Open problems on cyclic codes**

Pascale Charpin [*]

Contents

1 Introduction 3

2 Different kinds of cyclic codes. 4
- 2.1 Notation . . . 5
- 2.2 Definitions . . . 6
- 2.3 Primitive and non primitive cyclic codes . . . 17
- 2.4 Affine-Invariant codes . . . 21
  - 2.4.1 The poset of affine-invariant codes . . . 22
  - 2.4.2 Affine-invariant codes as ideals of $\mathcal{A}$ . . . 28

3 On parameters of cyclic codes. 34
- 3.1 Codewords and Newton identities . . . 35
- 3.2 Special locator polynomials . . . 47
- 3.3 On the minimum distance of BCH codes . . . 59
- 3.4 On the weight enumerators . . . 65
  - 3.4.1 The Reed-Muller codes . . . 67
  - 3.4.2 On cyclic codes with two zeros . . . 71
  - 3.4.3 On irreducible cyclic codes . . . 83
- 3.5 Automorphism groups of cyclic codes . . . 88
- 3.6 Are all cyclic codes asymptotically bad ? . . . 90

[*] INRIA, Projet CODES, Domaine de Voluceau, Rocquencourt BP 105, 78153 Le Chesnay Cedex, FRANCE. e-mail: Pascale.Charpin@inria.fr

4 Related problems. 90
4.1 Some problems in cryptography 91
4.2 Cyclic codes and Goppa codes 96
4.3 On the weight enumerator of Preparata codes 104

5 Conclusion 117

** **"Handbook of Coding Theory", Part 1: Algebraic Coding, chapter 11,** V. S. Pless, W. C. Huffman, editors, R. A. Brualdi, assistant editor.

Warning. The Handbook of Coding Theory was published in 1998. Some research problems, presented as *Open problems* in this chapter, are solved, or partially solved, today.

1 Introduction

We do not intend to give an exhaustive account of the research problems on cyclic codes. Many are suggested in Chapter 1 and in several other chapters. There are chapters which deal with a specific class of cyclic codes or with related problems and it would be superfluous to say it again. Above all we want to avoid a boring enumeration of the open problems; many are just mentioned and could be solved soon.

Our purpose is to emphasize that this topic remains of great interest for researchers in coding theory. It is a fact that cyclic codes are crucial objects of coding theory. The involvement of Reed-Solomon codes and of BCH codes in a number of applications is well-known. On the other hand the generalized Reed-Muller codes are at the core of algebraic coding theory and they should be considered as “classical”. The reader can be convinced of the importance of cyclic codes by referring to the recent publications and proceedings including as a topic *Error-control Coding* or, more generally, *Coding Theory*. However there are famous *old* problems which have remained open for a long time and we have chosen to focus on them. They essentially involve questions of weights and forms of codewords.

Our concern is to place the problem in a large theoretical context. It can be the general behaviour of group algebras, or of polynomials over finite fields, or of the solving of algebraic systems. We want to show that general tools can be used here in an extremely rich environment. Furthermore we wish to point out any results on cyclic codes that apply in other contexts.

We give an elementary presentation, choosing simple aspects and basic results. We don’t want to develop a theory, or even to suggest a method precisely. It is because we have in mind that a hard research problem is generally solved by building a theory for solving it. The main recent illustration of this fact in coding theory is the explanation of the duality between Preparata and Kerdock codes.

We will often give results without proofs or with a sketch of a proof because of the special subject of our chapter. Generally we prefer to explain rather than to prove precisely. Following the same idea, we mainly treat binary codes, which are simpler to handle. BCH codes and GRM codes appear many times. This is because these classes impose the main filters of the general class of cyclic codes — it is usual, when we study any cyclic code, to begin by looking at their relations with BCH codes, or with GRM codes when the code is primitive. For this reason, any result on BCH codes or on GRM codes could have surprising consequences. In contrast, the Quadratic Residue codes , which form a famous class with remarkable properties, appear as a specific class.

The main notation and definitions are introduced in Section 2 and they will be held to afterwards. However they will be specified again as often as necessary. We don't give a series of “research problems”. We think that “comments” are more suited to our purpose. They are placed at the end of the sections; short sections have no comments. Our purpose or our choices are explained at the beginning of the main sections.

This chapter is not self-contained. We suppose that at least the introduction on cyclic codes given in Chapter 1 is known. Our main reference for the theory of finite fields is [102].

2 Different kinds of cyclic codes.

In this section we introduce cyclic codes. We present notation, basic definitions and fundamental tools or properties. However our main purpose is to describe the general context of our chapter.

Cyclic codes are defined as *group algebra codes.* We distinguish cyclic codes and extended cyclic codes, primitive and non primitive cyclic codes, simple-root and repeated-root cyclic codes. We then define several group algebras, but we emphasize that the ambient space of the primitive extended codes is the fundamental algebra. That is *the field algebra*, say $\mathcal{A}$, in which the extended cyclic codes appear as central objects. For this reason, we explain how a non primitive code can be seen as a primitive code. We also give an extensive study of the “cyclic ideals” of $\mathcal{A}$, completing those of Assmus and Key (chapter XXX).

On the other hand, any cyclic code satisfies a set of equations on an extension field, say $\mathbf{F}$. These are stated by means of several Fourier transforms. Any simple-root cyclic code is fully defined by this set of equations.

Therefore, the properties related with the structure of any group algebra, especially of $\mathcal{A}$, and the Fourier transforms, from such a group algebra to $\mathbf{F}$, appear as general tools for considering open problems on cyclic codes.

