The minimum distance of some binary codes via the Newton's identities.

D. Augot [*] P. Charpin [†] N. Sendrier [†]

Abstract

In this paper, we give a natural way of deciding whether a given cyclic code contains a word of given weight. The method is based on the manipulation of the locators and of the locator polynomial of a codeword $\mathbf{x}$.

Because of the dimensions of the problem, we need to use a symbolic computation software, like Maple or Scratchpad II. The method can be ineffective when the length is too large.

The paper contains two parts :

In the first part we will present the main definitions and properties we need.

In the second part, we will explain how to use these properties, and, as illustration, we will prove the three following facts :

The dual of the BCH code of length 63 and designed distance 9 has true minimum distance 14 (which was already known).
The BCH code of length 1023 and designed distance 253 has minimum distance 253.
The cyclic codes of length $2^{11}-1, 2^{13}-1, 2^{17}-1$, with generator polynomial $m_1(x)$ and $m_7(x)$ have minimum distance 4 (see [5]).

1 Notation and properties.

1.1 Cyclic codes.

We use the following definition for cyclic codes :

Definition 1 *A primitive cyclic code C of length $n = 2^m - 1$ over $GF(2)$ is an ideal of the polynomial algebra $GF(2)[x]/(x^n-1)$. The roots of its generator polynomial are called the zeros of C. The code C is characterized by its defining set $I(C)$:*

$$I(C) = \{i \in [0..n-1] \mid \alpha^i \textit{ is a zero of } C\} \tag{1}$$

where α is a n^{th} root of unity in $GF(2^m)$.

[*]Université Paris 6, UFR d'Informatique, LITP, 2 pl. Jussieu, 75251 Paris CEDEX 05, FRANCE
[†]INRIA, Domaine de Voluceau, Rocquencourt, BP 105, 78153 Le Chesnay Cedex, FRANCE

We denote by $cl(s)$ the cyclotomic class of 2 mod n, containing s :

$$cl(s) = \{s, 2s, 2^2 s \ldots, 2^{m-1} s \bmod n\} \tag{2}$$

If α^i is a zero of the code C, then $(\alpha^i)^2$ is also a zero of the code C. So we can see that $I(C)$ is the union of cyclotomic classes mod n.

As an example of a cyclic code, let us recall the definition of the BCH codes :

Definition 2 *The narrow-sense BCH code of designed distance δ is the cyclic code whose defining set is the union of the cyclotomic classes $cl(1), cl(2) \ldots cl(\delta - 1)$.*

It is well-known that the true minimum distance of a BCH code of designed distance δ is greater or equal than δ. This is the BCH bound :

Theorem 1 *Let C be a cyclic code with defining set $I(C)$. If $I(C)$ contains a sequence of $\delta - 1$ consecutive integers (0 is treated consecutive to $n-1$), then the minimum distance of C is greater or equal to δ.*

There exist many ways to find lower bounds for the minimum distance of a cyclic code. Van Lint and Wilson give an overview of these methods in [6]. In this paper we will also need the following bound, called the Hartmann-Tzeng bound ([4]) :

Theorem 2 *Let C be a cyclic code of length n over $GF(q)$ with defining set $I(C)$. Let β be a primitive n^{th} root of unity. If the defining set $I(C)$ contains the following roots :*

$$\{\beta^{l+i_1c_1+i_2c_2}\}\ i_1 = 0, 1 \ldots d_0 - 2,\ i_2 = 0, 1 \ldots s,\ \textit{where } gcd(n, c_1) = 1,\ gcd(n, c_2) < d_0, \tag{3}$$

then the minimum distance d of C satisfies $d \geq d_0 + s$.

In general, no method is known for finding the true minimum distance of a given cyclic code. Our approach is to find properties of a given cyclic code by using equations in $GF(2^m)$, and by doing effective computations in $GF(2^m)$.

1.2 Locators, locator polynomial of a word

All the notions introduced here can be found in [3].

