The Golay codes

Mario de Boer and Ruud Pellikaan *

Appeared in *Some tapas of computer algebra*
(A.M. Cohen, H. Cuypers and H. Sterk eds.),
Project 7, The Golay codes, pp. 338-347,
Springer, Berlin 1999,
after the EIDMA/Galois minicourse on Computer Algebra,
September 27-30, 1995, Eindhoven.

*Both authors are from the Department of Mathematics and Computing Science, Eindhoven University of Technology, P.O. Box 513, 5600 MB Eindhoven, The Netherlands.

Contents

1 Introduction

In this project we will give examples of methods described in the previous chapters on finding the minimum weight codewords, the decoding of cyclic codes and working with the Mathieu groups. The codes that we use here are the well known *Golay codes*. These codes are among the most beautiful objects in coding theory, and we would like to give some reasons why.

There are two Golay codes: the ternary cyclic code $\mathcal{G}_{11}$ and the binary cyclic code $\mathcal{G}_{23}$.

The ternary Golay code $\mathcal{G}_{11}$ has parameters $[11, 6, 5]$, and it is the unique code with these parameters. The automorphism group $Aut(\mathcal{G}_{11})$ is the Mathieu group M_{11}. The group M_{11} is simple, 4-fold transitive and has size $11 \cdot 10 \cdot 9 \cdot 8$. The supports of the codewords of weight 5 form the blocks of a 4-design, the unique Steiner system $S(4, 5, 11)$. The ternary Golay code is a perfect code, this means that the Hamming spheres of radius $(d-1)/2 = 2$ centered at the codewords of $\mathcal{G}_{11}$ exactly cover the whole space $\mathbb{F}_3^{11}$. The code $\mathcal{G}_{11}$ can be uniquely extended to a $[12, 6, 6]$ code, which we will denote by $\mathcal{G}_{12}$. The code $\mathcal{G}_{12}$ is self-dual and $Aut(\mathcal{G}_{12}) = M_{12}$: the simple, 5-fold transitive Mathieu group of size $12{\cdot}11{\cdot}10{\cdot}9{\cdot}8$. The supports of the codewords of weight 6 in $\mathcal{G}_{12}$ form a 5-design, the unique $S(5, 6, 12)$.

The binary Golay code $\mathcal{G}_{23}$ has similar properties. Its parameters are $[23, 12, 7]$, and it is the unique code with these parameters. The automorphism group $Aut(\mathcal{G}_{23})$ is the Mathieu group M_{23}. The group M_{23} is simple, 4-fold transitive and has size $23 \cdot 22 \cdot 21 \cdot 20 \cdot 48$. The supports of the codewords of weight 7 form the blocks of a 4-design, the unique Steiner system $S(4, 7, 23)$. The binary Golay code is a perfect code, so the Hamming spheres of radius 3 centered at the codewords of $\mathcal{G}_{11}$ exactly cover the whole space $\mathbb{F}_2^{23}$. The code $\mathcal{G}_{23}$ can be uniquely extended to a $[24, 12, 8]$ code, which we will denote by $\mathcal{G}_{24}$. The code $\mathcal{G}_{24}$ is self-dual and $Aut(\mathcal{G}_{24}) = M_{24}$: the simple, 5-fold transitive Mathieu group of size $24 \cdot 23 \cdot 22 \cdot 21 \cdot 20 \cdot 48$. The supports of the codewords of weight 8 in $\mathcal{G}_{24}$ form a 5-design, the unique $S(5, 8, 24)$.

2 Minimal weight codewords of $\mathcal{G}_{11}$

$\mathcal{G}_{11}$ is the ternary cyclic code of length 11 with defining set $J = \{1\}$. It is a $[11, 6, d]$ code with complete defining set $J(\mathcal{G}_{11}) = \{1, 3, 4, 5, 9\}$. The generator polynomial is

$$g(X) = \prod_{j \in J(\mathcal{G}_{11})} (X - \alpha^j) = 2 + X^2 + 2X^3 + X^4 + X^5.$$

From the BCH bound we see that $d \geq 4$, and by computing Gröbner bases we will show that in fact $d = 5$. Moreover we will determine all codewords of

minimal weight.