2.1 Notation

In accordance with Chapter 1, a cyclic code is viewed as an ideal in a polynomial ring over a finite field; it is characterized by its generator polynomial. In Chapter 1, the proper context for studying cyclic codes of length n over the finite field $\mathbf{k}$ of order q, $q = p^r$ and p a prime, is the residue class ring

$$\mathcal{R}_n = \mathbf{k}[X]/(X^n - 1).$$

Coordinate positions are labelled as $0, 1, \ldots, n-1$ and the cyclicity is the invariance under the shift $i \longmapsto i+1$. Our presentation here is not really different because it is relevant also to the one-variable approach, as opposed to that introduced by KASAMI, LIN and PETERSON in [85] where the cyclic codes are defined as *polynomial codes* — such a code corresponds to a set of polynomials in m variables. This approach, which is usual for the description of the generalized Reed-Muller codes, was later called *the m-variables approach* [64]. In our approach, any cyclic code is always described by means of polynomials with one indeterminate.

However we take into account the fact that the support of a cyclic code is always a cyclic group G^*, the group of the roots of $X^n - 1$. *Cyclic codes are group algebra codes.* So coordinate positions will be labelled as α^0, $\alpha^1, \ldots$, α^{n-1}, where α is a primitive nth root of unity. The cyclicity is the invariance under multiplication by α. Thereby the symbols of any codeword are the values of the Mattson-Solomon (MS) polynomial on each α^i. The MS polynomial will play an important role: actually our definition of cyclic codes is based on this concept.

Two finite fields are necessary for defining the ambient space. They are the alphabet field $\mathbf{k}$ and the full *support field* $\mathbf{F}$, the splitting field of $X^n - 1$ over $\mathbf{k}$. The order of $\mathbf{F}$ is $q^{m'}$, where q is the order of $\mathbf{k}$. As $q = p^r$, p is the characteristic of the ambient space; the field $\mathbf{F}$ will be generally identified with the field of order p^m, $m = rm'$.

By the notation G^* we want to emphasize that the group is multiplicative and does not contain zero; G^* is a subgroup of the multiplicative group of $\mathbf{F}$. So the notation G means $G^* \cup \{0\}$. When the codes are primitive, G^* is exactly the multiplicative group of the field $\mathbf{F}$ and then $G = \mathbf{F}$. For clarity, if necessary, we will denote by $GF(q)$ the finite field of order q.

2.2 Definitions

Let us denote by $\mathcal{M}$ the group algebra $\mathbf{k}[\{G^*, \times\}]$, which is the group algebra of the multiplicative group G^*, over the field of order q denoted by $\mathbf{k}$. An element of $\mathcal{M}$ is a formal sum:

$$\mathrm{x} = \sum_{g \in G^*} x_g(g) \quad , \quad x_g \in \mathbf{k} \ .$$

Addition and scalar multiplication are component-wise and multiplication is given by the multiplication in G^*:

$$\lambda \left(\sum_{g \in G^*} x_g(g) \right) = \sum_{g \in G^*} \lambda x_g(g) \ , \quad \lambda \in \mathbf{k} \ ,$$

$$\sum_{g \in G^*} x_g(g) + \sum_{g \in G^*} y_g(g) = \sum_{g \in G^*} (x_g + y_g)(g) \ ,$$

and

$$\sum_{g \in G^*} x_g(g) \times \sum_{g \in G^*} y_g(g) = \sum_{g \in G^*} \left(\sum_{hk=g} x_h y_k \right) (g) \ .$$

It is clear that the following map ψ is an automorphism between the algebras $\mathcal{R}_n$ and $\mathcal{M}$:

$$\mathrm{x}(X) \in \mathcal{R}_n, \ \mathrm{x}(X) = \sum_{i=0}^{n-1} x_i X^i \quad \longmapsto \quad \psi(\mathrm{x}(X)) = \sum_{i=0}^{n-1} x_i(\alpha^i) = \sum_{g \in G^*} x_g(g)$$

where α is an nth root of unity. So any cyclic code can be seen as a *group algebra code*, an ideal of $\mathcal{M}$, say *a code of* $\mathcal{M}$, the image by ψ of an ideal of $\mathcal{R}_n$. The *shift* of the codeword x is the codeword $\sum_{g \in G^*} x_g(\alpha g)$. Consider the following $\mathbf{k}$-linear map of $\mathcal{M}$ into $\mathbf{F}$:

$$\rho_s \left(\sum_{g \in G^*} x_g(g) \right) = \sum_{g \in G^*} x_g g^s \tag{1}$$

where $0 \leq s \leq n$. Note that $\rho_s(\mathrm{x}) = \mathrm{x}(\alpha^s)$ for any x in $\mathcal{M}$ corresponding to $\psi(\mathrm{x}(X))$. Moreover we have obviously:

$$\rho_0(\mathrm{x}) \in \mathbf{k} \ , \quad \rho_n(\mathrm{x}) = \rho_0(\mathrm{x}) \quad \text{and} \quad \rho_{qs}(\mathrm{x}) = (\rho_s(\mathrm{x}))^q \ . \tag{2}$$

Definition 2.1 *Let C be a cyclic code of length n over $\mathbf{k}$. The defining set T of C is the largest subset of the range $[0, n-1]$, invariant under the multiplication by q (mod n), such that any codeword $\mathrm{x} \in C$ satisfies*

$$\rho_s(\mathrm{x}) = 0 \ , \ \forall s \in T \quad .$$

The set T is a union of q-cyclotomic cosets modulo n; any $s \in T$ corresponds to a zero of C, say α^s, (see Chapter 1, Section 4).
Note that $[0, n-1]$ is the set of integers i with $0 \leq i \leq n-1$.

Let C be a code of $\mathcal{M}$. It is called a *simple-root* cyclic code when the characteristic p of the alphabet field $\mathbf{k}$ does not divide the length n. As is stated in the next definition, a simple-root cyclic code is uniquely defined by its defining set.