Definition 3 *Let α be a n^{th} root of unity in $GF(2^m)$, let $\mathbf{x}$ be a word of length n and weight w, $\mathbf{x} = (x_0, x_1 \ldots, x_{n-1})$. The locators of $\mathbf{x}$ are the $X_1, X_2 \ldots, X_w$, defined as follows :*

$$X_i = \alpha^{k_i} \quad \textit{where} \quad x_{k_i} \neq 0 \tag{4}$$

We also define the locator polynomial of $\mathbf{x}$:

The locator polynomial of $\mathbf{x}$ is the following polynomial $\sigma_x(Z)$:

$$\sigma_x(Z) = \prod_{i=1}^{w} (1 - X_i Z) = \sum_{i=0}^{i=w} \sigma_i Z^i\ , \tag{5}$$

where the σ_i are the elementary symmetric functions of the X_i :

$$\sigma_i = \sum_{1 \leq k_1 < k_2 \ldots < k_i \leq w} X_{k_1} X_{k_2} \cdots X_{k_i} \tag{6}$$

We also recall the *power sum symmetric functions* :

Definition 4 *The power sum symmetric functions A_k of the locators of* $\mathbf{x}$ *are :*

$$A_k(X_1, X_2, \dots, X_w) = A_k = \sum_{i=1}^{w} X_i^k \quad , \forall k \in [0..n].$$

In accordance with the definition of cyclic codes, we have the following property :

Proposition 1 *Let C be a cyclic code with defining set $I(C)$ and* $\mathbf{x}$ *a word of length n. Then $\mathbf{x} \in C$ if and only if :*

$$A_k = 0 \text{ for } k \in I(C). \tag{7}$$

The following identities show how the A_i's are related to the σ_i's.

Proposition 2 *Let $X_1 \dots X_w$ be w indeterminates in a ring K, σ_i their elementary symmetric functions, A_i their power sum symmetric functions. Then the following identities hold :*

$$\begin{cases} r \leq w, & (eq_r): \quad A_r + A_{r-1}\sigma_1 + \dots + A_1\sigma_{r-1} + r\sigma_r = 0 \\ \\ r > w, & (eq_r): \quad A_r + A_{r-1}\sigma_1 + \dots + A_{r-w}\sigma_w = 0 \end{cases}$$

These identities are called the Newton's identities.

2 Presentation of the method

Let C be a cyclic code of length $n = 2^m - 1$ with defining set $I(C)$, let $\mathbf{x}$ be a codeword of C, let w be the weight of $\mathbf{x}$.

From the preceding part, we can state the following facts :

Let $X_1, X_2 \dots, X_w$ be the locators of $\mathbf{x}$, $A_1, A_2 \dots, A_n$ be the power sum symmetric functions of the X_i's. Then $A_i = 0$ for $i \in I(C)$.

The locator polynomial of $\mathbf{x}$, $\sigma_x(Z)$ splits over $GF(2^m)$.

The A_i's and the σ_i's are related by the Newton's identities.

So to find the codeword of weight w, we do the following :

1. Write the Newton's identities for a weight w with generic A_i's and σ_i's, using the fact that $A_i = 0$ for $i \in I(C)$.

2. Solve the system given by these equations, in order to obtain the σ_i's in terms of the A_i's.

3. Construct the locator polynomial corresponding to these σ_i's and test if it splits over $GF(2^m)$.

If we can find such a locator polynomial, then with the locators we can construct a word of weight w.

If there is a failure at any step of the method then we know that C contains no word of weight w.

We will show three ways of using this method.

2.1 Finding a contradiction in the Newton's Identities.

We want to find the minimum distance of the dual of the BCH code of designed distance 9 and length 63.

The defining set of this code C is $I(C)$:

$$0, cl(1), cl(3), cl(5), cl(9), cl(11), cl(13), cl(21), cl(27). \tag{8}$$

So the BCH bound gives $\delta \geq 8$ (As well as the Carlitz-Uchiyama bound).