First we consider the system $\mathcal{S}_{\mathcal{G}_{11}}(4)$:

$$\mathcal{S}_{\mathcal{G}_{11}}(4) = \begin{cases} A_5 + \sigma_1 A_4 + \sigma_2 A_3 + \sigma_3 A_2 + \sigma_4 A_1 &= 0 \\ A_6 + \sigma_1 A_5 + \sigma_2 A_4 + \sigma_3 A_3 + \sigma_4 A_2 &= 0 \\ \vdots & \vdots \ \vdots \\ A_4 + \sigma_1 A_3 + \sigma_2 A_2 + \sigma_3 A_1 + \sigma_4 A_0 &= 0 \\ A_j = 0 \ \text{ for } \ j \in J(\mathcal{G}_{11}) & \\ A_{3j} = A_j^3 \ \text{ for } \ j = 1, \ldots, 11. & \end{cases}$$

Using $A_{3i} = A_i^3$ we can express every A_i with $i \in \{1, 2, \ldots, 10\} \setminus J(\mathcal{G}_{11})$ as a power of A_2 (this can be done since all of these i form a single cyclotomic coset). Setting $A_i = 0$ for $i \in J(\mathcal{G}_{11})$ and writing $A_2 = a$ and $A_0 = b$ this reduces $\mathcal{S}_{\mathcal{G}_{11}}(4)$ to

$$\mathcal{S}_{\mathcal{G}_{11}}(4) = \begin{cases} \sigma_3 a &= 0 \\ a^3 + \sigma_4 a &= 0 \\ a^9 + \sigma_1 a^3 &= 0 \\ a^{81} + \sigma_1 a^9 + \sigma_2 a^3 &= 0 \\ \sigma_1 a^{81} + \sigma_2 a^9 + \sigma_3 a^3 &= 0 \\ a^{27} + \sigma_2 a^{81} + \sigma_3 a^9 + \sigma_4 a^3 &= 0 \\ b + \sigma_1 a^{27} + \sigma_3 a^{81} + \sigma_4 a^9 &= 0 \\ \sigma_1 b + \sigma_2 a^{27} + \sigma_4 a^{81} &= 0 \\ a + \sigma_2 b + \sigma_3 a^{27} &= 0 \\ \sigma_1 a + \sigma_3 b + \sigma_4 a^{27} &= 0 \\ \sigma_2 a + \sigma_4 b &= 0 \\ b^3 - b &= 0. \end{cases}$$

Computing a Gröbner basis $\mathcal{G}$ with respect to the lexicographic order with

$$\sigma_4 > \sigma_3 > \sigma_2 > \sigma_1 > b > a$$

gives $\mathcal{G} = \{b, a\}$ and hence there are no nonzero codewords of weight at most 4. We conclude $d \geq 5$, and even $d = 5$, since the weight of the generator polynomial is $wt(g(X)) = 5$. To determine the minimum weight codewords we consider the system $\mathcal{S}_{\mathcal{G}_{11}}(5)$:

$$\mathcal{S}_{\mathcal{G}_{11}}(5) = \begin{cases} A_6 + \sigma_1 A_5 + \sigma_2 A_4 + \sigma_3 A_3 + \sigma_4 A_2 + \sigma_5 A_1 &= 0 \\ A_7 + \sigma_1 A_6 + \sigma_2 A_5 + \sigma_3 A_4 + \sigma_4 A_3 + \sigma_5 A_2 &= 0 \\ \vdots & \vdots \ \vdots \\ A_5 + \sigma_1 A_4 + \sigma_2 A_3 + \sigma_3 A_2 + \sigma_4 A_1 + \sigma_5 A_0 &= 0 \\ A_i = 0 \ \text{ for } \ i \in J(\mathcal{G}_{11}) & \\ A_{3i} = A_i^3 \ \text{ for } \ i = 0, \ldots, 10 & \end{cases}$$