Definition 2.2 *Assume that n is prime to p. A cyclic code C of length n over $\mathbf{k}$, with defining set T can be defined as follows :*

$$C = \{ \ \mathrm{x} \in \mathcal{M} \mid \ \rho_s(\mathrm{x}) = 0 \ , \ \forall s \in T \ \} \ .$$

The dual $C^\perp$ of C is the cyclic code with defining set

$$T^\perp = \{ \ s \in [0, n-1] \mid n - s \notin T \ \} \ .$$

If p divides n, the code is said to be a *repeated-root* cyclic code . Such a cyclic code has length $n = p^\ell \delta$, for some ℓ and some δ prime with p. So the polynomial $X^n - 1$ is equal to $(X^\delta - 1)^{p^\ell}$. Hence it has δ distinct roots with multiplicity p^ℓ in its splitting field. That means that the general form of the generator polynomial of such a code is

$$g(X) = \prod_{i \in I} (g_i(X))^{k_i} \ , \quad k_i \in [1, p^\ell] \ ,$$

where g_i is the minimal polynomial of α^i over $\mathbf{k}$. In this case the defining set of the cyclic code does not define the code uniquely – i.e. the condition on the codewords given in Definition 2.1 is only a necessary condition. Henceforth, in the remainder of the chapter, a cyclic code will be implicitly a simple-root cyclic code, assuming that $gcd(n, p) = 1$. Although we will mainly treat cyclic codes, the repeated-root codes will be mentioned later several times.

The *Fourier transform* of any codeword x, referred to as the Mattson-Solomon (MS) polynomial , will be denoted by $M_{\mathrm{x}}(X)$. It is the polynomial

$$M_{\mathrm{x}}(X) = \sum_{s=0}^{n-1} \rho_{n-s}(\mathrm{x})\ X^s \ , \tag{3}$$

whose coefficients are in $\mathbf{F}$. The inverse of the MS polynomial is calculated by means of a simple argument. It is important to notice that M_{x} can be viewed as a mapping from G to $\mathbf{k}$. We have

$$M_{\mathrm{x}}(g) = \sum_{s=0}^{n-1} \left(\sum_{h \in G^*} x_h h^{n-s} \right) g^s = \sum_{h \in G^*} x_h \sum_{s=0}^{n-1} (gh^{-1})^s \ .$$

For any $\xi \in \mathbf{F}$ which is an nth root of unity the value of $\sum_{s=0}^{n-1} \xi^s$ is 0 if $\xi \neq 1$ and n otherwise – since it is equal to $(1-\xi^n)/(1-\xi)$. So we obtain:

$$M_{\mathrm{x}}(g) = (n\ mod\ p) x_g \ \ , \quad g \in G^* \ . \tag{4}$$

One obviously deduces from (4) that when $gcd(p, n) = 1$, the weight of x is n minus the number of roots of $M_{\mathrm{x}}(g)$. Note that one can define the MS polynomial of codewords when $gcd(n, p) \neq 1$, but it is generally not invertible. So it is of little interest for the codewords of a repeated-root cyclic code. Any codeword of $\mathcal{M}$ can be characterized by its MS polynomial but this tool is of most interest for the study of cyclic codes. In accordance with Definition 2.2 and with (3), (4), we can define a cyclic code by means of its MS polynomial.

Theorem 2.3 *Let T be a subset of the range $[0, n-1]$ which is invariant under multiplication by q (mod n). Denote by $\mathcal{L}$ the subspace of $\mathbf{F}^n$ whose elements are the n-tuples $(\Lambda_1, \ \ldots, \Lambda_n)$ satisfying*

$$\Lambda_{qs\ mod\ n} = (\Lambda_s)^q \quad \textit{and} \quad \Lambda_s = 0 \ \ \textit{for any } s \in T \ \ ,$$

Then there is a one-to-one correspondence Φ between the codewords of the cyclic code C with defining set T and the set of polynomials $\sum_{s=0}^{n-1} \Lambda_{n-s} X^s$, $(\Lambda_1, \ \ldots, \Lambda_n) \in \mathcal{L}$. This is the correspondence between a codeword and its MS polynomial:

$$\mathrm{x} \in C \ \ \longmapsto \ \Phi(\mathrm{x}) = \sum_{s=0}^{n-1} \ \Lambda_{n-s}\ X^s \ , \ \Lambda_{n-s} = \rho_{n-s}(\mathrm{x}) \ .$$

Note that the image of the shift of x *is as follows:*

$$\Phi\left(\sum_{g\in G^*} x_g(\alpha g)\right) \;=\; \sum_{s=0}^{n-1}\;\Lambda_{n-s}\;(\alpha^{-1}X)^s = M_{\rm x}(X/\alpha)\;. \tag{5}$$

One can say that the code C is formally defined by the polynomial

$$M_C(X) = \sum_{s=0}^{n-1}\Lambda_{n-s}\;X^s\;,$$

where $(\Lambda_1,\;\ldots,\Lambda_n)\in\mathcal{L}$.

Proof: We only need to verify that any polynomial

$$\Lambda(X) = \sum_{s=0}^{n-1}\;\Lambda_{n-s}\;X^s\quad,\quad(\Lambda_1,\;\ldots,\Lambda_n)\in\mathcal{L},$$

corresponds to a unique codeword x of C. As $\Lambda_{qs} = (\Lambda_s)^q$, $\Lambda(g)\in\mathbf{k}$ for all $g\in G$. So $\Lambda(X)$ is the MS polynomial of one and only one codeword x $\in\mathcal{M}$. Moreover x is in C because $\Lambda_s = 0$ for $s\in T$. It remains to prove (5). Set $\mathrm{x}' = \sum_{g\in G^*} x_g(\alpha g)$. By definition (see (1)) we have

$$\rho_j(\mathrm{x}') = \sum_{g\in G^*} x_g\alpha^j g^j = \alpha^j\sum_{g\in G^*} x_g g^j = \alpha^j\rho_j(\mathrm{x})\;.$$

Therefore

$$M_{\mathrm{x}'}(X) = \sum_{s=0}^{n-1}\rho_{n-s}(\mathrm{x}')\;X^s = \sum_{s=0}^{n-1}\alpha^{n-s}\rho_{n-s}(\mathrm{x})X^s = \sum_{s=0}^{n-1}\rho_{n-s}(\mathrm{x})(\alpha^{-1}X)^s\;,$$

completing the proof.

