Closed formulas for the error locator polynomials of cyclic codes

Dedicated to Tom Høholdt in honour of his 60-th birthday

by **Ruud Pellikaan**
Discrete Mathematics
Technical University of Eindhoven

June 2, 2005

Decoding cyclic codes

beyond the BCH error-correcting capacity.

Roughly four methods:

I) **Buchberger's algorithm, Gröbner basis**

syndrome equations in

error-positions and values

II) **Newton identities**

in syndromes and coefficients of
error-locator polynomial

III) **Majority voting of unknown syndromes, error-locating pairs**

IV) **Sudan's list decoding**

Ternary Golay code [11,6,5]

Cyclic code of length $n = 11$ over $\mathbb{F}_3$

11 divides $3^5 - 1$: $11 * 22 = 242$

$\alpha \in \mathbb{F}_{243}$ of order 11

$c(x) = c_0 + c_1 x + \cdots + c_{10} x^{10}$

with $c_i \in \mathbb{F}_3$ and $x^{11} = 1$

is a codeword if and only if $c(\alpha) = 0$

if $c(x)$is a codeword, then $c(\alpha) = 0$

so $c(\alpha^3) = 0$, $c(\alpha^9) = 0$, $\ldots$

Hence $c(\alpha^i) = 0$ for i one of

$1, 3, 9, 27 \equiv 5,\ 15 \equiv 4, 12 \equiv 1$

that is

$1, -, 3, 4, 5, -, -, -, 9, -, -$

complete defining set

$1, -, 3, 4, 5, -, -, -, 9, -, -$

hence the **dimension** is $11 - 5 = 6$

minimum distance d is at least $d_{BCH} = 4$

in fact $d = 5$

so 2 error-correcting

Error-correction

$c(x)$ the codeword sent over a channel

$y(x)$ the received word

$y(x) = c(x) + e(x)$ with

$e(x)$ the error vector/polynomial

$s_j = e(\alpha^j)$ the j-th **syndrome**

If j in the complete defining set, then

$s_j = y(\alpha^j)$ is a **known** syndrome,

otherwise an **unknown** syndrome

Now

$$s_j^3 = s_{3j}$$

Hence

$$s_1^3 = s_3 \qquad s_1^9 = s_9$$

$$s_1^{27} = s_5 \qquad s_1^{81} = s_4$$

$$s_1^{243} = s_1$$

in case of t errors

error polynomial $e(x)$

has weight t supported at positions

$$i_1 < \cdots < i_t$$

$$e(x) = e_{i_1} x^{i_1} + \cdots + e_{i_t} x^{i_t}$$

$$e(\alpha^j) = e_{i_1}\alpha^{ji_1} + \cdots + e_{i_t}\alpha^{ji_t}$$

$$s_j = e(\alpha^j) = y_1 x_1^j + \cdots + y_t x_t^j$$

$$x_w = \alpha^{i_w}$$ **error position**

$$y_w = e_{i_w}$$ **error value**

Minimum distance $d = 5$

Assume that number of errors $t \leq 2$

Then $c(x)$ is the unique closest codeword

and $s_1 = y_1 x_1 + y_2 x_2$

$y_i^3 = y_i$ and $x_i^{11} = 1$ for $i = 1, 2$

Try to solve these nonlinear equations by

clever manipulations,

or apply **Buchberger's algorithm**

for a **Gröbner basis**

1990-1994: Brinton Cooper III and
Chen-Helleseth-Reed-Truong

Polynomial equations

$$S_1 = Y_1 X_1 + Y_2 X_2$$

$$Y_1^2 = 1,\ X_1^{11} = 1,\ Y_2 = 1,\ X_2^{11} = 1$$