Again we can reduce the system as we did in the system $\mathcal{S}_{\mathcal{G}_{11}}(4)$ and compute its Gröbner basis with respect to the lexicographic order with

$$\sigma_5 > \sigma_4 > \sigma_3 > \sigma_2 > \sigma_1 > b > a.$$

After 2 minutes using Axiom or 10 minutes using Macaulay, the resulting basis $\mathcal{G}$ is

$$\mathcal{G} = \begin{cases} \sigma_5 a + 2a^{31} + 2a^9, \sigma_4 a + a^3, \sigma_3 a + 2a^{107} + a^{41} + 2a^{19}, \\ \sigma_2 a + a^{79} + 2a^{35} + a^{13}, \sigma_1 a + a^{29} + 2a^7, \\ b + a^{77} + 2a^{55} + a^{33} + a^{11}, a^{133} + 2a^{111} + 2a^{89} + 2a^{67} + a^{45} + a, \end{cases}$$

where $a = A_2$ and $b = A_0$. From the triangular form of the basis $\mathcal{G}$, it is easy to see that the number of codewords of weight 5 in $\mathcal{G}_{11}$ equals the number of nonzero solutions to

$$f(X) = X^{133} + 2X^{111} + 2X^{89} + 2X^{67} + X^{45} + X = 0$$

in $\mathbb{F}_{3^5}$. We determine these solutions in the following exercise.

Exercise 2.1 Let $\alpha \in \mathbb{F}_{3^5}$ be a primitive element. Now show
1. $f(1) = 0$;
2. $f(\alpha^2) = 0$ (you can use a computer algebra package for this);
3. $f(\alpha^{11} X) = \alpha^{11} f(X)$.

Conclude from this that the complete set of zeros of $f(X)$ in $\mathbb{F}_{3^5} \setminus \{0\}$ is

$$M = \{\alpha^{i+11j} \mid i \in \{0, 1, \ldots, 10\} \setminus J(\mathcal{G}_{11}),\ j \in \{0, 1, \ldots, 21\}\}.$$

So the number of codewords of weight 5 is $\#M = 132$ and the locators of these words (i.e. the polynomials having as zeros the reciprocals of positions where the codewords have a nonzero value) are given by

$$\sigma(X, a) = \begin{cases} (a^{30} + a^8)X^5 + 2a^2 X^4 + \\ (a^{106} + 2a^{40} + a^{18})X^3 + \\ (2a^{78} + a^{34} + 2a^{12})X^2 + \\ (2a^{28} + a^6)X + 1, \end{cases}$$

with $a \in M$.
Since the code is cyclic, any shift of a codeword of weight 5 is again a codeword of weight 5. We can recognize this fact from M in the following way.

Exercise 2.2 Show that there exists a primitive 11-th root of unity β such that $\sigma(X, \alpha^{11} a) = \sigma(\beta X, a)$ for all $a \in M$.

Now we can conclude that the codewords of weight 5 consist of the 6 codewords with locator polynomials $\sigma(X, a),\ a \in \{1, \alpha^2, \alpha^6, \alpha^7, \alpha^8, \alpha^{10}\}$, their cyclic shifts, and their non-zero multiples in $\mathbb{F}_3^{11}$.

Exercise 2.3 Let α again be a primitive element in $\mathbb{F}_{3^5}$, then $\beta = \alpha^{22}$ is a fixed 11-th root of unity. Check that the zeros of the 6 polynomials $\sigma(X, a)$ are:

polynomial	$\{i \mid \beta^{-i}$ is a zero$\}$
$\sigma(X, 1)$	2, 6, 7, 8, 10
$\sigma(X, \alpha^2)$	3, 4, 9, 10, 11
$\sigma(X, \alpha^6)$	1, 5, 8, 9, 11
$\sigma(X, \alpha^7)$	1, 2, 8, 10, 11
$\sigma(X, \alpha^8)$	2, 3, 5, 7, 9
$\sigma(X, \alpha^{10})$	3, 5, 8, 10, 11

Let $\mathcal{B}$ consists of the 6 subsets in $\{1,\ldots,11\}$ of size 5 in the table and their cyclic shifts modulo 11. Then $|\mathcal{B}| = 66$. Show that $\mathcal{B}$ is the set of blocks of a 4-design, the Steiner system $S(4,5,11)$.

3 Decoding of $\mathcal{G}_{23}$ with Gröbner bases

Let $\mathcal{G}_{23}$ be the binary cyclic code of length 23 with defining set $J = \{1\}$. Then the complete defining set is $J(\mathcal{G}_{23}) = \{1,2,3,4,6,8,9,12,13,16,18\}$ and the code has parameters $[23,12,d]$. The BCH bound states that $d \geq 5$ but in fact $d = 7$. This can be checked in the same way as we did in the previous section for the ternary Golay code. The computer algebra packages we tried, did not perform very well on the systems $\mathcal{S}_{\mathcal{G}_{23}}(w)$. Since the minimum distance is 7, $\mathcal{G}_{23}$ should be able to correct errors of weight at most 3. In this example we will decode a word with three errors.