♦

Example 2.4 Let C be the binary cyclic code of length $n = 15$ with defining set

$$T = \{\;1,\;2,\;4,\;8,\;5,\;10\;\}\;;$$

T is the union of two cyclotomic cosets modulo 15 containing respectively 1 and 5. We have here $\mathbf{k} = GF(2)$, $m = 4$ and α is a primitive root of the field $\mathbf{F}$ of order 16. Then

$$G^* = \mathbf{F}^* = \{\;1,\;\alpha,\;\alpha^2,\;...,\;\alpha^{14}\;\}$$

and $\mathcal{M} = \mathbf{k}[\{G^*, \times\}]$. Recall that the cyclotomic cosets modulo 15 are

$$\{0\},\ \{1,2,4,8\},\ \ \{3,6,12,9\},\ \{5,10\},\ \{7,14,13,11\}\ .$$

With the notation of Theorem 2.3, we have $\Lambda_i = 0$ for any $i \in T$; $\mathcal{L}$ is the set of the n-tuples

$$(\ 0,\ 0,\ \Lambda_3,\ 0,\ 0,\ \Lambda_6,\ \Lambda_7,\ 0,\ \Lambda_9,\ 0,\ \Lambda_{11},\ \Lambda_{12},\ \Lambda_{13},\ \Lambda_{14},\ \Lambda_{15}\ ),$$

where the Λ_i satisfy $\Lambda_{2i\ mod\ 15} = \Lambda_i^2$. So

$$M_C(X) = \Lambda_3 X^{12} + \Lambda_3^2 X^9 + \Lambda_7 X^8 + \Lambda_3^8 X^6 + \Lambda_7^8 X^4 + \Lambda_3^4 X^3 + \Lambda_7^4 X^2 + \Lambda_7^2 X + \Lambda_{15}\ .$$

Recall that $\Lambda_{15} \in \{0,1\}$. Set $\epsilon = \Lambda_{15}$, $\lambda = \Lambda_3$ and $\mu = \Lambda_7$. Each codeword x of C is uniquely defined by a triple $(\epsilon, \lambda, \mu) \in \mathbf{F}^3$; its MS polynomial is as follows:

$$\begin{aligned} M_{\mathrm{x}}(X) &= \lambda X^{12} + \lambda^2 X^9 + \mu X^8 + \lambda^8 X^6 + \mu^8 X^4 + \lambda^4 X^3 + \mu^4 X^2 + \mu^2 X + \epsilon \\ &= \epsilon\ +\ Tr(\lambda^4 X^3 + \mu^2 X)\ , \end{aligned}$$

where Tr is the trace function from $\mathbf{F}$ to $\mathbf{k}$. Note that the code C contains $2(2^4)^2$ codewords; C has dimension 9. Consider the generating idempotent of C. That is the codeword y defined by $\epsilon = \lambda = \mu = 1$. We obtain the symbols of y by computing, for $i \in [0,14]$,

$$y_{\alpha^i} = M_{\mathrm{y}}(\alpha^i) = 1\ +\ Tr(\alpha^{3i} + \alpha^i)\ . \qquad (6)$$

Note that we have $y_{\alpha^{2i}} = y_{\alpha^i}$, since y is an idempotent. Assuming that $\mathbf{F}$ is defined by the primitive polynomial $X^4 + X + 1$, we have the following representation:

1	α	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}
0	0	0	1	0	0	1	1	0	1	0	1	1	1	1
0	0	1	0	0	1	1	0	1	0	1	1	1	1	0
0	1	0	0	1	1	0	1	0	1	1	1	1	0	0
1	0	0	0	1	0	0	1	1	0	1	0	1	1	1

It is easy to check that

$$Tr(1) = Tr(\alpha) = Tr(\alpha^5) = 0\ \text{ and }\ Tr(\alpha^3) = Tr(\alpha^7) = 1\ ,$$

implying, by using (6),

$$y_1 = y_{\alpha^3} = y_{\alpha^5} = y_{\alpha^7} = 1 \ \text{ and } \ y_\alpha = 0 \ .$$

So the codeword y is as follows

$$\mathrm{y} = \sum_{j \in J} (\alpha^j) \ , \quad J = \{0,3,6,9,12,5,10,7,11,13,14\} \ ,$$

where $\{\alpha^j \mid j \in J\}$ is the support of y; note that $wt(\mathrm{y}) = 11$. We can check that y is the generating idempotent of C by computing the $\rho_s(\mathrm{y})$. According to (1) we obtain

$$\rho_s(\mathrm{y}) = 1 + Tr(\alpha^{3s} + \alpha^{7s}) + \alpha^{5s} + \alpha^{10s} \ ,$$

providing

$$\rho_0(\mathrm{y}) = \rho_3(\mathrm{y}) = \rho_7(\mathrm{y}) = 1 \ \text{ and } \ \rho_1(\mathrm{y}) = \rho_5(\mathrm{y}) = 0 \ .$$

So we find again the coefficients of the MS polynomial of y — since $\rho_0 = \Lambda_{15}$ and $\rho_s = \Lambda_s$ for all non zero s.

At the end of this brief background to MS polynomials we want to recall a well-known theorem, called *Blahut's Theorem* in coding theory [29], providing the link between the weight of a codeword and its MS polynomial.

