Studying the locator polynomials of minimum weight codewords of BCH codes.

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

Abstract

We consider only primitive binary cyclic codes of length $n = 2^m - 1$. A BCH-code with designed distance δ is denoted $B(n, \delta)$. A BCH-code is always a *narrow-sense* BCH-code. A codeword is identified with its *locator polynomial*, whose coefficients are the symmetric functions of the locators. The definition of the code by its zeros-set involves some properties for the power sums of the locators. Moreover the symmetric functions and the power sums of the locators are related with the NEWTON*'s identities*. We first present an algebraic point of view in order to prove or infirm the existence of words of a given weight in a code. The main tool is a symbolic computation software in exploring the NEWTON's identities. Our principal result is the true minimum distance of some BCH-codes of length 255 and 511, which were not known.
In a second part, we study the codes $B(n, 2^h - 1)$, $h \in [3, m-2]$. We prove that the set of the minimum weight codewords of the BCH-code $B(n, 2^{m-2} - 1)$ equals the set of the minimum weight codewords of the punctured Reed-Muller code of length n and order 2, for any m. We give some Corollaries of this result.

[*]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

1 Introduction

In this paper, we deal with primitive binary cyclic codes. We are going to introduce a method for finding the true minimum distance of these codes.

We will first recall usual definitions in section **2**, as they are introduced in [10]. Our aim is to have a algebraic approach of the codewords in a cyclic code, which are studied through their locator polynomial. We describe the Newton's identities which allow us to study the properties of the locator polynomial of a codeword.

In section **3**, we will show how to use the Newton's identities. In fact we explore the identities in an progressive manner, using a symbolic computation software. We have two strategic options : trying to establish a contradiction to the existence of solutions to the identities ; or trying to find an effective solution for the identities. This method enables us to complete the table of the minimum distance of the BCH codes in length 255, and to progress in the table of BCH codes in length 511. However the proofs are long and are given in the appendices **A, B and C**.

In section **4** we give a description of the set of the minimum weight codewords of the BCH codes of length $2^m - 1$ and designed distance $2^{m-2} - 1$ (Theorem 6). We prove that the locator polynomials of such codewords are, in fact, linearized polynomials. We obtain this result by studying the Newton's Identities associated to the minimum weight codewords of the BCH-codes of designed distance $2^h - 1$, $h \in [2, m-1]$. Some properties yield a complete characterization when $h = m - 2$. When $h \neq m - 2$, our proof involves an algorithm constructing cyclic codes whose minimum weight codewords have linearized locator polynomials.

2 Presentation and notations

In this whole chapter we recall the usual conventions and notations used in [10].

2.1 The BCH codes and their minimum distance

We denote by $GF(q)$ the Galois Field of order q, where $q = 2^m$ and by α a primitive n-root of unity in $GF(q)$. Any cyclic code C of length n can be defined by its *generator polynomial* whose roots are called the zeros of the code C. Thus we say that the defining set of C is the set :

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

We denote by $cl(s)$ the cyclotomic class of s modulo n :

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

If α^i is a zero of C then α^{2i} is also a zero of C, so we can see that $I(C)$ is a reunion of cyclotomic classes $cl(s)$.

Thus we can define the primitive narrow-sense BCH of length n of designed distance δ, denoted by $B(n, \delta)$, as the cyclic code of length n whose defining set is the union of the cyclotomic classes $cl(1), cl(2) \ldots cl(\delta - 1)$. This terminology of "designed distance" is used because of the well known BCH-bound theorem :

Theorem 1 *If the defining set of the cyclic code C contains a set of $\delta - 1$ consecutive integers (0 is treated consecutive to n-1), then the minimum distance of C is at least δ.*

So the code $B(n, \delta)$ has minimum distance at least δ.

But one will not be content with such a result. In general the designed distance is equal to the minimum distance, but we have no way to know systematically the true minimum distance.

Of course there exists many other bounds for cyclic codes (J.H. van Lint deeply treats the subject in [12]), but still these are bounds and it is a difficult problem to find the true minimum distance of a given BCH code, as soon as the length increases.

The problem encountered in finding the true minimum distance is to work with the real structure of the finite field $GF(q)$, which deeply influences the properties of cyclic codes, while bounds obtained with the properties of the defining set of cyclic codes do not reflect the underlying algebraic structure of $GF(q)$.

2.2 Mattson-Solomon polynomial and locator polynomial

Definition 1 *The Mattson-Solomon polynomial of the word $\mathbf{x} = (x_0, x_1 \ldots x_{n-1})$ is the polynomial of $GF(q)$:*

$$A(z) = \sum_{i=1}^{i=n} A_i z^{n-i} \tag{3}$$

where

$$A_i = \mathbf{x}(\alpha^i) = \sum_{j=0}^{j=n-1} x_j \alpha^{ij} \tag{4}$$

Remark :

- $A_{2i \bmod n} = A_i^2$
- $A_{i+n} = A_i$

So there is only one significant A_i for every cyclotomic class.

Definition 2 *The locator polynomial $\sigma(Z)$ of a word $\mathbf{x}$ is the following polynomial :*

$$\sigma(Z) = \prod_{i=1}^{i=w} (1 - X_i Z) \tag{5}$$

where the X_i are the elements of $GF(q)$ which are not zeros of the Mattson-Solomon polynomial of $\mathbf{x}$. They are called the locators of $\mathbf{x}$.

Definition 3 *The elementary symmetric functions of the locators* $X_1, X_2 \dots X_w$ *are the* σ_i *:*

$$\begin{array}{ll} 0 < i \leq w & \sigma_i = (-1)^i \sum_{1 \leq k_1 < k_2 \cdots < k_i \leq w} X_{k_1} X_{k_2} \cdots X_{k_i} \\ i = 0 & \sigma_0 = 1 \end{array}$$

And we have :

$$\sigma(Z) = \sum_{i=0}^{i=w} \sigma_i Z^i \tag{6}$$

In other words, the zeros of the locator polynomial are the locations of the non zero coordinates of $\mathbf{x}$, since $A(\alpha^i) = a_i$, thanks to the inversion formula ([10] p.240).

In case of binary codes, the notion of localisators becomes very interesting , since the binary words can be identified by their locators, and so by their locator polynomial.

We have the following property :

Proposition 1 *Let* $\mathbf{x}$ *a word of length* n *of weight* w*, with locators* $X_1, X_2 \dots X_w$*. Then* $\mathbf{x}$ *is in the cyclic code of defining set* $\{\alpha^{i_1}, \alpha^{i_2}, \dots \alpha^{i_l}\}$ *if and only if the following power sum symmetric functions of its locators are zeros :*

$$A_{i_1} = A_{i_2} = \cdots = A_{i_l} = 0 \tag{7}$$

Recall that the k^{th} *power sum symmetric function of* $X_1 \dots X_w$ *is :*

$$A_k = \sum_{i=1}^{i=w} X_i^k \tag{8}$$

and is the k^{th} *coefficient of the Mattson-Solomon polynomial of* $\mathbf{x}$*.*

The followings relations known as the NEWTON's *identities* allow us to study the elementary symmetric functions, knowing the power sum symmetric functions.

Proposition 2 *Let* $X_1, X_2 \dots X_w$ *be indeterminates over a field* K*,* σ_i *the elementary symmetric functions of the* X_i*,* A_i *the power sum symmetric functions of the* X_i*. Then we have the following relations :*

$$\begin{array}{lll} i \leq w, & I_r : & A_r + \sum_{i=1}^{i=r-1} A_{r-i}\sigma_i + r\sigma_r = 0 \\ i > w, & I_r : & A_r + \sum_{i=1}^{i=w} A_{r-i}\sigma_i = 0 \end{array} \tag{9}$$

2.3 The locator polynomial and BCH codes

From the NEWTON's identities, we have the following result ([10] Ch. 9 Lemma 4 p.260) :

Lemma 1 *Let*

$$\sigma(Z) = \sum_{i=0}^{i=w} \sigma_i Z^i \tag{10}$$

be a polynomial over $GF(2^m)$*. Then* $\sigma(Z)$ *is the locator polynomial of a codeword* $\mathbf{x}$ *of* $B(n, \delta)$ *if and only if :*

(i) $\sigma(Z)$ *divides* $Z^n - 1$.

(ii) $i \in [1, \delta - 1]$, *i odd* $\Rightarrow \sigma_i = 0$.

So we can try to find the true minimum distance of a $B(n, \delta)$ code by finding locator polynomials which satisfy conditions *(i)* and *(ii)* of lemma 1.

2.4 The codes $B(n, 2^k - 1)$ and the linearized polynomials

Definition 4 *Let $l(Z)$ be a polynomial over $GF(2^m)$, $l(Z)$ is a linearized polynomial if and only if :*

$$l(Z) = \sum_{i=0}^{i=l} a_l Z^{2^l} \tag{11}$$

The interesting point about linearized polynomial is the following proposition ([10] Ch. 4 p.119) :

Proposition 3 *$l(Z) \in GF(2^m)[Z]$ is a linearized polynomial if and only its zeros (eventually in an extension of $GF(2^m)$) forms a vector space over $GF(2)$.*

Now we can prove that the codes $B(n, \delta = 2^k - 1)$ have true minimum distance δ, following steps **1 2 3** :

- **1** Let H be a k-dimensionnal subspace of $GF(2^m)$ over $GF(2)$.
- **2** Then the polynomial : $l(Z) = \prod_{\mathbf{z} \in H}(Z - \mathbf{z})$ is a linearized polynomial.
- **3** It is easy to check that the polynomial $\sigma(Z) = \prod_{\mathbf{y} \in H \; \mathbf{y} \neq 0}(1 - \mathbf{y}Z)$ satisfies conditions *(i)* and *(ii)* of lemma 1.

Definition 5 *The punctured Reed-Muller code of length n of order k denoted by $\mathcal{R}(k, m)$ is the cyclic code of length $2^m - 1$ with the following defining set :*

$$I(\mathcal{R}(k, m)) = \{i \in [0..n-1] \mid w_2(i) \leq m - k\} \tag{12}$$

where :

$w_2(i)$ is the weight of the binary representation of i.

It is well known that the locators of any minimum weight codewords of the punctured Reed-Muller code of length $2^m - 1$ and order k, plus zero, forms a k-dimensionnal $GF(2)$-subspace. So their locator polynomials have the following form :

$$\sigma(Z) = \sum_{i=0}^{i=k} \sigma_{2^k - 2^i} Z^{2^k - 2^i} \tag{13}$$

In section **4**, we will use such a characterization of the minimum weight codewords of codes $\mathcal{R}(k, m)$.

3 The minimum distance of some BCH codes

Let C be any cyclic code of length n. $GF(2^m)$ is the smallest field containing the n^{th} roots of unity.

We consider the Newton's identities (9) written:

- for a weight w: that is for w locators $X_1, X_2, \ldots, X_w$.
- for a cyclic code C: for all i in the defining set of C, A_i is substituted by 0.

We call this set of equations, the *Newton's identities for the code C and for the weight w.*

We call *solution* of this system, a set of A_i's and σ_i's that verify these identities, and such that the polynomial $\sigma(z) = \sum_{i=0}^{w} \sigma_i z^i$ is square-free and splits in $GF(2^m)$.

Thus, the existence of solutions to the Newton's identities for a code C and a weight w is equivalent to the existence of codewords of weight w in C.

We therefore have two ways for exploring the identities:

- either we prove the absence of solution, so there is no codeword of this weight in the code,
- either we find a solution, and this solution gives us a codeword of the given weight.

We use a symbolic computation software to make this exploration, this enables us to manipulate the very large equations in their most general form (some of the biggest equations have hundreds of terms). The method we use in both cases can roughly be described as follows:

1. We write the Newton's identities for a given code and a given weight.
2. We introduce in the equations all the simplifications due to the kind of exploration we are about to do.
3. We examine the equations one after another, trying either to find the expression of an indeterminate depending on the others, either to find a (simple) necessary condition on a small number of indeterminates.

Up to now we are not able to make this exploration in a fully automatic manner, it is necessary to have a user interface to make the proper choice at the critical stages of the research. There are many possible decisions at step 3., including the decision to discard a too large equation, and it is difficult to make this choice efficiently within a program.

However we are able to determine empirically a program able to make most of the choices automatically.

We will use the following properties of the A_i's:

- $A_i^2 = A_{2i}$ and $A_{i+n} = A_i$, so there is exactly one significant A_i for each cyclotomic class.
- $A_i^{2^{m'}} = A_i$ where m' is the cardinal of the cyclotomic class of i (this is a consequence of the previous property).

- If a codeword is shifted each A_i is multiplied by α^i where α is the n^{th} root of unity choosen for the definition of the code. So, since $A_w \neq 0$, if n and w are relatively prime one can suppose that $A_w = 1$.