Take

$$\mathbb{F}_{2^{11}} = \mathbb{F}_2[\beta]/(\beta^{11} + \beta^2 + 1)$$

and set $\alpha = \beta^{89}$. Then β is a primitive element of $\mathbb{F}_{2^{11}}$ and α has order 23.

The generator polynomial of the code is

$$g(X) = \prod_{j \in J(\mathcal{G}_{23})} (X - \alpha^j) = 1 + X + X^5 + X^6 + X^7 + X^9 + X^{11}.$$

Suppose we send the codeword $g(X)$, which corresponds to the binary vector

$$\mathbf{c} = (1,1,0,0,0,1,1,1,0,1,0,1,0,0,0,0,0,0,0,0,0,0,0)$$

over a noisy channel, and the following error occurs during transmission:

$$\mathbf{e} = (1,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0).$$

As a result at the other end of the channel the following vector will be received:

$$\mathbf{y} = (0,1,0,1,0,1,1,1,0,1,0,1,0,0,0,0,0,1,0,0,0,0,0),$$

corresponding to the polynomial

$$r(X) = X + X^3 + X^5 + X^6 + X^7 + X^9 + X^{11} + X^{17}.$$

We will now decode the recieved word by applying the decoding algorithm. First we compute the syndrome:

$$s_1 = H\mathbf{y} = r(\alpha) = \alpha + \alpha^3 + \alpha^5 + \alpha^6 + \alpha^7 + \alpha^9 + \alpha^{11} + \alpha^{17} = \beta^9 + \beta^6 + \beta^3 + \beta^2 + 1.$$

Since $s_1 \neq 0$ we see that errors have occured during transmission.

We already remarked that the Y_i variables can be disposed of by setting them equal to 1, since 1 is the only error value that can occur.

Following the algorithm of Section **??** we set

$$\mathcal{S} = \{X_1 + \beta^9 + \beta^6 + \beta^3 + \beta^2 + 1, X_1^{23} + 1\}$$

and can conclude that there are no solutions since s_1 is not a 23-rd root of unity.

In the next step we set

$$\mathcal{S} = \{X_2 + X_1 + \beta^9 + \beta^6 + \beta^3 + \beta^2 + 1, X_2^{23} + 1, X_1^{23} + 1\}$$

and compute its Gröbner basis with respect to the lexicographic order with $X_2 > X_1$:

$$\mathcal{G} = \{1\}.$$

Since $1 \in \mathcal{G}$ there is no solution to these syndrome equations and we proceed with the loop of the algorithm. We set

$$\mathcal{S} = \{X_3 + X_2 + X_1 + \beta^9 + \beta^6 + \beta^3 + \beta^2 + 1, X_3^{23} + 1, X_2^{23} + 1, X_1^{23} + 1\},$$

and a Gröbner basis with respect to the lexicographic order with $X_3 > X_2 > X_1$ is computed:

$$\begin{cases} X_3 + X_2 + X_1 + \beta^9 + \beta^6 + \beta^3 + \beta^2 + 1, \\ X_2^2 + X_2X_1 + (\beta^9 + \beta^6 + \beta^3 + \beta^2 + 1)X_2 + X_1^2 + \\ \qquad +(\beta^9 + \beta^6 + \beta^3 + \beta^2 + 1)X_1 + \beta^6 + \beta^5 + \beta^2, \\ X_1^3 + (\beta^9 + \beta^6 + \beta^3 + \beta^2 + 1)X_1^2 + (\beta^6 + \beta^5 + \beta^2)X_1 + \beta^9 + \beta^5 + \beta^3. \end{cases}$$

This took 8 minutes using Axiom. We did the same computation with $X_j^{24} + X_j$ instead of $X_j^{23} + 1$ for $j = 1, 2, 3$ and it took only 90 seconds.