Theorem 2.5 *Let* $\mathrm{x} \in \mathcal{M}$ *and denote by* $\Lambda_1, \ \ldots, \Lambda_n$ *the coefficients of the MS polynomial of* x*. Then the weight of* x *is equal to the rank of the circulant matrix*

$$\mathcal{C}(\mathrm{x}) = \begin{pmatrix} \Lambda_n & \Lambda_{n-1} & \cdots & \Lambda_1 \\ \Lambda_1 & \Lambda_n & \cdots & \Lambda_2 \\ \vdots & \vdots & & \vdots \\ \Lambda_{n-1} & \Lambda_{n-2} & \cdots & \Lambda_n \end{pmatrix} ,$$

Proof: Recall that α is an nth root of unity. Let $\mathrm{x} = \sum_{g \in G^*} x_g(g)$. By definition (see (1) and (3)), we have for any i

$$\begin{pmatrix} \Lambda_i \\ \Lambda_{i+1} \\ \vdots \\ \Lambda_{i+n-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \alpha & \cdots & \alpha^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha^{n-1} & \cdots & (\alpha^{n-1})^{n-1} \end{pmatrix} \begin{pmatrix} x_1 \\ \alpha^i x_\alpha \\ \vdots \\ \alpha^{(n-1)i} x_{\alpha^{n-1}} \end{pmatrix}$$

Denote by L the $n \times n$ matrix above. By expressing each column of $\mathcal{C}(\mathrm{x})$ in the same way, it is easy to see that, up to rearrangement of columns:

$$\mathcal{C}(\mathrm{x}) = L \begin{pmatrix} x_1 & 0 & 0 & \cdots & 0 \\ 0 & x_\alpha & 0 & \cdots & 0 \\ \vdots & & & & \vdots \\ 0 & 0 & \cdots & 0 & x_{\alpha^{n-1}} \end{pmatrix} L \ .$$

Hence the rank of $\mathcal{C}(\mathrm{x})$ is equal to the number of non zero terms of the diagonal of the matrix above. That is exactly the weight of x.
♦

Example 2.6 As in Example 2.4, and later in Example 2.12, $\mathbf{k} = GF(2)$, $\mathbf{F} = GF(16)$ and α is a primitive root of the field $\mathbf{F}$. We consider here a binary cyclic code of length 5 ($\mathbf{F}$ is the splitting field of X^5+1). We choose a 5th root of unity, let $\beta = \alpha^3$; then $G^* = \{ \ \beta^i \mid i \in [0,4] \ \}$. The 2-cyclotomic cosets modulo 5 are

$$\{0 \text{ or } 5\} \ , \quad \{1, \ 2, \ 4, \ 3\} \ .$$

Consider the code C with defining set $T = \{0\}$. Actually C is the $[5,4,2]$ irreducible binary cyclic code whose weight enumerator is obviously

$$W_C(x,y) = x^5 + 10x^3y^2 + 5xy^4 \ .$$

The MS polynomial of C is

$$M_C(X) = \Lambda_4 X + \Lambda_3 X^2 + \Lambda_2 X^3 + \Lambda_1 X^4 \ .$$

Set $\lambda = \Lambda_1$. Any $\lambda \in \mathbf{F}$ defines one and only one codeword of C. For instance the MS polynomial of the generating idempotent y is

$$M_{\mathrm{y}}(X) = X + X^2 + X^3 + X^4 = \frac{X^5+1}{X+1} + 1 \ .$$

This polynomial has exactly one root in G^*, $X = 1$, implying $wt(\mathrm{y}) = 4$. On the other hand, consider the circulant matrix $\mathcal{C}(\mathrm{y})$ (with notation of Theorem 2.5)

$$\mathcal{C}(\mathrm{y}) = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix} ,$$

It is easy to check that the rank of $\mathcal{C}(\mathrm{y})$ is exactly 4. Note that both methods, especially the second, necessitate a computer, except for such very simple cases.

Whenever T does not contain 0, we *extend the code C by an overall parity check* (see Chapter 1, Section 2). We denote by $\widehat{C}$ the *extended code* of C:

$$\widehat{C} = \left\{ (-\sum_{g\in G^*} x_g)(0) + \sum_{g\in G^*} x_g(g) \mid \sum_{g\in G^*} x_g(g) \in C \right\} . \tag{7}$$

By convention the attached symbol is labelled by 0 and the defining set of $\widehat{C}$ is $T \cup \{0\}$. The extended code is defined with one more equation. An extended codeword is in $\widehat{C}$ if and only if it satisfies

$$\sum_{g\in G} x_g g^0 = 0 \quad \text{and} \quad \rho_s(\mathrm{x}) = 0,\ s \in T\ ,$$

where $0^0 = 1$. The support of $\widehat{C}$ is now the set G. These conventions will have a clear meaning for primitive codes. Conversely we say that C is the code obtained from $\widehat{C}$ by puncturing at the element $0 \in G$: *C is the punctured code of $\widehat{C}$*.

A code of length p^m-1 (or p^m), over a field of characteristic p, is generally said to be primitive. Suppose that $n = p^m - 1$, for some m. Then the codes C and $\widehat{C}$ are respectively said to be *primitive cyclic* and *primitive extended cyclic*. In that case G equals $\mathbf{F}$, the splitting field of $X^n - 1$. We can take as ambient space the algebra of the additive group of $\mathbf{F}$ over $\mathbf{k}$. This algebra will be denoted by $\mathcal{A}$, $\mathcal{A} = \mathbf{k}[\{G, +\}]$. In order to avoid confusion we will use the notation $\mathbf{F}$ instead of G in this context. An element of $\mathcal{A}$ is a formal sum:

$$\mathrm{x} = \sum_{g\in\mathbf{F}} x_g X^g \quad , \quad x_g \in \mathbf{k}\ .$$

The operations are:

$$\sum_{g\in\mathbf{F}} x_g X^g + \sum_{g\in\mathbf{F}} y_g X^g = \sum_{g\in\mathbf{F}} (x_g + y_g) X^g\ ,$$

and

$$\sum_{g\in\mathbf{F}} x_g X^g \times \sum_{g\in\mathbf{F}} y_g X^g = \sum_{g\in\mathbf{F}} \left(\sum_{h+k=g} x_h y_k \right) X^g\ .$$

Note that X^0 is the multiplicative unit. As previously (for the algebra $\mathcal{M}$) we consider the **k**-linear map of $\mathcal{A}$ into **F**:

$$\phi_s \left(\sum_{g \in \mathbf{F}} x_g X^g \right) = \sum_{g \in \mathbf{F}} x_g g^s \tag{8}$$

where $0 \le s \le n$ and $0^0 = 1$.