3.1 The minimum distance is known for all narrow-sense primitive binary BCH codes of length 255

Theorem 2 *All the narrow-sense primitive binary BCH codes of length 255 have their minimum distance equal to their designed distance except:*

- $B(255, 61)$ *which has minimum distance 63,*
- $B(255, 59)$ *which has minimum distance 61.*

Proof From [3, 4, 5, 10], we know that all narrow-sense primitive BCH codes of length 255 reach the BCH bound except $B(255, 61)$ and $B(255, 59)$.

For both of these codes we are able to produce words of weight $\delta + 2$. Indeed:

- $B(255, 61) \supset B(255, 63)$, and the latter code has minimum weight 63,
- for $B(255, 59)$, J-L. Dornstetter gives in [4] a word of weight 61.

Since the minimum distance of primitive BCH codes is odd, all we have to prove is that there are no codewords of weight 61 (*resp.* 59) in the code $B(255, 61)$ (*resp.* $B(255, 59)$). These two proofs were issued by our program in MAPLE, and are given in Annex A and Annex B. □

3.2 The minimum distance is known for most narrow-sense primitive binary BCH codes of length 511

We found a code whose minimum distance is over the BCH bound:

Theorem 3 *The code* $B(511, 123)$ *has minimum distance* $d = 127$.

Proof **(i)** $B(511, 123)$ is included in the punctured Reed-Muller code $\mathcal{R}(4, 9)$ (cf. Def. 5), and so has no codeword of weight 125, since $125 \equiv 1 \bmod 4$ [10, Cor. 13, page 447].

(ii) $B(511, 127) \subset B(511, 123)$, and $B(511, 127)$ reaches the BCH bound.

From **(i)** and **(ii)** we deduce easily that the minimum distance of $B(511, 123)$ is 123 or 127.

We show in Annex C that there is no word of weight 123. □

For codes of length 511 we also made an other kind of research from the Newton's identities: finding particular solutions by restricting the field of research. We introduced the following simplifications in the equations: all the A_i's and σ_i's are equal to 0 or 1. From the following lemma, this is exactly looking for the idempotents of given weight.

Definition 6 *The support of a word* $\mathbf{x} \in GF(q)^n$ *is the set of its positions different from zero. We denote it* $\mathrm{supp}(\mathbf{x})$*.*

Lemma 2 *Let* C *be a binary cyclic code of length* n*, and let* $GF(2^m)$ *be the smallest field containing a* n^{th} *root of unity.*

Let $\mathbf{x}$ *be a word of* C*, the following assertions are equivalent :*

(i) $\mathbf{x}$ *is an idempotent*

(ii) *the support of* $\mathbf{x}$ *is the union of cyclotomic classes (in* $GF(2^m)$*)*

(iii) *the coefficients of the locator polynomial of* $\mathbf{x}$ *(the* σ_i*'s) are in* $GF(2)$

(iv) *the power sum symmetric functions of* $\mathbf{x}$ *(the* A_i*'s) are in* $GF(2)$

Proof **(i)⇒(ii)** we have $\mathbf{x} = \mathbf{x}^2$. For any i :

$$i \in \mathrm{supp}(\mathbf{x}) \Rightarrow 2i \in \mathrm{supp}(\mathbf{x^2}) = \mathrm{supp}(\mathbf{x}).$$

So if $i \in \mathrm{supp}(\mathbf{x})$ then $cl(i) \subset \mathrm{supp}(\mathbf{x})$.

(ii)⇒(iii) The roots of the locator polynomial $\sigma(z)$ are the inverses of the locators, so the set of the roots is the union of cyclotomic classes and therefore $\sigma(z) \in GF(2)[z]$.

(iii)⇒(iv) If the σ_i's are given and are in $GF(2)$, then by induction, using the Newton's identities, all the A_i's are in $GF(2)$.

(iv)⇒(i) Let A be the Mattson-Solomon polynomial of $\mathbf{x}$, we have [10, Th. 22, page 240] :

$$\mathbf{x^2} = \mathbf{x} \text{ (as polynomial)} \Leftrightarrow A * A = A \text{ (component wise product).}$$

Since $A_j^2 = A_j$ for all j, we have $A * A = A$, and thus $\mathbf{x^2} = \mathbf{x}$.

□

This lemma is useful for two things : first it gives a way to find the idempotents from the Newton's identities, and it also gives us a way to describe very simply an idempotent by giving its support as union of cyclotomic classes.

We are able to find idempotents of given weight in some codes, for this research we give values in $GF(2)$ to some of the non-zero A_i's (8 of them for instance), and then the set of equations usualy becomes easy to solve. It is possible to implement this exploration in a fully automatic manner.

Theorem 4 *The code* $B(511, \delta)$ *contains idempotents of weight* δ *or* $\delta + 1$ *for :*

$$\delta = 19, 39, 45, 53, 57, 79, 83, 91, 103.$$

Proof We look for codewords with power sum symmetric functions in $GF(2)$. From Lemma 2, these words are idempotents, and they are fully described by the cyclotomic classes partitionning their supports.

We give here for a designed distance δ the support of a codeword $\mathbf{x}$ of weight δ or $\delta + 1$:

$$
\begin{array}{rl}
\delta = 19,\ \omega(\mathbf{x}) = 19, & \mathrm{supp}(\mathbf{x}) = cl(0) \cup cl(23) \cup cl(91) \\
\delta = 39,\ \omega(\mathbf{x}) = 39, & \mathrm{supp}(\mathbf{x}) = cl(63) \cup cl(87) \cup cl(117) \cup cl(127) \cup cl(219) \\
\delta = 45,\ \omega(\mathbf{x}) = 45, & \mathrm{supp}(\mathbf{x}) = cl(17) \cup cl(37) \cup cl(57) \cup cl(93) \cup cl(103) \\
\delta = 53,\ \omega(\mathbf{x}) = 54, & \mathrm{supp}(\mathbf{x}) = cl(17) \cup cl(31) \cup cl(41) \cup cl(45) \cup cl(103) \cup cl(117) \\
\delta = 57,\ \omega(\mathbf{x}) = 57, & \mathrm{supp}(\mathbf{x}) = cl(29) \cup cl(43) \cup cl(51) \cup cl(55) \cup cl(61) \cup cl(63) \\
 & \quad \cup\, cl(219) \\
\delta = 79,\ \omega(\mathbf{x}) = 79, & \mathrm{supp}(\mathbf{x}) = cl(0) \cup cl(3) \cup cl(13) \cup cl(39) \cup cl(41) \cup cl(61) \cup cl(73) \\
 & \quad \cup\, cl(77) \cup cl(107) \cup cl(117) \cup cl(219) \\
\delta = 83,\ \omega(\mathbf{x}) = 84, & \mathrm{supp}(\mathbf{x}) = cl(11) \cup cl(15) \cup cl(23) \cup cl(43) \cup cl(53) \cup cl(79) \\
 & \quad \cup\, cl(123) \cup cl(183) \cup cl(191) \cup cl(219) \\
\delta = 91,\ \omega(\mathbf{x}) = 91, & \mathrm{supp}(\mathbf{x}) = cl(0) \cup cl(7) \cup cl(13) \cup cl(25) \cup cl(37) \cup cl(41) \cup cl(59) \\
 & \quad \cup\, cl(61) \cup cl(117) \cup cl(175) \cup cl(239) \\
\delta = 103,\ \omega(\mathbf{x}) = 103, & \mathrm{supp}(\mathbf{x}) = cl(0) \cup cl(7) \cup cl(13) \cup cl(19) \cup cl(27) \cup cl(31) \cup cl(87) \\
 & \quad \cup\, cl(91) \cup cl(95) \cup cl(191) \cup cl(219) \cup cl(223) \cup cl(255)
\end{array}
$$

Since the true minimum distance d is odd, showing a word of weight $\delta + 1$ is sufficient to prove that $d = \delta$. □

remarks:

- the weight of an idempotent cannot be any integer, this integer has to be a sum of cardinal of cyclotomic classes. For instance in $GF(512)$ we have one class with one element, 2 classes with 3, and 57 this 9. So an idempotent has a weight multiple of 9 plus 0, 1, 3, 4, 6 or 7 (each class can be used once). For instance 29 cannot be the weight of an idempotent.

- We didn't found an idempotent for every possible weight, however this is not surprising, the surprise is that we did found some. Since the set of idempotent and the set of minimum weigth words are (very) small, their intersection should have been empty most of the time.

Some other minimum distance are known for length 511. Table 1 gives a list of them as well as the way they were found. We try to give as reference the first author known to us which explicitly gives the code and its true minimum distance.

n	k	δ	d		in	n	k	δ	d		in
511	502	3	3		[6]	511	241	73	73		[11]
	493	5	5		[6]		238	75	≥ 75		—
	484	7	7		[6]		229	77	≥ 77		—
	475	9	9		**		220	79	79		*
	466	11	11		[6]		211	83	83		*
	457	13	13		[5]		202	85	≥ 85		—
	448	15	15		[6]		193	87	≥ 87		—
	439	17	17		**		184	91	91		*
	430	19	19		*		175	93	95	#	[9]
	421	21	21		[11]		166	95	95		[6]
	412	23	23		[6]		157	103	103		*
	403	25	25		[5]		148	107	≥ 107		—
	394	27	27		[6]		139	109	111	#	[9]
	385	29	≥ 29		—		130	111	111		[6]
	376	31	31		[6]		121	117	119	#	[9]
	367	35	35		[11]		112	119	119		[6]
	358	37	≥ 37		—		103	123	127	##	*
	349	39	39		*		94	125	127	#	[9]
	340	41	≥ 41		—		85	127	127		[6]
	331	43	≥ 43		—		76	171	171		**
	322	45	45		*		67	175	175		**
	313	47	47		[6]		58	183	183		**
	304	51	≥ 51		—		49	187	187		**
	295	53	53		*		40	191	191		[6]
	286	55	55		[6]		31	219	219		[11]
	277	57	57		*		28	223	223		[6]
	268	59	≥ 59		—		19	239	239		[6]
	259	61	≥ 61		—		10	255	255		[6]
	250	63	63		[6]						

$d = \delta + 2$
$d = \delta + 4$
* new result obtained by the Newton's identities
** new result obtained by an exhaustive research

Table 1: BCH codes of length 511

4 The minimum weight codewords of the BCH-codes $B(2^m-1, 2^h-1)$

We denote by $B(h)$, $h \in [2, m-1]$ the BCH-code of length 2^m-1 and designed distance 2^h-1. Since $B(h)$ contains the minimum weight codewords (*mwc*'s) of the punctured RM-code $\mathcal{R}(m-h, m)$, its minimum distance is exactly 2^h-1. (see in Section 2). However the whole set of the *mwc*'s of $B(h)$ is not known, except for the trivial cases:

$$B(2) = \mathcal{R}(m-2, m) \quad , \quad B(m-1) = \mathcal{R}(1, m) \quad \textit{and} \quad B(3) = \mathcal{R}(2, 5) \ .$$

Thus we suppose in general that:

$$h \in [3, m-2] \qquad \textit{and} \qquad m \ > 5 \ .$$

In this Section we want to give some answers to this question: is there a *mwc* of $B(h)$ which is not in $\mathcal{R}(m-h, m)$? On the other hand, it is natural to conjecture that for each h, there exists a cyclic code $C \neq \mathcal{R}(m-h, m)$, which is included in $B(h)$ and has for *mwc*'s the *mwc*'s of $\mathcal{R}(m-h, m)$.

Let C be a binary cyclic code of length $n = 2^m-1$. We denote by $Mw(C)$ the set of the *mwc*'s of C. We say that C *has the property* $(\mathrm{RM_h})$, $h \in [3, m-2]$, if and only if:

$(\mathrm{RM_h})$: $\quad \mathcal{R}(m-h, m) \subset C \subseteq B(h) \quad$ and $\quad Mw(C) = Mw(\mathcal{R}(m-h, m))$

— where the first inclusion is strict —.

We shall prove (cf. Theorem 6) that the codes $B(m-2)$ have the property $(\mathrm{RM_{m-2}})$. We obtain this result throughout an exploration of the Newton's identities written for any *mwc* of a code $B(h)$, $h \in [3, m-2]$; we study this general case and derive the result for $h = m-2$. Moreover we can then provide an algorithm constructing cyclic codes which have the property $(\mathrm{RM_h})$ for a given h.

Let $\mathbf{x}$ be a *mwc* of $B(h)$. We have seen that $\mathbf{x} \in \mathcal{R}(m-h, m)$ if and only if its locator polynomial has the form: $\sigma(Z) = \sum_{j=0}^{h} \sigma_{2^h-2^j} Z^{2^h-2^j}$(cf. (12)). Thus we have the following explanation of the property $(\mathrm{RM_h})$:

Theorem 5 *For each $h \in [2, m-1]$, define:*

$$J_h = \{\ 2^h - 2^j \mid j \in [0, h]\ \} \ . \tag{14}$$

Let $\mathbf{x}$ be a codeword of weight 2^h-1 and let $\sigma(Z) = \sum_{i=0}^{2^h-1} \sigma_i Z^i$ be the locator polynomial of $\mathbf{x}$. Then $\mathbf{x}$ is a codeword of $\mathcal{R}(m-h, m)$ if and only if $\sigma_i = 0$ for all $i \notin J_h$.