Let us suppose there exists a codeword $\mathbf{x}$ of weight 8. Then its power sum symmetric functions satisfy :

$$A_0 = A_1 = A_3 = A_5 = A_9 = A_{11} = A_{13} = A_{21} = A_{27} = 0, \tag{9}$$

and we must have $A_7 \neq 0$ (If not then, by the BCH bound, the weight of $\mathbf{x}$ would be greater than 16.).

Now we can write down the Newton's identities, one by one :

$$\begin{array}{lrl}
(eq_7) & A_7 + \sigma_7 & = 0 \\
(eq_8) & 0 & = 0 \\
(eq_9) & A_7\sigma_2 & = 0 \\
(eq_{10}) & 0 & = 0 \\
(eq_{11}) & A_7\sigma_4 & = 0 \\
(eq_{12}) & 0 & = 0 \\
(eq_{13}) & A_7\sigma_6 & = 0 \\
(eq_{14}) & {A_7}^2 + A_7\sigma_7 & = 0 \\
(eq_{15}) & A_{15} + A_7\sigma_8 & = 0 \\
(eq_{16}) & {A_7}^2\sigma_2 & = 0 \\
(eq_{17}) & A_{15}\sigma_2 & = 0 \\
(eq_{18}) & {A_7}^2\sigma_4 & = 0 \\
(eq_{19}) & A_{15}\sigma_4 & = 0 \\
(eq_{20}) & {A_7}^2\sigma_6 & = 0 \\
(eq_{21}) & A_{15}\sigma_6 + {A_7}^2\sigma_7 & = 0
\end{array}$$

The contradiction appears when we see that A_7 supposed to be non zero has to be null :

$$\begin{array}{lcc}
(eq_7) & \Rightarrow & \sigma_7 = A_7 \neq 0 \\
(eq_{13}) & \Rightarrow & \sigma_6 = 0 \\
(eq_{21}) & \Rightarrow & (A_7)^3 = 0
\end{array}$$

Because there are no σ_i solutions of the Newton's identities, this proves that there can be no locator polynomial of a codeword of weight 8 in C. So there is no codeword of weight 8. The bound for C is raised, and we can try the method for a word of weight 10.

Using several times this method we proved that C contains no codewords of weight less than 14. Then we found a word of weight 14, which is an idempotent of C. So the true minimum distance of C is 14.

How to find an idempotent is presented in the next subsection :

2.2 Finding idempotents in a cyclic code.

We want to find the minimum distance of the BCH code of length 1023 and designed distance 253. Let us suppose there exists a codeword $\mathbf{x}$ of weight 253. For the power sum symmetric functions of the locators of $\mathbf{x}$, we have :

$$A_1 = A_2 = \cdots = A_{252} = 0, \tag{10}$$

and :

$$A_{253} \neq 0 \tag{11}$$

(If A_{253} is equal to zero, then the weight of $\mathbf{x}$ is greater than 253 because of the BCH bound.)

Because the length is large, in order to symplify the problem, we first try to find a codeword $\mathbf{x}$ which is an idempotent. This implies (see [3]) :

$$\begin{aligned} &\Rightarrow \quad \forall k \ , \ A_k \in GF(2). \\ &\Rightarrow \qquad A_{253} = 1. \end{aligned} \tag{12}$$

So the computations become much simplier. Here we give a part of a Maple session, where we compute the A_i :

Initialization of the parameter for the programm :
length=1023, designed distance=253, weight=253.
> init(1023,253,253);
The representants of the cyclotomic classes which are not in the defining set of C are :

$$\{511, 495, 479, 447, 439, 383, 379, 375, 367, 363, 351, 347, 343, 341, 255\}$$