Definition 2.7 *Let the ambient space be* $\mathcal{A} = \mathbf{k}[\{\mathbf{F}, +\}]$. *Let* T *be a subset of* $[0, n]$, *containing* 0 *and invariant under multiplication by* q *(mod* n*). The extended cyclic code* $\widehat{C}$ *with defining set* T *is defined as follows:*

$$\widehat{C} = \{ \ \mathrm{x} \in \mathcal{A} \mid \ \phi_s(\mathrm{x}) = 0 \ , \ \forall s \in T \ \} \ .$$

The code $\widehat{C}$ *is said to be an extended cyclic code in* $\mathcal{A}$. *The dual of* $\widehat{C}$ *is also an extended cyclic code. Its defining set is the set of those* s *such that* $n - s$ *is not in* T.

When we consider cyclic codes in $\mathcal{A}$, rather than in $\mathcal{M}$, we place these codes in the general ambient space of primitive codes of length p^m (extended cyclic or not). New operations, and then new tools, appear. The algebra $\mathcal{A}$ is actually a *field algebra*. Since the multiplication in **F** involves the shift on codewords, this point of view is of most interest for cyclic codes. But, conversely, the field algebra $\mathcal{A}$ is the appropriate ambient space for the study of any relation between a given primitive code and some cyclic codes. We will develop, or illustrate, these ideas several times in this chapter.

Remark on the functions ρ_s and ϕ_s. The mappings ρ_s are defined for $0 \le s \le n$, but we noticed that $\rho_n = \rho_0$. Definition 2.1 is classical, taking into account that $\alpha^0 = \alpha^n$.

For the definition of the extended code $\widehat{C}$ we must differentiate between 0 and n. We have, by convention,

$$\phi_0 \left(\sum_{g \in \mathbf{F}} x_g X^g \right) = \sum_{g \in \mathbf{F}} x_g \quad \text{and} \quad \phi_n \left(\sum_{g \in \mathbf{F}} x_g X^g \right) = \sum_{g \in \mathbf{F}^*} x_g \ .$$

By definition, any extended code in $\mathcal{A}$ satisfies $\phi_0(\mathrm{x}) = 0$, for any codeword x. Generally n is not in the defining set of $\widehat{C}$. If it is, it means that α^0 is a zero of the code C. So the extension of C is not really an extension. One simply considers C in the ambient space $\mathcal{A}$.

The mapping ϕ_n is more interesting for the study of subcodes of $\widehat{C}$. In any code $\widehat{C}$, we have the subcode containing the codewords x satisfying $\phi_n(\mathrm{x}) = 0$. This subcode can be seen as the extension of the cyclic subcode of C containing α^0 as zero. When C is binary, this is the subcode of codewords of even weight.

Finally we want to recall the definition of three "classical" classes of cyclic codes: the Generalized Reed-Muller (GRM) codes, the Bose-Chaudhury-Hocquenghem (BCH) codes, and the Quadratic Residue (QR) codes.

Definition 2.8 *Let the ambient space be $\mathcal{A}$; $n = q^{m'} - 1$, $q = p^r$ and $m = m'r$. For any q and any $s \in [0, n]$, the q-weight of s denoted by $wt_q(s)$ is*

$$wt_q(s) = \sum_{i=0}^{m'-1} s_i \ ,$$

where $\sum_{i=0}^{m'-1} s_i q^i$ is the q-ary expansion of s. The GRM code of order ν, $0 \leq \nu < m'(q-1)$, is the extended cyclic code over the field $\mathbf{k} = GF(q)$ with defining set

$$T_\nu = \{ \ s \in [0, n] \mid 0 \leq wt_q(s) < m'(q-1) - \nu \ \}.$$

This code is of length $p^m = q^{m'}$ and is denoted by $\mathcal{R}_q(\nu, m)$ while its punctured code is denoted by $\mathcal{R}_q^*(\nu, m)$. Binary Reed-Muller codes are usually called Reed-Muller (RM) codes. More generally, a GRM code defined on a prime field of order p is called a p-ary RM code.

Definition 2.9 *Let the ambient space be $\mathcal{M}$. Let δ be an integer in the range $[1, n-1]$ which is the smallest representative of a cyclotomic coset of q modulo n. The BCH code of designed distance δ is the cyclic code with defining set*

$$T_\delta = \bigcup_{s \in [1, \delta - 1]} cl(s) \ ,$$

where $cl(s)$ is the cyclotomic coset of q modulo n containing s.
When $n = p^m - 1$ and $\mathbf{k}$ is the field of order p^m, then $cl(s) = \{s\}$ and $T_\delta = [1, \delta - 1]$ is the defining set of the Reed-Solomon (RS) code of length n and minimum distance δ over $\mathbf{k}$.

Definition 2.10 *Let the ambient space be $\mathcal{M}$ with two further conditions:*

1. *the length n is an odd prime;*
2. *the order q of the alphabet field $\mathbf{k}$ is a quadratic residue modulo n — in other words, q is such that $q^{(n-1)/2} \equiv 1 \pmod{n}$.*

Denote by $\mathcal{Q}$ the set of the quadratic residues in the finite field F_n of order n and by $\mathcal{N}$ the set of non residues:

$$\mathcal{Q} = \{\ s^2 \pmod{n} \mid s \in F_n,\ s \neq 0\ \}\ .$$

Then the codes with defining sets

$$\mathcal{Q}\ ,\quad \{0\} \cup \mathcal{Q}\ ,\quad \mathcal{N}\ ,\quad \{0\} \cup \mathcal{N}\ ,$$

are the quadratic residue codes.

Comments on Section 2.2 There are few papers about the class of repeated-root cyclic codes. Some special such codes, related to RM codes, were studied by Berman in [25] (see also [114] where the practical interest is explained). Binary self-dual codes which are cyclic are repeated-root cyclic codes; some properties are given in [132]. The most important work on repeated-root cyclic codes is due to Castagnoli et al. [46, 1991]. The authors treat the full class and present general results. Actually they introduce the theory. They show precisely how some parameters of a repeated-root cyclic code can be expressed from those of a certain simple-root cyclic code. Thereby the repeated-root cyclic codes cannot be "better" than simple-root cyclic codes. However these codes appear more evidently as interesting objects. Complements are given in [113]. On the other hand, van Lint has described the binary cyclic codes of length $2n$, n odd, by means of the well-known $|u|u+v|$ construction [140]. The repeated-root cyclic codes, considered as ideals in a group algebra, have been extensively studied by Zimmermann [154].