Note that $0 \in J_h$ and that $j \in J_h - \{0\}$ implies $j \geq 2^{h-1}$; recall the following property of J_h presented by Kasami and al.:

Lemma 3 *[8] Let $h \in [2, m-1]$, $i_0 = 2^h-1$ and $r \in [1, i_0[$. Then:*

1. *$r \notin J_h \implies \omega_2(r + i_0) < h$.*

2. $r \in J_h \implies \omega_2(r+i_0) = h.$

Let $S = [1, 2^m - 1]$. From now on we assume that any *mwc* $\mathbf{x}$ of $B(h)$ is defined by its locators $X_1, \ldots, X_{i_0}$. The corresponding power sum symmetric functions A_k, $k \in S$ and the elementary symmetric functions σ_r, $r \in [0, i_0]$ are related by the NEWTON's identities I_k, $k \in S$. By definition $\sigma_0 = 1$; since $\mathbf{x} \in B(h)$ we know that:

- $A_k = 0$, for $k \in [1, i_0[$;
- r odd and $r < i_0 \implies \sigma_r = 0.$
- A_{i_0} cannot be zero, since the minimum distance of $B(h)$ is exactly i_0.

Then the identities I_k are satisfied for $k < i_0$; the identity I_{i_0} yields $\sigma_{i_0} = A_{i_0}$. In accordance with Theorem 5, we shall try to prove the following hypothesis $\mathrm{H_r}$ by induction on r:

$\mathrm{H_r}$: $r \in [1, i_0[$ and $r \notin J_h \implies \sigma_r = 0$ and $A_{i_0+r} = 0.$

We know that $\mathrm{H_r}$ is true for r odd (cf. Lemma 1). Recall the form of the identity I_{i_0+r}:

$$I_{i_0+r} \; : \; A_{i_0+r} + \sum_{k=1}^{r} A_{i_0+r-k}\sigma_k = 0 \quad . \tag{15}$$

The following Lemma means that the code $B(h)$ has the property ($\mathrm{RM_h}$) if and only if $\mathrm{H_r}$ is true for all $r \in [2, i_0[$, $i_0 = 2^h - 1$. This result still holds for any cyclic code C which contains $\mathcal{R}(m-h, m)$ and is contained in $B(h)$.

Lemma 4 *r is even. Suppose that $\mathrm{H_{r'}}$ is true for all $r' \in [1, r[$. Then we have:*

$$I_{i_0+r} \; : \; A_{i_0+r} + A_{i_0}\sigma_r = 0 \quad .$$

Proof We examine the term $A_{i_0+r-k}\sigma_k$ in 15, for $k \in [1, r[$:

- if $k \notin J_h$ then $\mathrm{H_k}$ implies $\sigma_k = 0$;
- if $k \in J_h$ then $k \geq 2^{h-1}$. Hence $r - k < 2^{h-1}$, which means that $r - k$ is not in J_h. Applying $\mathrm{H_{r-k}}$, we obtain $A_{i_0+r-k} = 0$.

$\square$

Remark: We know that the locator polynomials of the *mwc*'s of $\mathcal{R}(m-h, m)$ satisfy $\sigma_i = 0$ for $i \notin J_h$. From Lemma 4 we obtain another property:

$$r \in J_h \implies \sigma_r = \frac{A_{i_0+r}}{A_{i_0}} \quad . \tag{16}$$

`Example 1`: *The BCH-codes of designed distance* 7 — i.e. $h=3$, $i_0=7$ and $J_3=\{0,4,6,7\}$—. Recall that the defining-sets of $\mathcal{R}(m-3,m)$ and $B(3)$ are respectively:

$$S_3=\{\ s\in S \mid \omega_2(s)<3\ \} \quad \textit{and} \quad I(B(3))=cl(1)\cup cl(3)\cup cl(5)\ .$$

Since $\sigma_r=0$ for r odd, the lemma 1 implies that $B(3)$ has the property (RM_3) if and only if $\sigma_2=0$; we have seen that H_1 is always true; from Lemma 2, $\sigma_2=0$ if and only if $A_9=0$. In other words: $B(3)$ has the property (RM_3) if and only if each *mwc* of $B(3)$ is such that $A_9=0$. *We conjecture that, in general,* $B(3)$ *has not the property (*RM_3*).* For $m\in\{6,7,8,9\}$, we have obtained (with a computer) a *mwc* of $B(3)$ which is not in $\mathcal{R}(m-3,m)$.

Let $\hat{T}=cl(9)\cup I(B(3))$. Since $\omega_2(9)=2$, then $\hat{T}\subset S_3$.Now we examine a code C whose defining-set T is such that $\hat{T}\subseteq T\subset S_3$, where the right inclusion is strict. Thus C contains $\mathcal{R}(m-3,m)$ and is contained in $I(B(3))$. Moreover each codeword of C is such that its power sum symmetric function A_9 equals zero. If $m\in\{6,7\}$, it is easy to see that $\hat{T}$ equals S_3. When $m>7$, 17 is in S_3 and not in $\hat{T}$. In conclusion:

1. Assume that $m>7$. Then a cyclic code C with defining-set T satisfying:
$$cl(1)\cup cl(3)\cup cl(5)\cup cl(9)\subseteq T\subset\{\ s\in S\mid\omega_2(s)<3\ \}\ ,$$
has the property (RM_3). Conversely, we conjecture that a code C which has the property (RM_3), satisfies the property above.
2. If $m\leq 7$, it is impossible to construct a code C which has the property (RM_3).

Now we will distinguish two cases: $r\leq 2^{h-1}$ and $r>2^{h-1}$.

Lemma 5 *Assume that* $r\in[2,2^{h-1}]$*,* r *even, and that* $\mathrm{H}_{r'}$ *is true for all* $r'<r$*. Then the identity* I_{2i_0+3r} *becomes:*

$$I_{2i_0+3r}\ :\ A_{2i_0+3r}+A^2_{i_0+r}\sigma_r+A_{i_0+3r}\sigma_{i_0}=0\ \ ,\ if\ r>\frac{i_0-1}{3} \tag{17}$$

and

$$I_{2i_0+3r}\ :\ A_{2i_0+3r}+A^2_{i_0+r}\sigma_r+A^2_{i_0}\sigma_{3r}+A_{i_0+3r}\sigma_{i_0}=0\ \ ,\ if\ r\leq\frac{i_0-1}{3} \tag{18}$$

Proof $i_0=2^h-1$. Note that $2i_0+3r<2^{h+1}+3.2^{h-1}<2^m-1$, since $h<m-1$. Then the identity I_{2i_0+3r} is defined. Its general form is:

$$I_{2i_0+3r}\ :\ A_{2i_0+3r}+\sum_{k=1}^{i_0-1}A_{2i_0+3r-k}\sigma_k+A_{i_0+3r}\sigma_{i_0}=0\ . \tag{19}$$

Suppose that $\mathrm{H}_{r'}$ is true for $r'<r$ and consider the term $A_{2i_0+3r-k}\sigma_k$. If k is odd, then $\sigma_k=0$. If k is even , let $r-k=2k'$; we have:

$$A_{2(i_0+r)+r-k}\sigma_k=A^2_{i_0+r+k'}\sigma_k\ \ ,\ k\in[1,i_0[\ .$$

Then

- $k' > 0 \;\Rightarrow\; k < r \;\Rightarrow\; \sigma_k = 0$, from $\mathrm{H_k}$ (k cannot be in J_h, since $r \leq 2^{h-1}$).
- $k' < 0$ and $r + k' \neq 0 \;\Rightarrow\; r + k' < r \;\Rightarrow\; A_{i_0+r+k'} = 0$ (if $r + k' > 0$ apply $\mathrm{H_{r+k'}}$ else $i_0 + r + k'$ is an element of the defining-set of $B(h)$).
- $r + k' = 0$ is obtained when it is possible to have $k = 3r$; since $r < i_0$, this condition implies $r \leq \frac{i_0-1}{3}$.

In conclusion, the identity I_{2i_0+3r} is reduced to (4) if $r > \frac{i_0-1}{3}$ and to (5) otherwise. □

Lemma 6 *r even and $i_0 = 2^h - 1$, $h \in [3, m-2]$. Assume that $r \in [2^{h-1}, i_0[$ and $r \notin J_h$; suppose that $\mathrm{H_{r'}}$ is true for all $r' < r$. Then the identity $I_{2(i_0+r)}$ becomes:*

$$I_{2(i_0+r)} \;:\; A^2_{i_0+r} + A_{i_0+2r}\sigma_{i_0} = 0 \quad . \tag{20}$$

Proof Note that $2i_0 + 2r \leq 4i_0 - 2 \leq 2^{h+2} - 6 < 2^m - 1$. Hence the identity I_{2i_0+2r} is defined. Its general form is:

$$I_{2(i_0+r)} \;:\; A^2_{i_0+r} + \sum_{k=1}^{i_0-1} A_{2(i_0+r)-k}\sigma_k + A_{i_0+2r}\sigma_{i_0} = 0 \; . \tag{21}$$

Suppose that $\mathrm{H_{r'}}$ is true for $r' < r$; consider for k even, the general term $A^2_{i_0+r-k'}\sigma_k$, where $k = 2k'$. Remark that by hypothesis:

$$k' < \frac{i_0}{2} \quad \Rightarrow \quad r - k' > 2^{h-1} - \frac{2^h - 1}{2} \quad \Rightarrow \quad 0 < r - k' < r \quad .$$

Hence if $r - k' \notin J_h$ then $A_{i_0+r-k'} = 0$ (from $\mathrm{H_{r-k'}}$). Suppose that $r - k' \in J_h$; then there is a $j \in [1, h-1]$ such that $r - k' = 2^h - 2^j$. Now we have two possibilities:

1. $2k' < r$. If $k \notin J_h$ then $\sigma_k = 0$; if $k \in J_h$ there is a $j' \in [1, h-1]$ such that $k = 2^h - 2^{j'}$; thus $r = 2^h + 2^{h-1} - 2^j - 2^{j'-1}$; if $j < h-1$ we obtain $r > 2^h - 1$; if $j = h-1$ we obtain $r \in J_h$; so in all cases we are in contradiction with the hypothesis on r.
2. $2k' \geq r \quad \Rightarrow \quad r - k' \leq k' \leq \frac{2^h-2}{2}$. Then $r - k'$ cannot be in J_h; that contradicts the hypothesis on $r - k'$.

□

Lemma 7 *Assume that $h = m - 2$. Recall that the defining-set of $B(m-2)$ is denoted by $I(B(m-2))$ and that $i_0 = 2^h - 1$. The following properties are satisfied:*

(i) *Let $s \in [0, 2^m - 1]$ and let $\sum_{k=0}^{m-1} s_k 2^k$ be the 2-ary expansion of s. Then $s \in I(B(h))$ if and only if there is $k < m$ and $j \notin \{k, k' = k+1 (\bmod m)\}$ such that $s_k = s_{k'} = s_j = 0$.*

(ii) *Let $r \in [2, 2^{h-1}[$, r even such that $i_0 + r \notin I(B(h))$. Then :*

$$2i_0 + 3r \in I(B(h)) \quad and \quad i_0 + 3r \in I(B(h)) \quad .$$

(iii) *Let $r \in]2^{h-1}, i_0[$, r even and $r \notin J_h$. Then there is an element of the cyclotomic class of $i_0 + 2r$ (modulo $2^m - 1$), which can be written:*

$$i_0 + \epsilon \quad with \quad -i_0 < \epsilon < r \quad and \quad \epsilon \notin J_h \quad .$$

Proof (i) The hypotheses on s mean that $2^{m-k-1}s < 2^{m-2} - 1$ — i.e. that s is an element of the defining-set of $B(m-2)$ —.

(ii) Let $r' = r/2$. By hypothesis the 2-ary expansion of i_0, r and r' are:

$$i_0 = \sum_{j=0}^{m-3} 2^j \quad , \quad r = \sum_{j=1}^{m-4} r_j 2^j \quad , \quad r' = \sum_{j=0}^{m-5} r_{j+1} 2^j \quad .$$

Note that $i_0 + r + r' < 2^{m-2} + 3.2^{m-4} - 1 < 2^{m-1}$. Let k be the smaller j such that $r_j \neq 0$. Suppose that $r_{k+1} = 0$ or that $k = m-4$. We have:

$$i_0 + r = \sum_{j=0}^{k-1} 2^j + (1+1)2^k + 2^{k+1} + \sum_{j=k+2}^{m-4} (1 + r_j)2^j + 2^{m-3} \quad .$$

Then the 2-ary expansion of $i_0 + r$ is such that its kth term and its $(k+1)$th term are zero. From (i), that means $i_0 + r \in I(B(h))$, which contradicts the hypothesis. Thus $r_{k+1} = 1$ and $k < m-4$. Now the 2-ary expansion of $i_0 + r + r'$ is:

$$\begin{aligned} i_0 + r + r' &= \sum_{j=0}^{k-2} 2^j + (1+0+1)2^{k-1} + (1+1+1)2^k \\ &+ \sum_{j=k+1}^{m-5} (1 + r_j + r_{j+1})2^j + (1 + r_{m-4})2^{m-4} + 2^{m-3} \end{aligned}$$

— By convention a sum from a to b, with $a > b$, equals 0 —.
So we can see that the$(k-1)$th term and the kth term are zero. We can apply (i): the defining-set of $B(h)$ contains $2(i_0 + r + r') = 2i_0 + 3r$.