We try to find a solution for the particular case $A_{255} = 0$:
> $A_{255} := 0$;

$$A_{255} := 0$$

After computing the values of the σ_i in terms of the A_i, we have equations in terms of the A_i. With these equations, we can find the values of the A_i :

$$\begin{array}{lll}
eq_{507}: & A_{447} + A_{375} + A_{347} = 0 & \Rightarrow A_{447} := A_{347} + A_{375} \\
eq_{509}: & A_{383} + A_{351} = 0 & \Rightarrow A_{351} := A_{383} \\
eq_{511}: & A_{511} + A_{379} + A_{343} = 0 & \Rightarrow A_{343} := A_{511} + A_{379} \\
eq_{517}: & A_{341} + 1 = 0 & \Rightarrow A_{341} := 1 \\
eq_{519}: & A_{511} + A_{379} = 0 & \Rightarrow A_{511} := A_{379} \\
eq_{523}: & A_{347} = 0 & \Rightarrow A_{347} := 0 \\
eq_{527}: & A_{383} = 0 & \Rightarrow A_{383} := 0 \\
eq_{543}: & A_{367} = 0 & \Rightarrow A_{367} := 0 \\
eq_{551}: & A_{375} = 0 & \Rightarrow A_{375} := 0 \\
eq_{555}: & A_{379} = 0 & \Rightarrow A_{379} := 0 \\
eq_{571}: & A_{439} = 0 & \Rightarrow A_{439} := 0 \\
eq_{583}: & A_{363} + 1 = 0 & \Rightarrow A_{363} := 1 \\
eq_{611}: & A_{479} = 0 & \Rightarrow A_{479} := 0 \\
eq_{627}: & A_{495} + 1 = 0 & \Rightarrow A_{495} := 1
\end{array}$$

In a similar way we obtain a solution for the Newton's identities in the case $A_{255}=1$. These two solutions give us the following locator polynomials :

$$\boxed{A_{255}=0}$$

$$1+z^{66}+z^{88}+z^{110}+z^{132}+z^{198}+z^{242}+z^{253}$$

$$\boxed{A_{255}=1}$$

$$\begin{aligned}1&+z^{2}+z^{4}+z^{6}+z^{8}+z^{10}+z^{12}+z^{14}+z^{16}+z^{18}\\ &+z^{20}+z^{22}+z^{24}+z^{26}+z^{28}+z^{30}+z^{32}+z^{34}\\ &+z^{36}+z^{38}+z^{40}+z^{42}+z^{44}+z^{46}+z^{48}+z^{50}\\ &+z^{52}+z^{54}+z^{56}+z^{58}+z^{60}+z^{62}+z^{64}+z^{68}\\ &+z^{72}+z^{76}+z^{80}+z^{84}+z^{90}+z^{94}+z^{96}+z^{100}\\ &+z^{104}+z^{108}+z^{110}+z^{112}+z^{116}+z^{122}+z^{128}\\ &+z^{130}+z^{136}+z^{138}+z^{144}+z^{146}+z^{152}+z^{154}\\ &+z^{160}+z^{162}+z^{168}+z^{170}+z^{176}+z^{178}+z^{184}\\ &+z^{186}+z^{192}+z^{200}+z^{208}+z^{218}+z^{220}+z^{222}\\ &+z^{224}+z^{232}+z^{238}+z^{240}+z^{242}+z^{246}+z^{252}\\ &+z^{253}\end{aligned}$$

(Performed with Maple symbolic computation software.)

These polynomials factor over $GF(2)$ in distinct polynomials of degree 2, 5 or 10, which split over $GF(2^{10})$. So these locator polynomials have 253 distinct roots in $GF(2^{10})$. (Of course the factorization of these polynomials is also accomplished with Maple software.) There exist codewords of weight 253 in C ; in conclusion, the code C has true minimum distance 253.

2.3 Finding a locator polynomial by doing an exhaustive research.

We want to find the true minimum distance of the following codes :

let C_m be the binary primitive cyclic code of length 2^m-1 and zeros α^1 and α^7.

Van Lint and Wilson showed that C has minimum distance $\delta<5$, when $m\neq 5,11,13,17$ ([5]). Their demonstration is based on algebraic geometry theory, for they need to know deep algebraic properties of $GF(2^m)$.

In the case $m=5$, they proved that the minimum distance is five. So the remaining unsolved cases are : $m=11,13,17$.