$$(X_1 - X_2)^{242} = 1$$

in the variables with lex order

$$S_1 < X_1 < X_2 < Y_1 < Y_2$$

elimination order

Computer algebra packages

Maple, Mathematica: slow

Singular, Magma: fast

computing Gröbner bases

Example with Magma

```
P<Y2,Y1,X2,X1,S1> := PolynomialRing(GF(3),5);
I := ideal<P|X1*Y1+X2*Y2-S1,
Y1^2-1,Y2^2-1,X1^11-1,X2^11-1,
(X1-X2)^242-1>;
GroebnerBasis(I);
```

```
Magma V2.11-10    Fri May 13 2005 08:29:55 on modu
   ------------------------------------

[
     .
     .
     .
     .
X1^2 + 2*X1*S1^144 + X1*S1^100 + 2*X1*S1^34 +
     X1*S1^12 + 2*S1^200 + S1^178 + 2*S1^156 +
     2*S1^134 + S1^90 + 2*S1^68 + 2*S1^46 +
     S1^24 + 2*S1^2,
S1^220 + S1^198 + S1^176 + S1^154 + S1^132 +
     S1^110 + S1^88 + S1^66 + S1^44 + S1^22 + 1
]
Total time: 0.230 seconds,
Total memory usage: 3.99MB
```

```
X1^2 +

2*X1*S1^144 + X1*S1^100 + 2*X1*S1^34 + X1*S1^12 +

2*S1^200 + S1^178 + 2*S1^156 + 2*S1^134 + S1^90 +
2*S1^68 + 2*S1^46 + S1^24 + 2*S1^2
```

Coefficient of X_1^2: 1

Coefficient of X_1: $2S_1^{144} + S_1^{100} + 2S_1^{34} + S_1^{12}$

Coefficient of 1:

$2S_1^{200} + S_1^{178} + 2S_1^{156} + 2S_1^{134} +$

$S_1^{90} + 2S_1^{68} + 2S_1^{46} + S_1^{24} + 2S_1^2$

Closed formula of

error-locator polynomial

$$\sigma(X) = (X - x_1)(X - x_2) = 1 + \sigma_1 X + \sigma_2 X^2$$

$$\begin{aligned}
\sigma_1(S_1) &= -S_1^{144} + S_1^{100} - S_1^{34} + S_1^{12} \\
\sigma_2(S_1) &= -S_1^{200} + S_1^{178} - S_1^{156} - S_1^{134} + \\
&\quad S_1^{90} - S_1^{68} - S_1^{46} + S_1^{24} - S_1^{2}
\end{aligned}$$

Generic case of cyclic code

with $1, 2, \ldots, 2t$ in defining set

and received word with at most t errors

Syndrome equations:

$$S_j = Y_1 X_1^j + Y_2 X_2^j + \cdots + Y_t X_t^j \quad j = 1, \ldots, 2t,$$

Error-locator polynomial

$$\sigma^{(t)}(X) = \prod_{i=1}^{t} (X - X_i) = \sum_{j=0}^{t} \sigma_j^{(t)} X^{t-j}$$

Elementary symmetric functions:

$$\sigma_0^{(t)} = 1$$

$$\sigma_1^{(t)} = -(X_1 + X_2 + \cdots + X_t)$$

$$\vdots$$

$$\sigma_t^{(t)} = (-1)^t X_1 X_2 \cdots X_t$$

$$\sigma_j^{(t)} = (-1)^j \sum_{1 \le i_1 < \cdots < i_j \le t} X_{i_1} X_{i_2} \cdots X_{i_t}$$

Peterson-Arimoto

use **Generalized Newton identities**:

$$\begin{cases} S_{t+1} & + & \sigma_1 S_t & + & \cdots & + & \sigma_t S_1 & = & 0 \\ S_{t+2} & + & \sigma_1 S_{t+1} & + & \cdots & + & \sigma_t S_2 & = & 0 \\ & & & & \vdots & & & \vdots & \vdots \\ S_{2t} & + & \sigma_1 S_{2t-1} & + & \cdots & + & \sigma_t S_t & = & 0. \end{cases}$$

to solve linear equations in the variables σ_j with coefficients in the S_r.