Now we have:

$$i_0 + 3r < 2^{m-2} - 1 + 3.2^{m-3} < 2^{m-1} + 2^{m-3} - 1 < 2^m - 1 \quad . \tag{22}$$

We consider the 2-ary expansion of $i_0 + 3r$:

$$\begin{aligned} i_0 + r + 2r &= \sum_{j=0}^{k-1} 2^j + (1+1+0)2^k + (1+1+1)2^{k+1} \\ &+ \sum_{j=k+2}^{m-4} (1 + r_j + r_{j-1})2^j + (r_{m-4} + 1)2^{m-3} \quad . \end{aligned}$$

From 22, the lth term, $l = m-2$ or $l = m-3$ is zero. Applying (i), we obtain $i_0 + 3r \in I(B(h))$.

(iii) By hypothesis $2^{m-1} - 1 < i_0 + 2r < 2^m - 1$. We consider another element of the cyclotomic class of $i_0 + 2r$:

$$2(i_0 + 2r) - (2^m - 1) = i_0 + \epsilon \quad \mathit{where} \quad \epsilon = 4r + 2^{m-2} - 2^m \quad .$$

Since r is even and $2^{m-3} < r < 2^{m-2}$, we have:

$$\epsilon > 4(2^{m-3} + 1) + 2^{m-2} - 2^m \quad \Longrightarrow \quad \epsilon > 4 - 2^{m-2} > -i_0$$

and

$$\epsilon = r + 3(r - 2^{m-2}) \quad \Longrightarrow \quad \epsilon < r - 3 \quad .$$

Suppose that $\epsilon \in J_h$. Then there is a $j \in [0, m-2]$ such that:

$$4r + 2^{m-2} - 2^m = 2^{m-2} - 2^j \quad \Longrightarrow \quad r = 2^{m-2} - 2^{j-2} \quad ,$$

which implies $r \in J_h$, in contradiction with the hypothesis. Then we have proved that ϵ cannot be in J_h. □

Now we are able to prove that the code $B(m-2)$ has the property ($\mathrm{RM_{m-2}}$).

Theorem 6 *The minimum weight codewords of the BCH-codes of length $2^m - 1$ and designed distance $2^{m-2} - 1$ are those of the punctured RM-code of same length and order 2.*

Proof The notations are those previously defined; moreover assume that $h = m-2$. We shall prove that, for this particular value of h, $\mathrm{H_r}$ is true for all $r \in [1, i_0[$. If r is odd, we know that $\mathrm{H_r}$ is true; we suppose that $H_{r'}$ is true for all $r' \in [2, r[$ and we want to prove that $\mathrm{H_r}$ is true.

If $i_0 + r \in I(B(h))$ then $A_{i_0+r} = 0$ (by definition of $B(h)$). Remark that A_{i_0} cannot be zero, since the designed distance i_0 of $B(h)$ is exactly its minimum distance. Thus Lemma 4 implies $\sigma_r = 0$; then $\mathrm{H_r}$ is true. So we suppose now that r is even and that $i_0 + r \notin I(B(h))$. We consider two cases:

1) *Assume that* $r \in [2, 2^{h-1}[$. Then r cannot be in J_h. Let ρ be the smallest element of $[i_0 + 1, 2i_0[$, such that $\rho \notin I(B(m-2))$. From Lemma 7-(i), we have:

$$\rho = \begin{cases} \sum_{k=0}^{(m-2)/2} 2^{2k} = \frac{2^m - 1}{3} & \text{if } m \text{ is even} \\ 1 + \sum_{k=0}^{(m-3)/2} 2^{2k+1} = 1 + 2\frac{2^{m-1}-1}{3} & \text{if } m \text{ is odd} \end{cases} \quad .$$

If we suppose that $i_0 + r \notin I(B(m-2))$, then $i_0 + r \geq \rho$.
If m is even then

$$\rho - i_0 = \frac{2^m - 1}{3} - 2^{m-2} + 1 = \frac{2^{m-2} + 2}{3} \quad ,$$

and if m is odd then

$$\rho - i_0 = 1 + 2\frac{2^{m-1}-1}{3} - 2^{m-2} + 1 = 1 + \frac{2^{m-2}+1}{3} \quad .$$

Hence, in all cases, $r > \frac{i_0-1}{3}$. From Lemma 5, the identity I_{2i_0+3r} is reduced to 17. From Lemma 7-(ii), $A_{2i_0+3r} = A_{i_0+3r} = 0$. Then:

$$I_{2i_0+3r} \; : \; A_{i_0+r}^2 = 0 \quad \textit{and} \quad I_{i_0+r} \; : \; A_{i_0+r} + A_{i_0}\sigma_r = 0 \; ,$$

which yields $A_{i_0+r} = 0$ and $\sigma_r = 0$ - i.e. $\mathrm{H_r}$ is true.

2) *Assume that* $r \in [2^{h-1}, i_0[$. If $r \in J_h$ then $\mathrm{H_r}$ is true. So we suppose that $r \notin J_h$. From Lemma 7-(iii), there is an ϵ, $-i_0 < \epsilon < r$ and $\epsilon \notin J_h$, such that $i_0 + \epsilon$ is an element of the cyclotomic class of $i_0 + 2r$; thus

- $-i_0 < \epsilon < 0 \quad \Rightarrow \quad i_0 + \epsilon \in I(B(h)) \quad \Rightarrow \quad A_{i_0+\epsilon} = 0 \quad \Rightarrow \quad A_{i_0+2r} = 0$
- $0 < \epsilon < r \quad \Rightarrow \quad A_{i_0+\epsilon} = 0$, from $\mathrm{H}_\epsilon \quad \Rightarrow \quad \mathrm{A_{i_0+2r}} = 0$

From Lemma 6, the identity $I_{2(i_0+r)}$ is reduced to $A_{i_0+r}^2 = 0$. From Lemma 4, that yields $\sigma_r = 0$ — i.e. $\mathrm{H_r}$ is true —. In accordance with the Theorem 5, we have proved that $B(m-2)$ has the property $(\mathrm{RM_{m-2}})$. □

Let $\mathbf{x} \in B(m-2)$ such that $\omega(\mathbf{x}) = 2^{m-2} = \mu$; let $\mathbf{X} = \{X_1, \ldots, X_\mu\}$ be the set of the locators of $\mathbf{x}$. It is well-known that the extended BCH-codes and the Reed-Muller codes are invariant under the affine group [7][2]; this means that, for each $g \in GF(2^m)$, the locators $\{X_1 + g, \ldots, X_\mu + g\}$ are those of a codeword in the extension of the code $B(m-2)$. In particular we can state:

$$\mathbf{X} = X_1 + \{0\} \cup \mathbf{X}' \quad , \quad \mathbf{X}' = \{X_2 + X_1, \ldots, X_\mu + X_1\}$$

where $\mathbf{X}'$ is the set of the locators of a codeword $\mathbf{x}'$ of $B(m-2)$. Moreover $\mathbf{x}'$ is a *mwc* of $B(m-2)$. Hence the Theorem 6 implies:

Corollary 1 *Let* $\mathbf{x} \in B(m-2)$ *such that* $\omega(\mathbf{x}) = 2^{m-2}$. *Then* $\mathbf{x}$ *is a codeword of the punctured RM-code* $\mathcal{R}(2,m)$ *- i.e. the set of the locators of* $\mathbf{x}$ *is an* $m-2$*-dimensional affine subspace of* $GF(2^m)$.

It is well-known that the automorphism group of the binary punctured Reed-Muller codes is the linear group, denoted $GL(2,m)$ [10]. Hence a code C which has the property $(\mathrm{RM_h})$ is such that its automorphism group is contained in $GL(2,m)$. Moreover such a code cannot be generated by $Mw(C)$, since $\mathcal{R}(m-h,m)$ is strictly contained in it. Thus:

Corollary 2 $m > 5$. *The automorphism group of the BCH-code* $B(m-2)$ *is contained in* $GL(2,m)$.
The code generated by the set of the minimum weight codewords of $B(m-2)$ *is strictly contained in* $B(m-2)$.

The property ($\mathrm{RM_3}$) is studied in the Example 1 and the Theorem 6 gives a general result on the property ($\mathrm{RM_{m-2}}$). From now on, we are interested in the definition of cyclic codes which have the property ($\mathrm{RM_h}$), for $h \in [4, m-3]$, $m > 6$. We study the property ($\mathrm{RM_h}$) by explaining the hypotheses on the *mwc*'s of the codes $B(h)$. The main idea is that the NEWTON's identities yield some conditions on the power sum symmetric functions of these codewords. In accordance with Theorem 5 and Lemma 4, we can state a sufficient condition for a cyclic code to have the property ($\mathrm{RM_h}$):

Corollary 3 *Let us define*

$$T_h = \cup_{s \in U_h} cl(s) \ , \quad U_h = \{ \ s \in [i_0+1, 2i_0[\ | \ s \notin B(h), \ \omega_2(s) < h \ \} \ . \tag{23}$$

Let a cyclic code C such that its defining-set T satisfies

$$I(B(h)) \cup T_h \ \subseteq \ T \ \subseteq \ \{ \ s \in S \ | \ \omega_2(s) < h \ \} \ . \tag{24}$$

If $\mathcal{R}(m-h, m)$ is strictly contained in C then C has the property ($\mathrm{RM_h}$).

Proof Suppose that $C \neq \mathcal{R}(m-h, m)$. Then the second inclusion in (24) is strict. From Lemma 3, the elements of T_h are of the form $s = i_0 + r$ with $r \notin J_h$. Then any *mwc* of C is a *mwc* of $B(h)$ which satisfies $A_{i_0+r} = 0$, for all $r \notin J_h$ (with $r \in [1, i_0[$). Applying Lemma 4, we can prove by induction that $\mathrm{H_r}$ is true for all r. Then C has the property ($\mathrm{RM_h}$). □

The following conjectures are strengthened by all numerical results, we have obtained with a computer. For $h \in [4, m-3]$, $m > 6$:

1. The codes $B(h)$ do not have the property ($\mathrm{RM_h}$).
2. There exists a cyclic code C, the definition-set of which is strictly contained in $I(B(h)) \cup T_h$, which has the property ($\mathrm{RM_h}$).

We give later some examples which prove that the second conjecture is true for $m = 7$ and $m = 8$. We use the fact that the proof of Theorem 6, applied to the general case $h \neq m-2$, provides an algorithm constructing a cyclic code which has the property ($\mathrm{RM_h}$), for a given m. In the following, C is a cyclic code such that $\mathcal{R}(m-h, m) \subset C \subset B(h)$; T denotes its defining-set. The proof of the proposed algorithm is obvious: using the results of Lemmas 4, 5 and 6, we construct T such that $\mathrm{H_r}$ is true for all $r \in [1, i_0[$; if r is such that the NEWTON's identities, given by 17 or 18 or 20, do not imply $A_{i_0+r} = 0$, then we add $i_0 + r$ in T.

Algorithm constructing T

1. $T = I(B(h))$; $r = 0$; $i_0 = 2^h - 1$;
2. $r = r + 2$; if $r > i_0$ then go to 8 ;
3. If $i_0 + r \in T$ then put $\sigma_r := 0$ and go to 2 ;

4. If $r < 2^{h-1}$, examine the identity I_{2i_0+3r}:

   if $\quad I_{2i_0+3r} \ : \ A^2_{i_0+r}\sigma_r = 0 \quad$ then go to 7

   else put $\quad T := T \cup cl(i_0 + r) \quad$ and go to 7 ;

5. If $r \in J_h$ then go to 2 ;

6. If $r > 2^{h-1}$, examine the identity $I_{2(i_0+r)}$:

   if $\quad I_{2(i_0+r)} \ : \ A^2_{i_0+r} = 0 \quad$ then go to 7

   else put $\quad T := T \cup cl(i_0 + r) \quad$;

7. Put $\sigma_r := 0$ and $A^{2^j}_{i_0+r} := 0$, for $j \in [0, m-1]$; go to 2 ;

8. End.

`Example 2:` $m = 7$; $h = 4$; thus $i_0 = 15$ and $J_4 = \{0, 8, 12, 14\}$. The code $B(h)$ is the BCH-code of length 127 and designed distance 15. In accordance with Corollary 3, we have $T_4 = cl(19) \cup cl(21)$. Using the algorithm, we obtain that the code C with defining-set $T = B(4) \cup cl(19)$, satisfies (RM_4).

