\ h_1 \\ \vdots \\ h_e \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Let

$$y(x_i) = y_i, \quad \forall i = 0, 1, \dots, q-1$$

$$\deg(y) \leq q-1$$

Then

$$y(X) = \dots \underbrace{-S_{q-k-1}X^k - \dots - S_0X^{q-1}}_{\substack{\text{syndromes of received word} \\ \text{equal to error syndromes}}}$$

Polynomial key equation

$$y(X)h(X) \equiv g(X) \pmod{X^q - X}$$

Equal coefficients for  $X^{e+k}, \dots, X^{q-1}$   
gives previous system of linear equations

$$b = 1 \left\{ \begin{array}{l} h(x_i)y_i = g(x_i), \quad \forall i = 0, 1, \dots, q - 1 \\ h(x)y - g(x) = 0 \\ h(x)(y - f(x)) = 0 \\ y = f(x) \end{array} \right.$$

↓

$$b > 1 \left\{ \begin{array}{l} \dots \\ Q(x, y) = 0 \\ h_0(x)(y - f_1(x)) \cdots (y - f_b(x)) = 0 \\ y = f_1(x), \dots, f_b(x) \end{array} \right.$$

## Sudan I

# 12

Parameters: Integers  $q, k, \tau, b$

Key equation

$$h_0(x_i) y_i^b + \cdots + h_{b-1}(x_i) y_i = g(x_i)$$

$$\forall i = 0, 1, \dots, q-1$$

$$\deg(h_j) + (b-j)(k-1) \leq q-1-\tau$$

$$\deg(g) \leq q-1-\tau$$

$$Q(x, y) = h_0 y^b + \cdots + h_{b-1} y - g$$

## Example

# 13

$$q = 13, k = 2, \tau = 8, b = 3$$

Let

$$(x_i) = (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 0)$$

$$(y_i) = (3, 2, 1, 4, 6, 5, 8, 7, 9, 12, 11, 10, 0)$$

Solution to the key equation

$$x_i y_i^3 = x_i^4, \quad \forall i = 0, 1, \dots, 12$$

Optimal linear interpolations of  $(y_i)$

$$(x_i) = (-, 2, -, 4, -, -, -, -, 9, -, 11, -, 0)$$

$$(3x_i) = (3, -, -, -, -, 5, 8, -, -, -, -, 10, 0)$$

$$(9x_i) = (-, -, 1, -, 6, -, -, 7, -, 12, -, -, 0)$$

## Back to syndromes

# 14

Let  $S(\mathbf{y}) = \bar{\mathbf{G}} \text{diag}(\mathbf{y}) \bar{\mathbf{G}}^T$

Then  $y_i \neq f(x_i)$  in at most  $\tau$  positions

if and only if

$$\text{rank } S(y_i - f(x_i)) \leq \tau$$

## Example

# 15

$$q = 13, k = 2, \tau = 8, b = 3$$

$$(x_i) = (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 0)$$

$$(y_i) = (1, 5, 9, 8, 2, 6, 12, 4, 3, 11, 10, 7, 0)$$

$$S(y_i - ax_i - b) =$$

$$\begin{pmatrix} 0 & 4 & 0 & 0 & 3 & 0 & 0 & 12 & 0 & 0 & 6 & a & b \\ 4 & 0 & 0 & 3 & 0 & 0 & 12 & 0 & 0 & 6 & a & b & 4 \\ 0 & 0 & 3 & 0 & 0 & 12 & 0 & 0 & 6 & a & b & 4 & 0 \\ 0 & 3 & 0 & 0 & 12 & 0 & 0 & 6 & a & b & 4 & 0 & 0 \\ 3 & 0 & 0 & 12 & 0 & 0 & 6 & a & b & 4 & 0 & 0 & 3 \\ 0 & 0 & 12 & 0 & 0 & 6 & a & b & 4 & 0 & 0 & 3 & 0 \\ 0 & 12 & 0 & 0 & 6 & a & b & 4 & 0 & 0 & 3 & 0 & 0 \\ 12 & 0 & 0 & 6 & a & b & 4 & 0 & 0 & 3 & 0 & 0 & 12 \\ 0 & 0 & 6 & a & b & 4 & 0 & 0 & 3 & 0 & 0 & 12 & 0 \\ 0 & 6 & a & b & 4 & 0 & 0 & 3 & 0 & 0 & 12 & 0 & 0 \\ 6 & a & b & 4 & 0 & 0 & 3 & 0 & 0 & 12 & 0 & 0 & 6 \\ a & b & 4 & 0 & 0 & 3 & 0 & 0 & 12 & 0 & 0 & 6 & a \\ b & 4 & 0 & 0 & 3 & 0 & 0 & 12 & 0 & 0 & 6 & a & b \end{pmatrix}$$