We use our method to find a minimum weight codeword :

The defining set contains : $1,2,7,8$. So, the Hartmann-Tzeng bound shows that $d\geq 4$. ($d_0=3$, $s=1$, $l=1$, $c_1=1$, $c_2=7$.)

Let us suppose there exists a codeword $\mathbf{x}$ of C of weight 4. We associate to $\mathbf{x}$ its locator polynomial $\sigma(Z)$:

$$\sigma_{\mathbf{x}}(Z) = 1 + \sigma_1 Z + \sigma_2 Z^2 + \sigma_3 Z^3 + \sigma_4 Z^4 \ .$$

For the power sum symmetric functions, we have $A_1 = A_7 = 0$.

The Newton's Identities give :

$$\begin{array}{lcll} (eq_1) & : & A_1 + \sigma_1 = 0 & \Longrightarrow \ \sigma_1 = \hfill 0 \\ (eq_3) & : & A_3 + \sigma_3 = 0 & \Longrightarrow \ \sigma_3 = \hfill A_3 \\ (eq_5) & : & A_5 + A_3\sigma_2 = 0 & \Longrightarrow \ \sigma_2 = \ A_5/A_3 \\ (eq_7) & : & A_5\sigma_2 + A_3\sigma_4 = 0 & \Longrightarrow \ \sigma_4 = \hfill \sigma_2^2 \end{array}$$

Shifting the word by one position corresponds to multiplication of the locators by α. Because 3 and n are coprime we can shift the word in such a way that $A_3 = 1$. So we want to find a polynomial with the following form :

$$\sigma_x(Z) = 1 + A_5 Z^2 + Z^3 + A_5^2 Z^4 \ , \tag{13}$$

which satisfies the following condition :

$$\sigma_x(Z) \text{ has four different roots in } GF(2^m).$$

Because there is no explicit condition on the coefficients of a polynomial for its decomposition, our only solution is to make an exhaustive research on all the possible values of A_5, testing each time if $\sigma_x(Z)$ splits over $GF(2^m)$.

The test is the following : compute $Z^{2^m} \bmod \sigma_x(Z)$ and test if it is equal to Z. It only requires m repeated squaring operations of a polynomial modulus an other polynomial, which is of small degree (i.e. 4).

Using `Scratchpad II` computation software which is able to compute with polynomials with coefficients in an extension of $GF(2^m)$, we found a word of weight 4 in the three cases $m = 11, 13, 17$, at relative low cost. After doing the change of indeterminates $Z^2 \leftarrow A_5 Z^2$, we search for polynomials of the form :

$$\sigma_x(Z) = 1 + Z^2 + YZ^3 + Z^4, \tag{14}$$

where :

$$Y = A_5^{-\frac{3}{2}}$$

because less operations in finite field are needed for computing these polynomials.

Here are the locators we found in the three cases $m = 11$, $m = 13$, $m = 17$:

$$\boxed{m = 11}$$

$$GF(2^{11}) = GF(2)[X]/(X^{11} + X^2 + 1) \ , \ u = \overline{X} \bmod (X^{11} + X^2 + 1)$$

(In the three cases we have $\alpha = \overline{X}$.)

$$\begin{aligned} u^{10} + u^8 + u^7 + u^6 + u^2 + u + 1 &= \alpha^{660} \\ u^9 + u^3 + u &= \alpha^{487} \\ u^9 + u^3 + 1 &= \alpha^{1769} \\ u^{10} + u^8 + u^7 + u^6 + u^2 &= \alpha^{1178} \end{aligned}$$