`Example 3:` $m = 8$. 1) $h = 4$. The code $B(4)$ is the BCH-code of length 255 and designed distance 15. We have:

$$T_4 = cl(17) \cup cl(19) \cup cl(21) \cup cl(25) \quad .$$

The algorithm produces: $T = I(B(4)) \cup cl(17) \cup cl(19)$.

2) $h = 5$; $J_5 = \{0, 16, 24, 28, 30, 31\}$. The code $B(5)$ is the BCH-code of length 255 and designed distance 31. We have

$$T_5 = cl(37) \cup cl(39) \cup cl(43) \cup cl(45) \cup cl(51) \cup cl(53) \quad .$$

The algorithm produces: $T = I(B(5)) \cup cl(37) \cup cl(39)$.

Acknowledgment

The auhors wish to thank E.F. Assmus, G.D. Cohen and H.F. Mattson for enriching discussions and valuable suggestions.

Annex A $B(255,61)$ has minimum distance > 61

We consider the Newton's identities I_r for $0 < r \leq n = 255$, for the code $B(255,61)$, and for the weight $\delta = 61$. We want to prove that there exists no codeword of such weight.

The non-null power sum symmetric functions of the code are:

$$A_{61},\ A_{63},\ A_{85},\ A_{87},\ A_{91},\ A_{95},\ A_{111},\ A_{119},\ A_{127}.$$

And since 255 and 61 are relatively prime we can suppose $A_{61} = 1$ (the shift corresponds to a multiplication of each A_i by α^i).

In the the case of a narrow-sense primitive BCH code, and for a weight equal to the designed distance, the Newton's identities I_r (9) for odd r from $\delta+2$ to $2\delta-1$ form a linear triangular system giving the σ_i's for even i as polynomials depending on the non-null A_i's. Here the system consists of the 30 following equations:

$$\begin{aligned}
I_{63} &: A_{63} + \sigma_2 = 0\\
I_{65} &: A_{63}\sigma_2 + \sigma_4 = 0\\
I_{67} &: A_{63}\sigma_4 + \sigma_6 = 0\\
I_{69} &: A_{63}\sigma_6 + \sigma_8 = 0\\
I_{71} &: A_{63}\sigma_8 + \sigma_{10} = 0\\
I_{73} &: A_{63}\sigma_{10} + \sigma_{12} = 0\\
I_{75} &: A_{63}\sigma_{12} + \sigma_{14} = 0\\
I_{77} &: A_{63}\sigma_{14} + \sigma_{16} = 0\\
I_{79} &: 1 + A_{63}\sigma_{16} + \sigma_{18} = 0\\
I_{81} &: \sigma_2 + A_{63}\sigma_{18} + \sigma_{20} = 0\\
I_{83} &: \sigma_4 + A_{63}\sigma_{20} + \sigma_{22} = 0\\
I_{85} &: A_{85} + \sigma_6 + A_{63}\sigma_{22} + \sigma_{24} = 0\\
I_{87} &: A_{87} + A_{85}\sigma_2 + \sigma_8 + A_{63}\sigma_{24} + \sigma_{26} = 0\\
I_{89} &: A_{87}\sigma_2 + A_{85}\sigma_4 + \sigma_{10} + A_{63}\sigma_{26} + \sigma_{28} = 0\\
I_{91} &: A_{91} + A_{87}\sigma_4 + A_{85}\sigma_6 + \sigma_{12} + A_{63}\sigma_{28} + \sigma_{30} = 0\\
I_{93} &: A_{87}^4 + A_{91}\sigma_2 + A_{87}\sigma_6 + A_{85}\sigma_8 + \sigma_{14} + A_{63}\sigma_{30} + \sigma_{32} = 0\\
I_{95} &: A_{95} + A_{87}^4\sigma_2 + A_{91}\sigma_4 + A_{87}\sigma_8 + A_{85}\sigma_{10} + \sigma_{16} + A_{63}\sigma_{32} + \sigma_{34} = 0\\
I_{97} &: A_{95}\sigma_2 + A_{87}^4\sigma_4 + A_{91}\sigma_6 + A_{87}\sigma_{10} + A_{85}\sigma_{12} + \sigma_{18} + A_{63}\sigma_{34} + \sigma_{36} = 0\\
I_{99} &: A_{95}\sigma_4 + A_{87}^4\sigma_6 + A_{91}\sigma_8 + A_{87}\sigma_{12} + A_{85}\sigma_{14} + \sigma_{20} + A_{63}\sigma_{36} + \sigma_{38} = 0\\
I_{101} &: A_{95}\sigma_6 + A_{87}^4\sigma_8 + A_{91}\sigma_{10} + A_{87}\sigma_{14} + A_{85}\sigma_{16} + \sigma_{22} + A_{63}\sigma_{38} + \sigma_{40} = 0\\
I_{103} &: A_{95}\sigma_8 + A_{87}^4\sigma_{10} + A_{91}\sigma_{12} + A_{87}\sigma_{16} + A_{85}\sigma_{18} + \sigma_{24} + A_{63}\sigma_{40} + \sigma_{42} = 0\\
I_{105} &: A_{95}\sigma_{10} + A_{87}^4\sigma_{12} + A_{91}\sigma_{14} + A_{87}\sigma_{18} + A_{85}\sigma_{20} + \sigma_{26} + A_{63}\sigma_{42} + \sigma_{44} = 0\\
I_{107} &: A_{91}^{32} + A_{95}\sigma_{12} + A_{87}^4\sigma_{14} + A_{91}\sigma_{16} + A_{87}\sigma_{20} + A_{85}\sigma_{22} + \sigma_{28} + A_{63}\sigma_{44} + \sigma_{46} = 0\\
I_{109} &: A_{91}^4 + A_{91}^{32}\sigma_2 + A_{95}\sigma_{14} + A_{87}^4\sigma_{16} + A_{91}\sigma_{18} + A_{87}\sigma_{22} + A_{85}\sigma_{24} + \sigma_{30} + A_{63}\sigma_{46}\\
&\quad +\sigma_{48} = 0
\end{aligned}$$

$$\begin{aligned}
I_{111} &: A_{111} + A_{91}^4\sigma_2 + A_{91}^{32}\sigma_4 + A_{95}\sigma_{16} + A_{87}^4\sigma_{18} + A_{91}\sigma_{20} + A_{87}\sigma_{24} + A_{85}\sigma_{26} + \sigma_{32} \\
&\quad + A_{63}\sigma_{48} + \sigma_{50} = 0 \\
I_{113} &: A_{111}\sigma_2 + A_{91}^4\sigma_4 + A_{91}^{32}\sigma_6 + A_{95}\sigma_{18} + A_{87}^4\sigma_{20} + A_{91}\sigma_{22} + A_{87}\sigma_{26} + A_{85}\sigma_{28} + \sigma_{34} \\
&\quad + A_{63}\sigma_{50} + \sigma_{52} = 0 \\
I_{115} &: A_{111}\sigma_4 + A_{91}^4\sigma_6 + A_{91}^{32}\sigma_8 + A_{95}\sigma_{20} + A_{87}^4\sigma_{22} + A_{91}\sigma_{24} + A_{87}\sigma_{28} + A_{85}\sigma_{30} + \sigma_{36} \\
&\quad + A_{63}\sigma_{52} + \sigma_{54} = 0 \\
I_{117} &: A_{87}^{16} + A_{111}\sigma_6 + A_{91}^4\sigma_8 + A_{91}^{32}\sigma_{10} + A_{95}\sigma_{22} + A_{87}^4\sigma_{24} + A_{91}\sigma_{26} + A_{87}\sigma_{30} + A_{85}\sigma_{32} \\
&\quad + \sigma_{38} + A_{63}\sigma_{54} + \sigma_{56} = 0 \\
I_{119} &: A_{119} + A_{87}^{16}\sigma_2 + A_{111}\sigma_8 + A_{91}^4\sigma_{10} + A_{91}^{32}\sigma_{12} + A_{95}\sigma_{24} + A_{87}^4\sigma_{26} + A_{91}\sigma_{28} + A_{87}\sigma_{32} \\
&\quad + A_{85}\sigma_{34} + \sigma_{40} + A_{63}\sigma_{56} + \sigma_{58} = 0 \\
I_{121} &: A_{119}\sigma_2 + A_{87}^{16}\sigma_4 + A_{111}\sigma_{10} + A_{91}^4\sigma_{12} + A_{91}^{32}\sigma_{14} + A_{95}\sigma_{26} + A_{87}^4\sigma_{28} + A_{91}\sigma_{30} + A_{87}\sigma_{34} \\
&\quad + A_{85}\sigma_{36} + \sigma_{42} + A_{63}\sigma_{58} + \sigma_{60} = 0
\end{aligned}$$

which gives us the following values for the σ_i's:

$$\begin{aligned}
\sigma_2 &:= A_{63} \\
\sigma_4 &:= A_{63}^2 \\
\sigma_6 &:= A_{63}^3 \\
\sigma_8 &:= A_{63}^4 \\
\sigma_{10} &:= A_{63}^5 \\
\sigma_{12} &:= A_{63}^6 \\
\sigma_{14} &:= A_{63}^7 \\
\sigma_{16} &:= A_{63}^8 \\
\sigma_{18} &:= 1 + A_{63}^9 \\
\sigma_{20} &:= A_{63}^{10} \\
\sigma_{22} &:= A_{63}^2 + A_{63}^{11} \\
\sigma_{24} &:= A_{85} + A_{63}^{12} \\
\sigma_{26} &:= A_{87} + A_{63}^4 + A_{63}^{13} \\
\sigma_{28} &:= A_{85}A_{63}^2 + A_{63}^{14} \\
\sigma_{30} &:= A_{91} + A_{87}A_{63}^2 + A_{63}^6 + A_{63}^{15} \\
\sigma_{32} &:= A_{87}^4 + A_{85}A_{63}^4 + A_{63}^{16} \\
\sigma_{34} &:= A_{95} + A_{91}A_{63}^2 + A_{87}A_{63}^4 + A_{63}^8 + A_{63}^{17} \\
\sigma_{36} &:= A_{87}^4A_{63}^2 + A_{85}A_{63}^6 + 1 + A_{63}^{18} \\
\sigma_{38} &:= A_{95}A_{63}^2 + A_{91}A_{63}^4 + A_{87}A_{63}^6 + A_{63}^{10} + A_{63} + A_{63}^{19} \\
\sigma_{40} &:= A_{87}^4A_{63}^4 + A_{85}A_{63}^8 + A_{63}^{20} \\
\sigma_{42} &:= A_{95}A_{63}^4 + A_{91}A_{63}^6 + A_{87}A_{63}^8 + A_{63}^{12} + A_{63}^{21} \\
\sigma_{44} &:= A_{87}^4A_{63}^6 + A_{85}A_{63}^{10} + A_{63}^4 + A_{63}^{22} \\
\sigma_{46} &:= A_{91}^{32} + A_{95}A_{63}^6 + A_{91}A_{63}^8 + A_{87}A_{63}^{10} + A_{63}^{14} + A_{63}^5 + A_{63}^{23}
\end{aligned}$$

$$
\begin{aligned}
\sigma_{48} &:= A_{91}^4 + A_{87}^4 A_{63}^8 + A_{85}^2 + A_{85} A_{63}^{12} + A_{63}^{24}\\
\sigma_{50} &:= A_{111} + A_{91}^{32} A_{63}^2 + A_{95} A_{63}^8 + A_{91} A_{63}^{10} + A_{87} A_{63}^{12} + A_{63}^{16} + A_{63} A_{85}^2 + A_{63}^{25}\\
\sigma_{52} &:= A_{63}^8 + A_{87}^2 + A_{63}^{26} + A_{91}^4 A_{63}^2 + A_{87}^4 A_{63}^{10} + A_{85} A_{63}^{14}\\
\sigma_{54} &:= 1 + A_{63}^9 + A_{91}^{32} A_{63}^4 + A_{63}^{27} + A_{95} A_{63}^{10} + A_{91} A_{63}^{12} + A_{87} A_{63}^{14} + A_{63} A_{87}^2 + A_{111} A_{63}^2 + A_{63}^{18}\\
\sigma_{56} &:= A_{91}^4 A_{63}^4 + A_{87}^{16} + A_{63}^{28} + A_{87}^4 A_{63}^{12} + A_{85}^2 A_{63}^4 + A_{85} A_{63}^{16}\\
\sigma_{58} &:= A_{111} A_{63}^4 + A_{119} + A_{63}^{29} + A_{91}^{32} A_{63}^6 + A_{95} A_{63}^{12} + A_{91} A_{63}^{14} + A_{87} A_{63}^{16} + A_{85}^2 A_{63}^5 + A_{63}^{20}\\
\sigma_{60} &:= A_{85} + A_{91}^2 + A_{87}^2 A_{63}^4 + A_{85} A_{63}^{18} + A_{87}^{16} A_{63}^2 + A_{91}^4 A_{63}^6 + A_{87}^4 A_{63}^{14} + A_{63}^{30} + A_{63}^{12}
\end{aligned}
$$

The other values are $\sigma_0 = 1$, by definition, and $\sigma_i = 0$ for odd i, given by the δ first identities.