Now $1 \notin \mathcal{G}$ and there are solutions to the syndrome equations. The error locator polynomial is

$$g(X_1) = X_1^3 + (\beta^9 + \beta^6 + \beta^3 + \beta^2 + 1)X_1^2 + (\beta^6 + \beta^5 + \beta^2)X_1 + \beta^9 + \beta^5 + \beta^3$$

and its zeros are the error locators $\{\alpha^0, \alpha^3, \alpha^{17}\}$. Hence the errors occurred at positions 0, 3 and 17 and the word that was sent is

$$\mathbf{y} - (1,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0) =$$

$$(1,1,0,0,0,1,1,1,0,1,0,1,0,0,0,0,0,0,0,0,0,0,0).$$

We have recovered the transmitted codeword $\mathbf{c}$.

4 One-step decoding of $\mathcal{G}_{23}$

In this paragraph we will decode all error patterns of weight 3 that can occur in a codeword of the code $\mathcal{G}_{23}$ at once by computing the Gröbner basis for variable syndromes S. Apart from the advantage that all syndromes are treated at once,

it also has the advantage that the computations take place over the field $\mathbb{F}_2$ instead of the large field $\mathbb{F}_{2^{11}}$. The system of equations is:

$$\mathcal{S} = \begin{cases} X_3 + X_2 + X_1 + S &= 0 \\ X_3^{23} + 1 &= 0 \\ X_2^{23} + 1 &= 0 \\ X_1^{23} + 1 &= 0. \end{cases}$$

The outcome of this set of equations is quite complicated. The result is much simpler if we consider the following set of equations.

$$\mathcal{S}' = \begin{cases} X_3 + X_2 + S + X_1 &= 0 \\ X_3^{24} + X_3 &= 0 \\ X_2^{24} + X_2 &= 0 \\ X_1^{24} + X_1 &= 0. \end{cases}$$

With the lexicographic order with $X_3 > X_2 > X_1 > S$ the computer was still not finished with its computations after 24 hours. Loustaunau and York did this example where they started with the above system, which is a Gröbner bases with respect to lexicographic order with $S > X_3 > X_2 > X_1$, and transformed it into a Gröbner bases with respect to lexicographic order with $X_3 > X_2 > X_1 > S$ as explained in the Notes of Chapter **??**. Using the lexicographic order with $X_3 > X_2 > S > X_1$ we obtain the Gröbner basis:

$$\mathcal{G} = \begin{cases} X_3 + X_2 + S + X_1, \\ X_2^{24} + X_2, \\ X_2^2 S + X_2^2 X_1 + X_2 S^2 + X_2 X_1^2 + S^{256} + S^3 + S^2 X_1 + S X_1^2, \\ g(X_1), \\ X_1^{24} + X_1, \end{cases}$$

with

$$g(X_1) = \begin{cases} (S^{256} + S^3)X_1^{21} &+ (S^{257} + S^4)X_1^{20} + \\ (S^{260} + S^7)X_1^{17} &+ (S^{261} + S^8)X_1^{16} + \\ (S^{32} + S^9)X_1^{15} &+ (S^{33} + S^{10})X_1^{14} + \\ (S^{34} + S^{11})X_1^{13} &+ (S^{35} + S^{12})X_1^{12} + \\ (S^{36} + S^{13})X_1^{11} &+ (S^{37} + S^{14})X_1^{10} + \\ (S^{38} + S^{15})X_1^{9} &+ (S^{39} + S^{16})X_1^{8} + \\ (S^{40} + S^{17})X_1^{7} &+ (S^{64} + S^{41})X_1^{6} + \\ (S^{272} + S^{42})X_1^{5} &+ (S^{273} + S^{66} + S^{43} + S^{20})X_1^{4} + \\ (S^{44} + S^{21})X_1^{3} &+ (S^{68} + S^{45})X_1^{2} + \\ (S^{276} + S^{46})X_1 &+ (S^{277} + S^{70} + S^{47} + S). \end{cases}$$

We conclude that for a general syndrome S we find the error-locator polynomial

$$\gcd(g(X_1), X_1^{23} + 1).$$

These computations took 120 seconds using Axiom. The original set of equations $\mathcal{S}$ took 150 seconds. Macaulay did both these computations on the same computer in 3 seconds.

Exercise 4.1 Notice that the coefficient of X^i is divisible by $S^{23}+1$ for all i. Denote $g(X_1)/(S^{23}+1)$ by $h(X_1)$.