## **How to solve list decoding in the partial realisation setting?**

1. Take Fourier transform of Sudan's key equation
2. Write Sudan's key equation in polynomial form

## Fourrier transform

# 17

$$S(\mathbf{y}) = \bar{\mathbf{G}} \text{diag}(\mathbf{y}) \bar{\mathbf{G}}^T$$

Let

$$T(\mathbf{y}) = \bar{\mathbf{G}} \text{diag}(\mathbf{y}) \bar{\mathbf{G}}^{-1} = S(\mathbf{y})(\bar{\mathbf{G}}\bar{\mathbf{G}}^T)^{-1}$$

Key equation

$$T(h_0) T(y - f_1) \cdots T(y - f_b) = 0$$

Observation: **Rather than minimizing the rank of one particular matrix, one should look for a finite set of similar matrices with zero product**

## Affine line

# 18

$$\bar{G}\bar{G}^T = \begin{pmatrix} 0 & 0 & \dots & 0 & -1 \\ 0 & & & -1 & 0 \\ \vdots & & & & \vdots \\ 0 & -1 & & & 0 \\ -1 & 0 & \dots & 0 & -1 \end{pmatrix}$$

$$(\bar{G}\bar{G}^T)^{-1} = \begin{pmatrix} 1 & 0 & \dots & 0 & -1 \\ 0 & & & -1 & 0 \\ \vdots & & & & \vdots \\ 0 & -1 & & & 0 \\ -1 & 0 & \dots & 0 & 0 \end{pmatrix}$$

## Computation of $g(x)$ suffices

# 19

Let

$$Q(x, y) = h_0 y^b + \dots + h_{b-1} y - g$$

be the unique solution to the key equation

$$Q(x_i, y_i) = 0, \quad \forall i = 0, 1, \dots, q-1$$

Then

$$R(x_i, y_i - f(x_i)) = 0, \quad \forall i = 0, 1, \dots, q-1$$

has unique solution  $R(x, y) = Q(x, y + f)$

$$\text{And } (y - f) \mid Q(x, y) \Leftrightarrow y \mid R(x, y)$$

**Idea: Find the translated vector  $(y_i - f(x_i))$  whose interpolation polynomial  $Q(x, y)$  has  $g(x) = 0$**

## Example

# 20

$$q = 13, k = 2, \tau = 8, b = 3$$

$$(x_i) = (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 0)$$

$$(y_i) = (1, 5, 9, 8, 2, 6, 12, 4, 3, 11, 10, 7, 0)$$

Solution to the key equation for  $(y_i - ax_i - b)$

$$Q(x, y) =$$

$$\begin{aligned} & xy^3 + (10ax^2 + 3bx)y^2 + \\ & + (10a^2x^3 + (10 + 6ba)x^2 + 10b^2x)y + \\ & + (\underline{1 + a^3})x^4 + (\underline{3a + 10ba^2})x^3 + \\ & + (10b + 3ab^2)x^2 + (12b^3 + 12)x \end{aligned}$$

$$g(x) = 0 \text{ for } a^3 = -1 \text{ and } ab = 1$$

Optimal linear interpolations of  $(y_i)$

$$f_1 = 4x - 3, \quad f_2 = 10x - 9, \quad f_3 = 12x - 1$$

## **Syndrome extension**

# 21

Theorem (Elimination of unknown syndromes):

**Under the conditions of Sudan I, the unknown syndromes can be computed from the known syndromes one by one as the zeros of univariate polynomials whose coefficients are determinental expressions in the known syndromes**