So the polynomial $\mathbf{x}$ in $GF(2)[X]/(X^{11}-1)$ is :

$$X^{487}+X^{660}+X^{1178}+X^{1769}$$

Then we can verify that α^1 and α^7 are zeros of $\mathbf{x}$:

$$(\alpha^1)^{660}+(\alpha^1)^{487}+(\alpha^1)^{1769}+(\alpha^1)^{1178}=0 \tag{15}$$

$$(\alpha^7)^{660}+(\alpha^7)^{487}+(\alpha^7)^{1769}+(\alpha^7)^{1178}=0 \tag{16}$$

$$\boxed{m=13}$$

$$GF(2^{13})=GF(2)[X]/(X^{13}+X^4+X^3+X+1)\ ,\ u=\overline{X} \bmod (X^{13}+X^4+X^3+X+1)$$

$$\begin{aligned} 1 &= \alpha^0 \\ u^{12}+u^6+u^5+u^4+1 &= \alpha^{6399} \\ u^{12}+u^{10}+u^8+u^7+u^6+u^3+u &= \alpha^{2735} \\ u^{10}+u^8+u^7+u^5+u^4+u^3+u &= \alpha^{6454} \end{aligned}$$

$$\mathbf{x}=X^0+X^{6399}+X^{2735}+X^{6454}$$

And we can verify that $\mathbf{x}$ is in C :

$$(\alpha^1)^0+(\alpha^1)^{6399}+(\alpha^1)^{2735}+(\alpha^1)^{6454}=0 \tag{17}$$

$$(\alpha^7)^0+(\alpha^7)^{6399}+(\alpha^7)^{2735}+(\alpha^7)^{6454}=0 \tag{18}$$

$$\boxed{m=17}$$

$$GF(2^{17})=GF(2)[X]/(X^{17}+X^3+1)\ ,\ u=\overline{X} \bmod (X^{13}+X^3+1)$$

$$\begin{aligned} u^{16}+u^{14}+u^{13}+u^{10}+u^8+u^7+u^3+u &= \alpha^{124733} \\ u^{16}+u^{15}+u^{13}+u^{12}+u^{11}+u^{10}+u^8+u^6+u^5+u^3 &= \alpha^{58930} \\ u^{16}+u^{12}+u^9+u^5+u^4+u^2 &= \alpha^{88726} \\ u^{16}+u^{15}+u^{14}+u^{11}+u^9+u^7+u^6+u^4+u^2+u &= \alpha^{120824} \end{aligned}$$

$$\mathbf{x}=X^{124733}+X^{58930}+X^{88726}+X^{120824}$$

And we can again verify :

$$(\alpha^1)^{124733}+(\alpha^1)^{58930}+(\alpha^1)^{88726}+(\alpha^1)^{120824}=0 \tag{19}$$

$$(\alpha^7)^{124733} + (\alpha^7)^{58930} + (\alpha^7)^{88726} + (\alpha^7)^{120824} = 0 \tag{20}$$

So in these three cases, the minimum distance is 4.

3 Conclusion

We saw how the use of the Newton's identities is helpful for studying the minimum weight codewords of cyclic codes. Of course, we need to use a symbolic computation software for the manipulation of these identities.

With this method, we proved that the minimum distances of the two BCH codes of length 255 and designed distance 59 and 61 (See [2]) are 61 and 63 respectively. We also found a general property of the minimum weight codewords of the BCH codes of length $2^m - 1$ and designed distance $2^{m-2} - 1$ (See [1]).

Acknowledgment

The authors wish to thank G. Norton for his careful and patient reading which improved the paper.

References

[1] D. Augot, P. Charpin, and N. Sendrier. Studying the locator polynomials of minimum weight codewords of BCH codes. *submitted.*

[2] G. Cohen. On the minimum distance of some BCH codes. *IEEE Transaction on Information Theory*, 26, 1980.

[3] F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error Correcting Codes.* North-Holland, 1986.

[4] J.H. van Lint. *Coding Theory.* Springer-Verlag, 1971.

[5] J.H. van Lint and R.M. Wilson. Binary cyclic codes generated by $m_1 m_7$. *IEEE Transaction on Information Theory*, 32(2):283, March 1986.

[6] J.H. van Lint and R.M. Wilson. On the minimum distance of cyclic codes. *IEEE Transaction on Information Theory*, 32(1):23, January 1986.