Exercise 4.2 Suppose $s = x_1 + x_2 + x_3$ with $x_j \in \mathbb{F}_{2^{11}}$ and $x_j^{23} = 1$ for all j. Show that $s^{23} = 1$ if and only if $x_i = x_j$ for some i, j with $1 \leq i < j \leq 3$.

Exercise 4.3 Compute $gcd(h(X_1), X_1^{23}+1)$ with Euclid's algorithm in the ring $\mathbb{F}_q(S)[X_1]$ and show that it is a polynomial of degree 3 in X_1 and rational functions in S as coefficients.

5 The key equation for $\mathcal{G}_{23}$

In this section we will use the Euclidean algorithm to decode an error that occured during the transmission of a codeword of the binary Golay code $\mathcal{G}_{23}$. As we mentioned in Section **??**, decoding a cyclic code C by solving the key equation only works for errors of weight at most $(\delta-1)/2$, where δ is is maximal such that $\{1, 2, \ldots, \delta-1\} \subset J(C)$. In the case of the binary Golay code, this means we can only expect to decode errors of weight at most 2 in this way.

As in the previous section, we assume that the transmitted codeword was $g(X)$. Suppose the following error occurs:

$$\mathbf{e} = (1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0).$$

Then the received word is

$$\mathbf{y} = (0,1,0,0,0,1,1,1,0,1,0,1,0,0,0,0,0,1,0,0,0,0,0),$$

corresponding to the polynomial

$$r(X) = X + X^5 + X^6 + X^7 + X^9 + X^{11} + X^{17}.$$

After we receive this word, we can compute the following syndromes:

$$\begin{array}{lllllll} s_1 & = & r(\alpha) & & & = & \beta^{10}+\beta^9+\beta^7+\beta^6+1 \\ s_2 & = & r(\alpha^2) & = & s_1^2 & = & \beta^7+\beta^5+\beta^2+\beta \\ s_3 & = & r(\alpha^3) & = & s_1^{256} & = & \beta^8+\beta^7+\beta^6+\beta^5 \\ s_4 & = & r(\alpha^4) & = & s_1^4 & = & \beta^{10}+\beta^5+\beta^4+\beta^3+\beta^2. \end{array}$$

Following Section **??** we define

$$S(Z) = s_1 + s_2 Z + s_3 Z^2 + s_4 Z^3$$

and we start the Euclidean algorithm on $S(Z)$ and Z^4. We find

$$Z^4 = S(Z)q_1(Z) + r_1(Z),$$

with

$$q_1(Z) = (\beta^9+\beta^3+\beta^2+1)Z + \beta^{10}+\beta^9+\beta^5+\beta$$

and

$$\begin{aligned} r_1(Z) &= (\beta^{10}+\beta^9+\beta^7+\beta^6+\beta^5+\beta^4)Z^2 + \\ &\quad (\beta^{10}+\beta^9+\beta^7+\beta^5+\beta^4+\beta^3)Z + \\ &\quad (\beta^9+\beta^6+\beta^2+1). \end{aligned}$$

In the following step we get

$$S(Z) = r_1(Z)q_2(Z) + r_2(Z),$$

with

$$q_2(Z) = (\beta^{10}+\beta^3+\beta^2+1)Z + (\beta^{10}+\beta^7+\beta^6+\beta)$$

and

$$r_2(Z) = (\beta^7+\beta^6+\beta^3+\beta^2+\beta+1).$$

Since $\deg(r_1(Z)) \geq 2$ and $\deg(r_2(Z)) \leq 1$ we can stop the algorithm and compute

$$\begin{aligned} U_2(Z) &= q_2(Z)U_1(Z) + U_0(Z) \\ &= q_2(Z)q_1(Z) + 1 \\ &= (\beta^9+\beta^8+\beta^6)Z^2 + \\ &\quad (\beta^7+\beta^6+\beta^3+\beta^2+\beta+1)Z + \\ &\quad \beta^9+\beta^8+\beta^7+\beta^3+\beta^2+\beta+1. \end{aligned}$$

From this we find

$$\sigma(Z) = U_2(Z)/(\beta^9+\beta^8+\beta^7+\beta^3+\beta^2+\beta+1) =$$

$$(\beta^{10}+\beta^9+\beta^7+\beta^6)Z^2 + (\beta^{10}+\beta^9+\beta^7+\beta^6+1)Z + 1.$$

Since the zeros of $\sigma(Z)$ are $Z = 1$ and $Z = \alpha^6$, we conclude that the error locators are 1 and α^{17} and thus that the error vector is

$$\mathbf{e} = (1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0).$$

We retrieve the transmitted codeword by computing $\mathbf{c} = \mathbf{y} - \mathbf{e}$.