The weight enumerators of GRM codes, BCH codes and QR codes are not always known, except RS codes, since they are MDS codes, and some particular codes (such as the Hamming codes). For the RS codes the question is to determine their complete weight enumerators. The minimum distance of GRM codes is known (see comments of Section 3.2 and 3.4.1). This is generally not known for BCH codes and QR codes. The automorphism groups of GRM codes, QR codes and narrow-sense BCH codes are known (see Chapter(Huffman) and §3.5). There is no decoding algorithm known for QR codes.

2.3 Primitive and non primitive cyclic codes

In this section we want to show that any non primitive cyclic code can be considered as a primitive cyclic code. More precisely it can be viewed in the ambient space of the primitive cyclic codes. Therefore the extended code can be viewed as a code of $\mathcal{A}$.

We need to be more precise; in particular we take specific notation (only for this section). Assume that

$$N = p^m - 1 \ , \quad N = n\nu \ , \quad n < N \ .$$

The finite field of order p^m is denoted by $\mathbf{F}$ and G^* is the cyclic subgroup of $\mathbf{F}$ of order n generated by β, a primitive nth root of unity. We choose α, a primitive element of the field $\mathbf{F}$, such that $\beta = \alpha^\nu$. Recall that the alphabet field $\mathbf{k}$ is a subfield of $\mathbf{F}$. Note that, in this section, the mappings ρ_s apply to the codewords of $\mathbf{k}[\{\mathbf{F}^*, \times\}]$.

Denote by C a non primitive cyclic code. It is a code of length n over $\mathbf{k}$ with defining set $T(C)$. Then the set of zeros of C is the set $\{\beta^j \mid j \in T(C)\}$, as well as the set $\{\alpha^{j\nu} \mid j \in T(C)\}$. Consider the cyclic code D of length N over $\mathbf{k}$ with defining set

$$T(D) = \ [\ 0,\ N-1\ ] \setminus \{\ j\nu \mid j \in [0, n-1],\ j \notin T(C)\ \}\ . \tag{9}$$

Thereby the non-zeros of D are exactly the non-zeros of C. Let $\mathrm{x} \in D$ and consider its MS polynomial. By definition and since $\rho_j(\mathrm{x}) = 0$ for any j in the defining set of D, we have

$$M_{\mathrm{x}}(X) = \sum_{\substack{0 \le s \le N-1 \\ N-s \notin T(D)}} \rho_{N-s}(\mathrm{x})\ X^s = \sum_{\substack{0 \le t \le n-1 \\ n-t \notin T(C)}} \rho_{(n-t)\nu}(\mathrm{x})\ X^{t\nu}$$

(see Definition 2.1 and (3)). Now we compute the symbols of x by the inverse Fourier transform; we obtain

$$N\ x_{\alpha^i}\ =\ M_{\mathrm{x}}(\alpha^i)\ , \quad i \in [0, N-1]\ .$$

Set $i = ni_1 + i_2$ with $0 \leq i_2 < n$. We have

$$M_{\mathrm{x}}(\alpha^i) = \sum_{\substack{0 \leq t \leq n-1 \\ n-t \notin T(C)}} \rho_{(n-t)\nu}(\mathrm{x})\alpha^{t\nu(ni_1+i_2)} = \sum_{\substack{0 \leq t \leq n-1 \\ n-t \notin T(C)}} \rho_{(n-t)\nu}(\mathrm{x})\beta^{ti_2} , \tag{10}$$

since $\alpha^\nu = \beta$ and $\beta^n = 1$. Hence

$$M_{\mathrm{x}}(\alpha^{ni_1+i_2}) = M_{\mathrm{x}}(\alpha^{i_2}) \ , \ \ i_1 \in [0, \nu-1] \ , \ \ i_2 < n \ ,$$

which means $x_{\alpha^i} = x_{\alpha^{i_2}}$ for $i \equiv i_2$ modulo n. Now we take $(\Lambda_1, \ \ldots, \Lambda_n) \in \mathbf{F}^n$ such that $\Lambda_j = \rho_{j\nu}(\mathrm{x})$. Consider the codeword y in C whose MS polynomial is

$$M_{\mathrm{y}}(X) = \sum_{\substack{0 \leq t \leq n-1 \\ n-t \notin T(C)}} \Lambda_{n-t}X^t \ .$$

According to (10), we have for any $i_2 \in [0, n-1]$:

$$M_{\mathrm{y}}(\beta^{i_2}) = M_{\mathrm{x}}(\alpha^{i_2}) \ ,$$

which means

$$y_{\beta^{i_2}} = (N/n \ mod \ p) \ x_{\alpha^{i_2}} = (\nu \ mod \ p) \ x_{\alpha^{i_2}} \ , \ \ i_2 \in [0, n-1] \ .$$

On the other hand, any primitive cyclic code whose defining set is of the form (9), for some $T(C)$ which is invariant under the multiplication by q (mod n), corresponds to a non primitive cyclic code. We summarize this in the next proposition (with notation introduced above).

Proposition 2.11 *The cyclic code D is the "primitive form" of the code C. Any codeword* $\mathrm{x} = \sum_{g \in \mathbf{F}^*} x_g(g)$ *of D is obtained from a codeword* $\mathrm{y} = \sum_{g \in G^*} y_g(g)$ *by repetition of symbols. That is:*

$$\mathrm{x} = \sum_{i=0}^{N-1} x_{\alpha^i}(\alpha^i) = \sum_{j=0}^{n-1} x_{\alpha^j} \sum_{i \ mod \ n = j} (\alpha^i)$$

and

$$\mathrm{y} = \sum_{j=0}^{n-1} y_{\beta^j}(\beta^j) = (\nu \ mod \ p) \sum_{j=0}^{n-1} x_{\alpha^j}(\beta^j) \ .$$

Therefore $wt(\mathrm{x}) = \nu \ wt(\mathrm{y})$.