After substitution of the σ_i's by their values, the remaining equations are sorted in increasing size (number of monomials) order :

186, 190, 188, 194, 198, 192, 202, 123, 184, 189, 191, 196, 206, 254, 127, 195, 200, 210, 135, 193, 187, 199, 214, 125, 131, 204, 252, 197, 222, 203, 238, 129, 139, 208, 250, 143, 201, 218, 133, 137, 226, 230, 246, 248, 234, 185, 212, 242, 207, 141, 181, 216, 236, 244, 151, 183, 205, 220, 232, 147, 224, 159, 179, 211, 240, 149, 175, 155, 145, 157, 209, 173, 163, 167, 228, 153, 171, 215, 253, 251, 165, 169, 161, 177, 213, 223, 239, 247, 249, 243, 217, 235, 237, 245, 219, 221, 229, 231, 233, 227, 225, 241

We will proceed as follow :

- we successively check the equations in the order given above, up to a "solvable" one.
- After solving one equation, we restart from the beginning. (*at each stage we substitute all the known A_i's in the current equation, and we simplify it as much as possible*)

We give here in the resolution order all the "solvable" equations, and the way we used them.

$$
I_{186} \ : \ A_{87}^8 + A_{85}^2 A_{63}^8 + A_{85} A_{63}^{20} + A_{87}^{16} A_{63}^4 + A_{91}^4 A_{63}^8 + A_{87}^4 A_{63}^{16} + A_{63}^{32} + \mathbf{A_{95}^4} = 0
$$

$$
\Rightarrow \ \mathbf{A_{95}} := A_{87}^2 + A_{85}^2 A_{63}^2 + A_{85} A_{63}^5 + A_{87}^4 A_{63} + A_{91} A_{63}^2 + A_{87} A_{63}^4 + A_{63}^8
$$

$$
\begin{aligned}
I_{188} \ : \ & A_{87}^8 A_{63} + A_{91}^2 A_{63}^3 + A_{87}^2 A_{63}^7 + A_{85}^2 + A_{85}^2 A_{63}^9 + A_{91} + A_{87} A_{63}^2 + A_{63}^6 + A_{63}^{15}\\
& + \mathbf{A_{127}} = 0
\end{aligned}
$$

$$
\Rightarrow \ \mathbf{A_{127}} := A_{87}^8 A_{63} + A_{91}^2 A_{63}^3 + A_{87}^2 A_{63}^7 + A_{85}^2 + A_{85}^2 A_{63}^9 + A_{91} + A_{87} A_{63}^2 + A_{63}^6 + A_{63}^{15}
$$

$$
I_{194} : \ \mathbf{A_{85}^3} + 1 = 0 \ \Rightarrow \ \mathbf{A_{85}} \neq 0
$$

$$I_{198}:\ A_{85}\mathbf{A_{87}^2} + A_{63}^2 = 0 \ \Rightarrow\ \mathbf{A_{87}} := A_{63}A_{85}$$

$$\begin{aligned} I_{187} \quad : \quad & 1 + A_{91}A_{85}A_{63}^{18} + A_{85}^2A_{91}A_{63}^6 + A_{91}^4A_{63}^{21} + A_{63}^2 + A_{63}^{142} + A_{63}^{130}A_{85} + A_{111}^{128}A_{63}^2 \\ & + A_{91}^{16}A_{63}^3 + A_{85}^2A_{63}^{39} + \mathbf{A_{119}^8} + A_{91}^6A_{63}^9 + A_{91}^2A_{63}^{33} + A_{91}^4A_{63}^3 + A_{85}^2A_{91}^2 \\ & + A_{85}^2A_{63}^{21} + A_{63}^{36} + A_{63}^{15}A_{85} + A_{91}A_{63}^{30} + A_{91}^3 + A_{85}A_{63}^{24} + A_{85}^2A_{63}^{15}A_{91}^4 \\ & + A_{91}^2A_{63}^{21}A_{85} + A_{63}^9A_{85}A_{91}^4 + A_{91}^4A_{63}^{12} + A_{91}^2A_{63}^6 + A_{91}^5A_{63}^6 + A_{85}^2A_{91}^4A_{63}^6 \\ & + A_{85}^2A_{63}^{30} + A_{63}^{45} + A_{91}A_{85} + A_{91}A_{63}^{12} + A_{63}^3A_{85}^2 = 0 \end{aligned}$$

$$\begin{aligned} \Rightarrow\ \mathbf{A_{119}} \ := \ & 1 + A_{111}^{16}A_{63}^{64} + A_{85}A_{63}^{228} + A_{91}^{160}A_{63}^{192} + A_{91}^{32}A_{85}^2A_{63}^{66} + A_{63}^{64} + A_{85}A_{63}^{225}A_{91}^{128} \\ & + A_{63}^{80}A_{85}^2 + A_{63}^{225}A_{85}^2 + A_{91}^{32}A_{63}^{195} + A_{85}A_{63}^{195} + A_{91}^2A_{63}^{96} + A_{91}^{64}A_{85} + A_{63}^{132} \\ & + A_{91}^{128}A_{63}^{96} + A_{91}^{192}A_{63}^{33} + A_{91}^{64}A_{63}^{162}A_{85}^2 + A_{63}^{96}A_{85} + A_{63}^{33}A_{85}^2A_{91}^{128} + A_{85}A_{91}^{128}A_{63}^{192} \\ & + A_{91}^{32}A_{63}^{129} + A_{63}^{209} + A_{91}^{128}A_{63}^{162} + A_{63}^{165} + A_{85}A_{91}^{32}A_{63}^{192} + A_{63}^3A_{85}^2 + A_{91}^{128}A_{63}^{129} \\ & + A_{91}^{64}A_{63}^{36} + A_{85}A_{63}^{162} + A_{91}^{64}A_{63}^{192} + A_{91}^{96} + A_{91}^{32}A_{85}^2 \end{aligned}$$

$$\begin{aligned} I_{189} \quad : \quad & A_{91}^2A_{63}^{34} + A_{91}^4A_{85}A_{63}^{10} + A_{91}A_{63}^{31} + A_{63}A_{91}^3 + A_{91}^4A_{63}^4 + A_{85}A_{63}^{25} + A_{85}^2A_{63}^{22} \\ & + A_{91}A_{85}A_{63}^{19} + A_{63}^7A_{91}^2 + A_{91}^4A_{63}^{13} + A_{91}^5A_{63}^7 + A_{85}^2A_{63}^{31}A_{63} + A_{63}^2 + A_{63}^{128}A_{91} \\ & + A_{63}^{37} + \mathbf{A_{111}^4} + A_{91}A_{63}^{13} + A_{91}^4A_{63}^{22} + A_{63}^{128}A_{85}^2 + A_{91}^2A_{63}A_{85}^2 + A_{85}^2A_{63}^4 \\ & + A_{85}A_{63}^{16} + A_{63}^3 + A_{63}^{134} + A_{85}^2A_{63}^{40} + A_{91}^6A_{63}^{10} + A_{63}^{46} + A_{85}^2A_{91}A_{63}^7 \\ & + A_{85}^2A_{63}^{16}A_{91}^4 + A_{91}^2A_{63}^{22}A_{85} + A_{85}^2A_{91}^4A_{63}^7 + A_{63}A_{91}A_{85} = 0 \end{aligned}$$

$$\begin{aligned} \Rightarrow\ \mathbf{A_{111}} \ := \ & A_{91}A_{85}^2A_{63}^4 + A_{63}^{133}A_{85}^2 + A_{91}A_{85}A_{63}^{130} + A_{91}^{64}A_{85}A_{63}^{196} + A_{91}^{128}A_{63}^{64}A_{85}^2 \\ & + A_{85}^2A_{91}^{64}A_{63}^{193} + A_{63}^{70}A_{85} + A_{63}^{64} + A_{63}^{128} + A_{63}^{139} + A_{85}^2A_{63}^{10} + A_{91}^{129}A_{63}^{130} \\ & + A_{91}^{128}A_{63}^{133}A_{85} + A_{85}^2A_{91}A_{63}^{193} + A_{63}A_{85}^2 + A_{63}^{32}A_{85}^2 + A_{63}^{64}A_{91}^{64}A_{85} + A_{63}^{73} \\ & + A_{91}A_{63} + A_{85}A_{63}^4 + A_{63}^{133}A_{91} + A_{91}^{65}A_{63}^{193} + A_{85}^2A_{63}^{199} + A_{91}^{64}A_{63}^{67} + A_{63}^{161} \\ & + A_{91}^{64}A_{63}^{199} + A_{91}A_{63}^{67} + A_{91}^{128}A_{63}^{136} + A_{63}^{193}A_{91}^{128} + A_{63}^{32}A_{91}^{64} + A_{63}^{192} + A_{63}^{64}A_{91}^{192} \end{aligned}$$

$$I_{199}:\ \mathbf{A_{91}^{16}} = 0 \ \Rightarrow\ \mathbf{A_{91}} := 0$$

$$I_{203}:\ 1 = 0$$

□

Annex B $B(255, 59)$ has minimum distance > 59

We consider the Newton's identities I_r for $0 < r \leq n = 255$, for the code $B(255, 59)$, and for the weight $\delta = 59$. We want to prove that there exists no codeword of such weight.

The non-null power sum symmetric functions of the code are:

$$A_{59},\ A_{61},\ A_{63},\ A_{85},\ A_{87},\ A_{91},\ A_{95},\ A_{111},\ A_{119},\ A_{127}.$$

And since 255 and 59 are relatively prime we can suppose $A_{59} = 1$.

We will first solve the linear triangular system giving the σ_i's for even i as polynomials depending on the non-null A_i's. The system consists of the 29 following equations:

$$
\begin{aligned}
I_{61} &: A_{61} + \sigma_2 = 0 \\
I_{63} &: A_{63} + A_{61}\sigma_2 + \sigma_4 = 0 \\
I_{65} &: A_{63}\sigma_2 + A_{61}\sigma_4 + \sigma_6 = 0 \\
I_{67} &: A_{63}\sigma_4 + A_{61}\sigma_6 + \sigma_8 = 0 \\
I_{69} &: A_{63}\sigma_6 + A_{61}\sigma_8 + \sigma_{10} = 0 \\
I_{71} &: A_{63}\sigma_8 + A_{61}\sigma_{10} + \sigma_{12} = 0 \\
I_{73} &: A_{63}\sigma_{10} + A_{61}\sigma_{12} + \sigma_{14} = 0 \\
I_{75} &: A_{63}\sigma_{12} + A_{61}\sigma_{14} + \sigma_{16} = 0 \\
I_{77} &: A_{63}\sigma_{14} + A_{61}\sigma_{16} + \sigma_{18} = 0 \\
I_{79} &: A_{61}^{64} + A_{63}\sigma_{16} + A_{61}\sigma_{18} + \sigma_{20} = 0 \\
I_{81} &: A_{61}^{64}\sigma_2 + A_{63}\sigma_{18} + A_{61}\sigma_{20} + \sigma_{22} = 0 \\
I_{83} &: A_{61}^{64}\sigma_4 + A_{63}\sigma_{20} + A_{61}\sigma_{22} + \sigma_{24} = 0 \\
I_{85} &: A_{85} + A_{61}^{64}\sigma_6 + A_{63}\sigma_{22} + A_{61}\sigma_{24} + \sigma_{26} = 0 \\
I_{87} &: A_{87} + A_{85}\sigma_2 + A_{61}^{64}\sigma_8 + A_{63}\sigma_{24} + A_{61}\sigma_{26} + \sigma_{28} = 0 \\
I_{89} &: A_{87}\sigma_2 + A_{85}\sigma_4 + A_{61}^{64}\sigma_{10} + A_{63}\sigma_{26} + A_{61}\sigma_{28} + \sigma_{30} = 0 \\
I_{91} &: A_{91} + A_{87}\sigma_4 + A_{85}\sigma_6 + A_{61}^{64}\sigma_{12} + A_{63}\sigma_{28} + A_{61}\sigma_{30} + \sigma_{32} = 0 \\
I_{93} &: A_{87}^{4} + A_{91}\sigma_2 + A_{87}\sigma_6 + A_{85}\sigma_8 + A_{61}^{64}\sigma_{14} + A_{63}\sigma_{30} + A_{61}\sigma_{32} + \sigma_{34} = 0 \\
I_{95} &: A_{95} + A_{87}^{4}\sigma_2 + A_{91}\sigma_4 + A_{87}\sigma_8 + A_{85}\sigma_{10} + A_{61}^{64}\sigma_{16} + A_{63}\sigma_{32} + A_{61}\sigma_{34} + \sigma_{36} = 0 \\
I_{97} &: A_{95}\sigma_2 + A_{87}^{4}\sigma_4 + A_{91}\sigma_6 + A_{87}\sigma_{10} + A_{85}\sigma_{12} + A_{61}^{64}\sigma_{18} + A_{63}\sigma_{34} + A_{61}\sigma_{36} + \sigma_{38} = 0 \\
I_{99} &: A_{95}\sigma_4 + A_{87}^{4}\sigma_6 + A_{91}\sigma_8 + A_{87}\sigma_{12} + A_{85}\sigma_{14} + A_{61}^{64}\sigma_{20} + A_{63}\sigma_{36} + A_{61}\sigma_{38} + \sigma_{40} = 0 \\
I_{101} &: A_{95}\sigma_6 + A_{87}^{4}\sigma_8 + A_{91}\sigma_{10} + A_{87}\sigma_{14} + A_{85}\sigma_{16} + A_{61}^{64}\sigma_{22} + A_{63}\sigma_{38} + A_{61}\sigma_{40} + \sigma_{42} = 0 \\
I_{103} &: 1 + A_{95}\sigma_8 + A_{87}^{4}\sigma_{10} + A_{91}\sigma_{12} + A_{87}\sigma_{16} + A_{85}\sigma_{18} + A_{61}^{64}\sigma_{24} + A_{63}\sigma_{40} + A_{61}\sigma_{42} \\
&\quad +\sigma_{44} = 0 \\
I_{105} &: \sigma_2 + A_{95}\sigma_{10} + A_{87}^{4}\sigma_{12} + A_{91}\sigma_{14} + A_{87}\sigma_{18} + A_{85}\sigma_{20} + A_{61}^{64}\sigma_{26} + A_{63}\sigma_{42} + A_{61}\sigma_{44} \\
&\quad +\sigma_{46} = 0 \\
I_{107} &: A_{91}^{32} + \sigma_4 + A_{95}\sigma_{12} + A_{87}^{4}\sigma_{14} + A_{91}\sigma_{16} + A_{87}\sigma_{20} + A_{85}\sigma_{22} + A_{61}^{64}\sigma_{28} + A_{63}\sigma_{44} \\
&\quad +A_{61}\sigma_{46} + \sigma_{48} = 0 \\
I_{109} &: A_{91}^{4} + A_{91}^{32}\sigma_2 + \sigma_6 + A_{95}\sigma_{14} + A_{87}^{4}\sigma_{16} + A_{91}\sigma_{18} + A_{87}\sigma_{22} + A_{85}\sigma_{24} + A_{61}^{64}\sigma_{30} + A_{63}\sigma_{46} \\
&\quad +A_{61}\sigma_{48} + \sigma_{50} = 0 \\
I_{111} &: A_{111} + A_{91}^{4}\sigma_2 + A_{91}^{32}\sigma_4 + \sigma_8 + A_{95}\sigma_{16} + A_{87}^{4}\sigma_{18} + A_{91}\sigma_{20} + A_{87}\sigma_{24} + A_{85}\sigma_{26} + A_{61}^{64}\sigma_{32} \\
&\quad +A_{63}\sigma_{48} + A_{61}\sigma_{50} + \sigma_{52} = 0
\end{aligned}
$$

$$
\begin{aligned}
I_{113} &: A_{111}\sigma_2 + A_{91}^4\sigma_4 + A_{91}^{32}\sigma_6 + \sigma_{10} + A_{95}\sigma_{18} + A_{87}^4\sigma_{20} + A_{91}\sigma_{22} + A_{87}\sigma_{26} + A_{85}\sigma_{28} \\
&\quad + A_{61}^{64}\sigma_{34} + A_{63}\sigma_{50} + A_{61}\sigma_{52} + \sigma_{54} = 0 \\
I_{115} &: A_{111}\sigma_4 + A_{91}^4\sigma_6 + A_{91}^{32}\sigma_8 + \sigma_{12} + A_{95}\sigma_{20} + A_{87}^4\sigma_{22} + A_{91}\sigma_{24} + A_{87}\sigma_{28} + A_{85}\sigma_{30} \\
&\quad + A_{61}^{64}\sigma_{36} + A_{63}\sigma_{52} + A_{61}\sigma_{54} + \sigma_{56} = 0 \\
I_{117} &: A_{87}^{16} + A_{111}\sigma_6 + A_{91}^4\sigma_8 + A_{91}^{32}\sigma_{10} + \sigma_{14} + A_{95}\sigma_{22} + A_{87}^4\sigma_{24} + A_{91}\sigma_{26} + A_{87}\sigma_{30} \\
&\quad + A_{85}\sigma_{32} + A_{61}^{64}\sigma_{38} + A_{63}\sigma_{54} + A_{61}\sigma_{56} + \sigma_{58} = 0 \\
I_{119} &: A_{119} + A_{87}^{16}\sigma_2 + A_{111}\sigma_8 + A_{91}^4\sigma_{10} + A_{91}^{32}\sigma_{12} + \sigma_{16} + A_{95}\sigma_{24} + A_{87}^4\sigma_{26} + A_{91}\sigma_{28} \\
&\quad + A_{87}\sigma_{32} + A_{85}\sigma_{34} + A_{61}^{64}\sigma_{40} + A_{63}\sigma_{56} + A_{61}\sigma_{58} = 0
\end{aligned}
$$

which gives us the following values for the σ_i's:

$$
\begin{aligned}
\sigma_2 &:= A_{61} \\
\sigma_4 &:= A_{61}^2 + A_{63} \\
\sigma_6 &:= A_{61}^3 \\
\sigma_8 &:= A_{63}A_{61}^2 + A_{63}^2 + A_{61}^4 \\
\sigma_{10} &:= A_{61}A_{63}^2 + A_{61}^5 \\
\sigma_{12} &:= A_{63}^3 + A_{63}A_{61}^4 + A_{61}^6 \\
\sigma_{14} &:= A_{61}^7 \\
\sigma_{16} &:= A_{63}^4 + A_{63}^2A_{61}^4 + A_{63}A_{61}^6 + A_{61}^8 \\
\sigma_{18} &:= A_{61}A_{63}^4 + A_{63}^2A_{61}^5 + A_{61}^9 \\
\sigma_{20} &:= A_{61}^{64} + A_{63}^5 + A_{63}^3A_{61}^4 + A_{63}A_{61}^8 + A_{61}^2A_{63}^4 + A_{61}^{10} \\
\sigma_{22} &:= A_{61}^3A_{63}^4 + A_{61}^{11} \\
\sigma_{24} &:= A_{61}^{66} + A_{63}^6 + A_{63}^2A_{61}^8 + A_{61}^2A_{63}^5 + A_{63}A_{61}^{10} + A_{61}^{12} \\
\sigma_{26} &:= A_{85} + A_{61}A_{63}^6 + A_{63}^2A_{61}^9 + A_{61}^{13} \\
\sigma_{28} &:= A_{87} + A_{61}^{64}A_{63}^2 + A_{61}^{68} + A_{63}^7 + A_{63}^3A_{61}^8 + A_{63}A_{61}^{12} + A_{61}^{14} \\
\sigma_{30} &:= A_{85}A_{61}^2 + A_{61}^{15} \\
\sigma_{32} &:= A_{91} + A_{87}A_{61}^2 + A_{61}^{70} + A_{63}^8 + A_{63}^4A_{61}^8 + A_{63}^2A_{61}^{12} + A_{63}A_{61}^{14} + A_{61}^{16} \\
\sigma_{34} &:= A_{87}^4 + A_{85}A_{63}^2 + A_{85}A_{61}^4 + A_{61}A_{63}^8 + A_{63}^4A_{61}^9 + A_{63}^2A_{61}^{13} + A_{61}^{17} \\
\sigma_{36} &:= A_{95} + A_{61}^{18} + A_{61}^{72} + A_{63}^9 + A_{91}A_{61}^2 + A_{87}A_{63}^2 + A_{87}A_{61}^4 + A_{61}^{64}A_{63}^4 + A_{61}^{68}A_{63}^2 + A_{63}^5A_{61}^8 \\
&\qquad + A_{63}^3A_{61}^{12} + A_{63}A_{61}^{16} + A_{61}^2A_{63}^8 + A_{63}^4A_{61}^{10} \\
\sigma_{38} &:= A_{85}A_{61}^6 + A_{61}^3A_{63}^8 + A_{63}^4A_{61}^{11} + A_{61}^{19} + A_{87}^4A_{61}^2 \\
\sigma_{40} &:= A_{61}^{128} + A_{63}^6A_{61}^8 + A_{63}^2A_{61}^{16} + A_{61}^2A_{63}^9 + A_{63}^5A_{61}^{10} + A_{61}^4A_{63}^8 + A_{61}^{66}A_{63}^4 + A_{95}A_{61}^2 \\
&\qquad + A_{91}A_{63}^2 + A_{91}A_{61}^4 + A_{61}^{74} + A_{63}^{10} + A_{61}^{20} + A_{87}A_{61}^6 + A_{63}A_{61}^{18} \\
\sigma_{42} &:= A_{85}A_{63}^2A_{61}^4 + A_{87}^4A_{63}^2 + A_{87}^4A_{61}^4 + A_{85}A_{63}^4 + A_{85}A_{61}^8 + A_{63}^6A_{61}^9 + A_{63}^2A_{61}^{17} + A_{61}^5A_{63}^8 \\
&\qquad + A_{61}A_{63}^{10} + A_{61}^{129} + A_{61}^{21} \\
\sigma_{44} &:= 1 + A_{87}A_{63}^2A_{61}^4 + A_{63}A_{61}^{128} + A_{61}^{22} + A_{61}^{76} + A_{63}^{11} + A_{95}A_{63}^2 + A_{95}A_{61}^4 + A_{91}A_{61}^6 \\
&\qquad + A_{87}A_{63}^4 + A_{87}A_{61}^8 + A_{61}^{64}A_{63}^6 + A_{61}^{72}A_{63}^2 + A_{63}^7A_{61}^8 + A_{63}^3A_{61}^{16} + A_{61}^4A_{63}^9 + A_{63}A_{61}^{20} \\
&\qquad + A_{61}^6A_{63}^8
\end{aligned}
$$

$$
\begin{aligned}
\sigma_{46} &:= A_{85}A_{61}^{2}A_{63}^{4} + A_{61}^{7}A_{63}^{8} + A_{61}^{23} + A_{87}^{4}A_{61}^{6} + A_{85}A_{61}^{10} \\
\sigma_{48} &:= A_{91}A_{63}^{2}A_{61}^{4} + A_{87}A_{61}^{2}A_{63}^{4} + A_{63}^{12} + A_{61}^{24} + A_{61}^{132} + A_{61}^{78} + A_{61}^{2} + A_{91}^{32} + A_{95}A_{61}^{6} + A_{91}A_{63}^{4} \\
&\quad + A_{91}A_{61}^{8} + A_{87}A_{61}^{10} + A_{63}A_{61}^{22} + A_{63}^{4}A_{61}^{16} + A_{61}^{4}A_{63}^{10} + A_{63}^{2}A_{61}^{20} + A_{61}^{6}A_{63}^{9} \\
\sigma_{50} &:= A_{91}^{4} + A_{85}A_{61}^{12} + A_{61}A_{63}^{12} + A_{63}^{4}A_{61}^{17} + A_{61}^{5}A_{63}^{10} + A_{63}^{2}A_{61}^{21} + A_{85}A_{63}^{2}A_{61}^{8} + A_{87}^{4}A_{63}^{2}A_{61}^{4} \\
&\quad + A_{61}^{25} + A_{61}^{133} + A_{87}^{4}A_{63}^{4} + A_{87}^{4}A_{61}^{8} + A_{85}A_{63}^{6} \\
\sigma_{52} &:= A_{61}^{4} + A_{63}^{2} + A_{61}^{64}A_{63}^{8} + A_{61}^{72}A_{63}^{4} + A_{61}^{76}A_{63}^{2} + A_{63}A_{61}^{24} + A_{63}A_{61}^{132} + A_{63}^{5}A_{61}^{16} + A_{61}^{4}A_{63}^{11} \\
&\quad + A_{63}^{3}A_{61}^{20} + A_{61}^{2}A_{63}^{12} + A_{63}^{4}A_{61}^{18} + A_{61}^{80} + A_{63}^{13} + A_{61}^{26} + A_{95}A_{63}^{2}A_{61}^{4} + A_{91}A_{61}^{2}A_{63}^{4} \\
&\quad + A_{87}A_{63}^{2}A_{61}^{8} + A_{95}A_{63}^{4} + A_{87}A_{61}^{12} + A_{91}^{32}A_{61}^{2} + A_{95}A_{61}^{8} + A_{87}A_{63}^{6} + A_{91}A_{61}^{10} + A_{85}^{2} \\
&\quad + A_{111} \\
\sigma_{54} &:= A_{87}^{4}A_{61}^{2}A_{63}^{4} + A_{85}A_{61}^{14} + A_{61}A_{85}^{2} + A_{61}^{3}A_{63}^{12} + A_{63}^{4}A_{61}^{19} + A_{61}^{27} + A_{87}^{4}A_{61}^{10} + A_{91}^{4}A_{61}^{2} \\
\sigma_{56} &:= A_{91}A_{63}^{2}A_{61}^{8} + A_{95}A_{61}^{2}A_{63}^{4} + A_{63}^{14} + A_{87}^{2} + A_{61}^{82} + A_{61}^{136} + A_{61}^{28} + A_{111}A_{61}^{2} + A_{91}^{32}A_{63}^{2} \\
&\quad + A_{91}^{32}A_{61}^{4} + A_{95}A_{61}^{10} + A_{91}A_{63}^{6} + A_{91}A_{61}^{12} + A_{87}A_{61}^{14} + A_{61}^{128}A_{63}^{4} + A_{61}^{66}A_{63}^{8} + A_{61}^{74}A_{63}^{4} \\
&\quad + A_{63}A_{85}^{2} + A_{63}^{2}A_{61}^{24} + A_{63}^{6}A_{61}^{16} + A_{61}^{2}A_{63}^{13} + A_{63}^{5}A_{61}^{18} + A_{63}A_{61}^{26} + A_{61}^{6} \\
\sigma_{58} &:= A_{85}A_{63}^{2}A_{61}^{12} + A_{85}A_{63}^{4}A_{61}^{8} + A_{87}^{4}A_{63}^{2}A_{61}^{8} + A_{87}^{16} + A_{61}^{129}A_{63}^{4} + A_{61}A_{63}^{14} + A_{61}A_{87}^{2} \\
&\quad + A_{63}^{2}A_{61}^{25} + A_{63}^{6}A_{61}^{17} + A_{61}^{137} + A_{61}^{29} + A_{91}^{4}A_{63}^{2} + A_{91}^{4}A_{61}^{4} + A_{87}^{4}A_{63}^{6} + A_{87}^{4}A_{61}^{12} \\
&\quad + A_{85}A_{63}^{8} + A_{85}A_{61}^{16}
\end{aligned}
$$