Exercise 5.1 Do the same example with the algorithm of Berlekamp-Massey instead of Euclid's algorithm.

6 Exercises

Let C be the binary cyclic code C of length 15 with defining set $J = \{1,3,5\}$. In the following, $\alpha \in \mathbb{F}_{16}$ will denote a primitive element satisfying

$$\alpha^4 + \alpha + 1 = 0.$$

Exercise 6.1 Show that the complete defining set is given by

$$J(C) = \{1, 2, 3, 4, 5, 6, 8, 9, 10, 12\},$$

and that C has generator polynomial

$$g(X) = 1 + X + X^2 + X^4 + X^5 + X^8 + X^{10}.$$

Determine the dimension of the code and apply the BCH bound on the minimum distance.

In order to find the true minimum distance of C, we will determine all codewords of weight 7.

Exercise 6.2 Write down the equations of the system $\mathcal{S}_C(7)$ and reduce the system by setting $A_0 = b$ and $A_7 = a$ and expressing everything in a, b and $\sigma_1, \sigma_2, \ldots, \sigma_7$. Compute a Gröbner basis for the ideal defined by $\mathcal{S}_C(7)$ and answer the following questions:

1. How many codewords of weight 7 does C have?
2. Determine a set M and polynomials $\sigma(X, a)$ such that $\sigma(X, a)$ has as zeros the locators of a codeword of weight 7 is and only if $a \in M$.
3. Prove that $\sigma(X, \alpha^i) = \sigma(\alpha^{13i}X, 1)$. What does this show?

We will now use code C to decode a word that is a transmitted codeword in which errors have occured. First we choose a codeword in C.

Exercise 6.3 Pick your favorite polynomial $m(X) \in \mathbb{F}_2[X]$ of degree at most 4 and encode it by computing

$$c(X) = m(X)g(X) \bmod (X^{15} + 1).$$

Now choose a random binary error vector $\mathbf{e}$ of weight at most 3 and compute the word $\mathbf{r}$ that is received at the other end of the channel:

$$\mathbf{r} = \mathbf{c} + \mathbf{e}.$$

We will decode the received codeword using all the algorithms we have discussed. If you want you can exchange the word $\mathbf{r}$ you ave chosen with someone else and try to decode the word "he/she sent you".

Exercise 6.4 Compute the syndromes $s_1 = r(\alpha)$, $s_3 = r(\alpha^3)$ and $s_5 = r(\alpha^5)$ and proceed with Algorithm **??**. You have to use a computer algebra package that can compute Gröbner bases over $\mathbb{F}_{16}$. Compare your result with the codeword that was sent.

Now compute all syndromes $s_1, s_2, \ldots, s_6$ and define the syndrome polynomial

$$S(Z) = s_1 + s_2 Z + s_3 Z^2 + s_4 Z^3 + s_5 Z^4 + s_6 Z^5.$$

Set

$$\sigma(Z) = 1 + \sigma_1 Z + \sigma_2 Z^2 + \sigma_3 Z^3.$$

We want to determine the σ_i such that $\sigma(Z)$ has as its zeros the reciprocals of the error positions of $\mathbf{e}$. We have seen two algorithms for this.

Exercise 6.5 Apply Sugiyama's algorithm to the situation here: compute the greatest common divisor of Z^6 and $S(Z)$ until the stop criterion of the algorithm is reached. Determine $\sigma(Z)$ from this and determine its zeros and thus the error positions. Compare your result with the codeword that was sent.

Exercise 6.6 Determine $\sigma(Z)$ by applying the Berlekamp-Massey algorithm. Again find the error locators and compare this with your result from the previous exercise.

If the number of errors that were made during transmission is equal to 3, we can use the formulas we found by one-step decoding.

Exercise 6.7 Lookup in Example **??** the formula corresponding to a 3-error correcting binary BCH code, substitute the syndromes you have computed, and determine the zeros and hence the error positions of the equation.