Matrix equation:

$$\begin{pmatrix} S_{t+1} & S_t & \cdots & S_1 \\ S_{t+2} & S_{t+1} & \cdots & S_2 \\ \vdots & \vdots & \vdots & \vdots \\ S_{2t} & S_{2t-1} & \cdots & S_t \end{pmatrix} \begin{pmatrix} 1 \\ \sigma_1 \\ \sigma_2 \\ \vdots \\ \sigma_t \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

or equivalently

$$\begin{pmatrix} S_t & \cdots & S_1 \\ S_{t+1} & \cdots & S_2 \\ \vdots & \vdots & \vdots \\ S_{2t-1} & \cdots & S_t \end{pmatrix} \begin{pmatrix} \sigma_1 \\ \sigma_2 \\ \vdots \\ \sigma_t \end{pmatrix} = - \begin{pmatrix} S_{t+1} \\ S_{t+2} \\ \vdots \\ S_{2t} \end{pmatrix}.$$

Case $t = 2$

$$\begin{cases} S_2\sigma_1 & + & S_1\sigma_2 & = & -S_3 \\ S_3\sigma_1 & + & S_2\sigma_2 & = & -S_4 \end{cases}$$

Cramer's rule:

$$\sigma_1 = \frac{\begin{vmatrix} -S_3 & S_1 \\ -S_4 & S_2 \end{vmatrix}}{\begin{vmatrix} S_2 & S_1 \\ S_3 & S_2 \end{vmatrix}} = \frac{S_1S_4 - S_2S_3}{S_2^2 - S_1S_3}$$

and similarly

$$\sigma_2 = \frac{S_3^2 - S_2S_4}{S_2^2 - S_1S_3}$$

Generic error-locator polynomial for $t = 2$

$$(S_2^2 - S_1S_3)X^2 + (S_1S_4 - S_2S_3)X + (S_3^2 - S_2S_4)$$

$$= \begin{vmatrix} X^2 & X & 1 \\ S_3 & S_2 & S_1 \\ S_4 & S_3 & S_2 \end{vmatrix}$$

Closed formula of

generic error-locator polynomial

$$\sigma^{(t)}(X) = \begin{vmatrix} X^t & X^{t-1} & \cdots & 1 \\ S_{t+1} & S_t & \cdots & S_1 \\ S_{t+2} & S_{t+1} & \cdots & S_2 \\ \vdots & \vdots & \vdots & \vdots \\ S_{2t} & S_{2t-1} & \cdots & S_t \end{vmatrix}$$

Binary cyclic codes

error values are always one: $Y_i = 1$,

syndromes: $S_{2j} = S_j^2$

equations:

$$S_{2j-1} = X_1^{2j-1} + X_2^{2j-1} + \cdots + X_t^{2j-1}$$

for $j = 1, \ldots, t$

Algebraic system of

t equations in $2t$ variables.

Eliminate the $X_2, \ldots, X_t$.

Gives one equation

$$\beta^{(t)}(X_1) = 0$$

in the variable X_1

with coefficients

$$\beta_i^{(t)}(S_1, S_3 \ldots, S_{2t-1})$$

For $t = 1$

$$\beta^{(1)}(X) = X + S_1$$

Compare:

$$\sigma^{(1)}(X) = S_1 X - S_2$$

Reduce mod 2 and $S_{2j} = S_j^2$

$$\sigma^{(1)}(X) = S_1 X + S_1^2 = S_1 \beta^{(1)}(X)$$

For $t = 2$,

$$\beta^{(2)}(X) = S_1 X^2 + S_1^2 X + (S_3 + S_1^3)$$

Compare:

$$\sigma^{(2)}(X) =$$

$$(S_3 S_1 - S_2^2) X^2 - (S_4 S_1 - S_2 S_3) X + (S_4 S_2 - S_3^2)$$

Reduction mod 2 and $S_{2j} = S_j^2$ gives

$$(S_3 S_1 + S_1^4)X^2 + (S_3 S_1^3 + S_1^5)X + (S_3^2 + S_1^6)$$

Divide by $S_3 + S_1^3$

$$S_1 X^2 + S_1^2 X + (S_3 + S_1^3)$$

is again $\beta^{(2)}(X)$

For $t = 3$,

$$\beta^{(3)}(X) =$$

$$(S_3 + S_1^3)X^3 + S_1(S_3 + S_1^3)X^2 +$$

$$(S_5 + S_3S_1^2)X + (S_5S_1 + S_3^2 + S_3S_1^3 + S_1^6)$$

Compare:

$$\sigma^{(3)}(X) =$$

$$(S_5S_3S_1 - S_5S_2^2 - S_4^2S_1 + 2S_4S_3S_2 - S_3^3)X^3$$

$$-(S_6S_3S_1 - S_6S_2^2 - S_5S_4S_1 + S_5S_3S_2 - S_4S_3^2 + S_4^2S_2)X^2$$

$$+(S_6S_4S_1 - S_6S_3S_2 - S_5^2S_1 + S_5S_3^2 + S_5S_4S_2 - S_4^2S_3)X$$

$$-(S_6S_4S_2 - S_3^2S_6 - S_5^2S_2 + 2S_5S_4S_3 - S_4^3)$$

Reduction mod 2 and $S_{2j} = S_j^2$ gives

$$(S_5 S_3 S_1 + S_5 S_1^4 + S_3^3 + S_1^9) X^3 +$$

$$(S_3^3 S_1 + S_5 S_1^5 + S_5 S_3 S_1^2 + S_1^{10}) X^2 +$$

$$(S_5^2 S_1 + S_5 S_3^2 + S_5 S_1^6 + S_3^3 S_1^2 + S_3^2 S_1^5 + S_3 S_1^8) X +$$

$$(S_5^2 S_1^2 + S_3^4 + S_3^2 S_1^6 + S_1^{12})$$

Division by $(S_3 S_1^3 + S_3^2 + S_5 S_1 + S_1^6)$ gives

$$(S_3 + S_1^3) X^3 + S_1 (S_3 + S_1^3) X^2 +$$

$$(S_5 + S_3 S_1^2) X + (S_5 S_1 + S_3^2 + S_3 S_1^3 + S_1^6)$$

is again $\beta^{(3)}(X)$

General result

– $\beta^{(t)}(X)$ weighted homogeneous of

degree $t(t+1)/2$

– $\beta_t^{(t)} = \beta_0^{(t+1)}$

– $\beta_1^{(t)} = S_1 \beta_0^{(t)}$

– The reduction of $\sigma^{(t)}(X)$

modulo 2 and $S_{2j} = S_j^2$

is equal to $\beta_0^{(t)} \beta^{(t)}(X)$

Newton identities

$$\begin{cases} S_1 & +\sigma_1 & +0 & +0 & +\cdots & +0 & =0 \\ S_2 & +\sigma_1 S_1 & +2\sigma_2 & +0 & +\cdots & +0 & =0 \\ S_3 & +\sigma_1 S_2 & +\sigma_2 S_1 & +3\sigma_3 & +\cdots & +0 & =0 \\ & & \vdots & & \vdots & & \vdots \\ S_t & +\sigma_1 S_{t-1} & +\sigma_2 S_{t-2} & +\sigma_3 S_{t-3} & +\cdots & +t\sigma_t & =0. \end{cases}$$

$$\begin{cases} S_{t+1} & + & \sigma_1 S_t & + & \cdots & + & \sigma_t S_1 & = & 0 \\ S_{t+2} & + & \sigma_1 S_{t+1} & + & \cdots & + & \sigma_t S_2 & = & 0 \\ & & & & \vdots & & & \vdots & \vdots \\ S_{2t} & + & \sigma_1 S_{2t-1} & + & \cdots & + & \sigma_t S_t & = & 0. \end{cases}$$