The other values are $\sigma_0 = 1$, by definition, and $\sigma_i = 0$ for odd i, given by the first identities.

After substitution of the σ_i's by their values, the remaining equations will be sorted in increasing size (number of monomials) order :

> 180, 188, 196, 192, 186, 184, 204, 200, 190, 252, 189, 119, 178, 182, 187, 212, 121, 194, 208, 220, 236, 198, 125, 185, 244, 191, 193, 202, 248, 197, 216, 228, 224, 123, 133, 195, 129, 206, 232, 250, 240, 205, 137, 141, 201, 181, 183, 246, 254, 218, 127, 199, 210, 173, 179, 203, 157, 253, 131, 214, 177, 149, 171, 234, 249, 139, 145, 153, 222, 242, 230, 135, 251, 169, 238, 245, 155, 165, 213, 221, 209, 207, 237, 241, 217, 226, 147, 175, 161, 143, 243, 163, 151, 211, 167, 247, 233, 235, 219, 159, 229, 225, 239, 227, 215, 231, 223

We will proceed as follow :

- we successively check the equations in the order given above, up to a "solvable" one.
- After solving one equation, we restart from the beginning.
  (*at each stage we substitute all the known A_i's, and we show the most simple equation possible*)

We will first show that $A_{61} \neq 0$

Suppose that $A_{61} = 0$, then :

$$I_{196} : \ \mathbf{A_{85}^3} = 0 \ \Rightarrow \ \mathbf{A_{85}} := 0,$$

$$I_{208}: \ \mathbf{A_{87}^6} = 0 \ \Rightarrow \ \mathbf{A_{87}} := 0,$$

$$I_{236}: \ 1 = 0,$$

so $A_{61} \neq 0$.

We give here in the resolution order all the "solvable" equations, and the way we used them.

$$I_{180} \ : \ A_{61}^8 A_{85} A_{63}^4 + A_{85} A_{63}^8 + A_{61}^4 \mathbf{A_{91}^4} + A_{61}^{29} + A_{61}^3 A_{85}^2 + A_{61}^{16} A_{85} + A_{61}^{12} A_{87}^4 + A_{87}^{16} = 0$$

$$\Rightarrow \ \mathbf{A_{91}} \ := \ A_{61} A_{85} A_{63} + A_{61}^{254} A_{85} A_{63}^2 + A_{61}^2 A_{87} + A_{61}^{70} + A_{61}^{191} A_{85}^2 + A_{61}^3 A_{85} + A_{61}^{254} A_{87}^4$$

$$\begin{aligned} I_{196} \ : \ & \mathbf{A_{95}^2} A_{61}^3 + A_{87}^8 A_{61} A_{63}^2 + A_{85}^2 A_{61} A_{63}^6 + A_{87}^2 A_{61}^3 A_{63}^4 + A_{85}^3 + A_{61}^{131} A_{63}^8 + A_{61}^{139} A_{63}^4 \\ & + A_{61}^{130} A_{87}^4 + A_{61}^5 A_{85}^2 A_{63}^4 = 0 \end{aligned}$$

$$\begin{aligned} \Rightarrow \ \mathbf{A_{95}} \ := \ & A_{61}^{126} A_{85}^3 + A_{61}^{254} A_{87}^4 A_{63} + A_{61}^{254} A_{85} A_{63}^3 + A_{87} A_{63}^2 + A_{61} A_{85} A_{63}^2 + A_{61}^{64} A_{63}^4 \\ & + A_{61}^{68} A_{63}^2 + A_{61}^{191} A_{87}^2 \end{aligned}$$

$$I_{192}: \ \mathbf{A_{85}^3} = 0 \ \Rightarrow \ \mathbf{A_{85}} = 0$$

$$I_{200}: \ 1 = 0$$

□

Annex C $B(511, 123)$ has minimum distance > 123

We consider the Newton's identities for $0 < i \leq n = 511$ for the code $B(511, 123)$, and for the weight $\delta = 123$. We want to prove that there exists no codeword of such weight.

The non-null power sum symmetric functions of the code are:

$$A_{123}, \ A_{125}, \ A_{127}, \ A_{171}, \ A_{175}, \ A_{183}, \ A_{187}, \ A_{191}, \ A_{219}, \ A_{223}, \ A_{239}, \ A_{255}.$$

And since 511 and 123 are relatively prime we can suppose $A_{123} = 1$.

We will show for this code a shorter proof. The complete proof would be too long to appear here.

We will first solve the linear triangular system giving the σ_i's for even i as polynomials depending on the non-null A_i's. The σ_i's for odd i are null. We consider that the σ_i's have been substituted in the equations.

Furthermore we will suppose $A_{125} \neq 0$ (when $A_{125} = 0$, we found a contradiction).

We give here the equations we used for the resolution, and the way we used them.

$$\begin{aligned}
I_{372} \quad : \quad & A_{125}^{63} + A_{171}^{8}A_{125}^{13} + A_{171}^{32}A_{125}^{5} + A_{171}^{4}A_{127}^{8}A_{125}^{22} + A_{171}^{4}A_{125}^{6}A_{127}^{16} + \mathbf{A_{187}^{4}}A_{125}^{6} \\
& + A_{175}^{16}A_{125}^{2} + A_{183}^{4}A_{125}^{14} + A_{171}^{4}A_{125}^{38} + A_{171}^{16}A_{127}^{8}A_{125}^{18} + A_{171}^{16}A_{125}^{2}A_{127}^{16} \\
& + A_{171}^{16}A_{127}^{4}A_{125}^{26} + A_{171}^{16}A_{125}^{34} + A_{175}^{4}A_{125}^{30} + A_{171}^{64}A_{125}^{2}A_{127}^{8} + A_{171}^{64}A_{127}^{4}A_{125}^{10} \\
& + A_{171}^{64}A_{125}^{18} = 0 \\
\Rightarrow \mathbf{A_{187}} \quad := \quad & A_{125}^{142} + A_{125}^{385}A_{171}^{2} + A_{125}^{383}A_{171}^{8} + A_{171}A_{127}^{2}A_{125}^{4} + A_{171}A_{127}^{4} + A_{125}^{3}A_{171}^{4}A_{127}^{2} \\
& + A_{125}^{510}A_{175}^{4} + A_{183}A_{125}^{2} + A_{171}A_{125}^{8} + A_{175}A_{125}^{6} + A_{125}^{510}A_{171}^{4}A_{127}^{4} \\
& + A_{125}^{5}A_{171}^{4}A_{127} + A_{171}^{4}A_{125}^{7} + A_{125}^{510}A_{171}^{16}A_{127}^{2} + A_{125}A_{171}^{16}A_{127} + A_{171}^{16}A_{125}^{3}
\end{aligned}$$

$$\begin{aligned}
I_{388} \quad : \quad & A_{171}^{8}A_{127}^{10} + A_{125}^{258}A_{127}^{16} + A_{175}^{4}A_{125}^{257} + A_{125}^{274}A_{127}^{8} + A_{125}^{282}A_{127}^{4} + A_{171}^{4}A_{125}^{257}A_{127}^{4} \\
& + A_{175}^{2}A_{127}^{4}A_{125}^{10} + A_{171}^{8}A_{127}^{6}A_{125}^{8} + A_{171}^{32}A_{127}^{6} + A_{175}^{2}A_{125}^{2}A_{127}^{8} + A_{175}^{8}A_{127}^{2} \\
& + A_{183}^{2}A_{125}^{2}A_{127}^{4} + \mathbf{A_{191}^{2}}A_{125}^{2} + A_{125}^{4}A_{171}^{32}A_{127}^{4} + A_{125}^{12}A_{171}^{8}A_{127}^{4} \\
& + A_{125}^{14}A_{171}^{2}A_{127}^{4} = 0 \\
\Rightarrow \mathbf{A_{191}} \quad := \quad & A_{125}^{510}A_{171}^{4}A_{127}^{5} + A_{125}^{128}A_{127}^{8} + A_{125}^{383}A_{175}^{2} + A_{125}^{136}A_{127}^{4} + A_{125}^{140}A_{127}^{2} + A_{125}^{383}A_{171}^{2}A_{127}^{2} \\
& + A_{175}A_{127}^{2}A_{125}^{4} + A_{125}^{3}A_{171}^{4}A_{127}^{3} + A_{125}^{510}A_{171}^{16}A_{127}^{3} + A_{175}A_{127}^{4} + A_{125}^{510}A_{175}^{4}A_{127} \\
& + A_{183}A_{127}^{2} + A_{171}^{16}A_{125}A_{127}^{2} + A_{171}^{4}A_{127}^{2}A_{125}^{5} + A_{125}^{6}A_{171}A_{127}^{2}
\end{aligned}$$

$$I_{392} : A_{125}^{2} + \mathbf{A_{171}^{6}} = 0 \Rightarrow \mathbf{A_{171}} := A_{125}^{341}$$

$$I_{404} : A_{127}^{2} + A_{125}^{340}\mathbf{A_{175}^{2}} = 0 \Rightarrow \mathbf{A_{175}} := A_{127}A_{125}^{341}$$

$$I_{412} : \mathbf{A_{125}^{97}} + 1 = 0 \Rightarrow \mathbf{A_{125}} := 1$$

$$I_{420} : \mathbf{A_{127}^{2}} + A_{183}^{2} + A_{183}^{4} = 0 \Rightarrow \mathbf{A_{127}} := A_{183} + A_{183}^{2}$$

$$I_{428} : 1 = 0$$

$\square$

References

[1] E.F. Assmus and J.D. Key. Affine and projective planes. *Discrete Mathematics*, 83:161–187, 1990.

[2] P. Charpin. Codes cycliques étendus affines-invariants et antichaînes d'un ensemble partiellement ordonné. *Discrete Mathematics*, 80:229–247, 1990.

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

[4] J-L. Dornstetter. Quelques resultats sur les codes BCH binaires en longueur 255. ENSTA stage report, Annex, July 1982.

[5] H.J. Helgert and R.D. Stinaff. Shortened BCH codes. *IEEE Transaction on Information Theory*, pages 818–820, November 1973.

[6] T. Kasami and S. Lin. Some results on the minimum weight of primitive BCH codes. *IEEE Transaction on Information Theory*, pages 824–825, November 1972.

[7] T. Kasami, S. Lin, and W.W. Peterson. Some results on cyclic codes which are invariant under the affine group and their applications. *Information and Control*, 11:475–496, 1967.

[8] T. Kasami, S. Lin, and W.W. Peterson. New generalisations of the Reed-Muller codes – Part I: Primitive codes. *IEEE Transaction on Information Theory*, 14(2):189–199, March 1968.

[9] T. Kasami and N. Tokura. Some remarks on BCH bounds and minimum weights of binary primitive BCH codes. *IEEE Transaction on Information Theory*, 15(3):408–413, May 1969.

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

[11] W. W. Peterson. *Error-Correcting Codes*. MIT Press, 1961.

[12] 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.