To conclude we would like to illustrate the link between the *irreducible cyclic codes* and some *diagonal equations*. Suppose that C is an irreducible cyclic code of length n over $\mathbf{k}$. Then, up to equivalence, it is the code of $\mathcal{M}$ which has as non zeros only β^{-1} and its conjugates. Let $cl(-1)$ be the q-cyclotomic coset of -1 modulo n. So

$$T(C) = [0, n-1] \setminus \ cl(-1) \ .$$

(see Chapter 1, Theorem 5.25). Consider the code D, as previously defined from C. According to (9) we have:

$$T(D) = [0, N-1] \setminus \ \{ \ -\nu, \ \ -q\nu \ , \ \ \ldots, \ (-q^{m-1}\nu) \ mod \ N \ \} \ ,$$

implying that the defining set of the dual of D is the q-cyclotomic coset of ν modulo N. Let us consider the equations over $\mathbf{F}$ of the type

$$a_1 X_1^\nu \ + \ \ldots \ + \ a_w X_w^\nu \ = \ 0 \ , \qquad (11)$$

where $a_i \in \mathbf{k}$ and w is an integer greater than two. They are diagonal equations with a constant exponent over $\mathbf{F}$ [102, Chapter 6]. A solution of (11) is a w-tuple $(g_1, \ldots, g_w)$, $g_i \in \mathbf{F}$, satisfying $\sum_{i=1}^{w} a_i g_i^\nu = 0$. Suppose that such a solution S is composed of k pairwise distinct nonzero elements, say $g_1, \ldots, g_k$, and of $w-k$ zeros. Then it corresponds to the codeword

$$\mathrm{x} = \sum_{i=1}^{k} a_i(g_i) \ , \quad \mathrm{x} \in \mathbf{k}[\{\mathbf{F}^*, \times\}] \ .$$

As the g_i satisfy (11), $\rho_\nu(\mathrm{x}) = 0$. Hence x is a codeword of $D^\perp$ of weight k. More generally *any codeword of $D^\perp$ of weight less than or equal to w provides a solution of an equation of type (11).*

In the binary case, the connection with the weight enumerator of a given irreducible cyclic code is more clear and of most interest. Indeed if $\mathbf{k}$ is the field of order two, the knowledge of the solutions of the diagonal equations

$$X_1^\nu \ + \ \ldots \ + \ X_w^\nu \ = \ 0 \qquad (12)$$

over $\mathbf{F}$, for any w, is equivalent to the knowledge of the weight enumerator of the code C. More precisely *the number of the codewords of weight w in $D^\perp$ is equal to the number of the solutions S of (12) composed of w distinct non zero elements of* $\mathbf{F}$. The weight enumerator of C can be obtained from the one of D.

Example 2.12 Let $N = 15$ and $n = 5$; so $\mathbf{F} = GF(16)$ and $\nu = 3$. Consider the binary cyclic code D of length 15 with defining set

$$T(D) = \{ \ s \in [0,15] \mid s \notin \{3,6,12,9\} \ \}.$$

That is the binary cyclic code with *only one non zero class*, α^3 (and its conjugates). So its dimension is 4. The diagonal equations (12) providing the weight enumerator of $D^\perp$ are

$$X_1^3 \ + \ \ldots \ + \ X_w^3 \ = \ 0 \ \ , \quad 0 \leq w \leq 15 \ ,$$

with solutions in $GF(16)$. The MS polynomial of any $\mathrm{x} \in D$ is

$$\begin{aligned} M_{\mathrm{x}}(X) &= \rho_3(\mathrm{x})X^{12} + \rho_6(\mathrm{x})X^9 + \rho_9(\mathrm{x})X^6 + \rho_{12}(\mathrm{x})X^3 \\ &= \lambda(X^3)^4 + \lambda^2(X^3)^3 + \lambda^8(X^3)^2 + \lambda^4X^3 \ , \end{aligned}$$

where $\lambda = \rho_3(\mathrm{x})$ is any element in $\mathbf{F}$. We remark that by taking $Y = X^3$ we obtain the MS polynomial of some codeword of the code C of Example 2.6. We have, for $0 \leq i_1 \leq 2$ and $0 \leq i_2 \leq 4$,

$$M_{\mathrm{x}}(\alpha^{5i_1+i_2}) = M_{\mathrm{x}}(\alpha^{i_2}) \ .$$

Actually *the code D is the primitive form of the code C* of Example 2.6. Indeed the set of non-zeros of D and C are respectively

$$\{3 \times 1, \ 3 \times 2, \ 3 \times 4, \ 3 \times 3 \ \} \quad \text{and} \quad \{1, \ 2, \ 4, \ 3\}$$

and that is exactly definition (9). According to Proposition 2.11, D is a $[15,4,6]$ code whose weight enumerator is

$$W_D(x,y) = x^{15} + 10x^9y^6 + 5x^3y^{12} \ ,$$

since each codeword of D is obtained from only one codeword of C by repetition of each symbol three times. The non-zero weights of codewords of C are 2 and 4 so that they are respectively 6 and 12 for the code D. By way of illustration, consider the idempotents of these codes. Denote by z the idempotent of D. We have

$$M_{\mathrm{z}}(X) = X^{12} + X^9 + X^6 + X^3 = \frac{X^{15}-1}{X^3-1} + 1 \ .$$

The zeros of $M_{\rm z}(X)$ are those α^k such that $\alpha^{3k} = 1$. The idempotent of C was denoted by y; we showed that its MS polynomial is equal to $(X^5 - 1)/(X-1)+1$. In $\mathbf{k}[G^*, \times]$, where G^* is generated by β, we have

$$\mathrm{y} = (\beta) + (\beta^2) + (\beta^3) + (\beta^4)$$

providing in $\mathbf{k}[\mathbf{F}^*, \times]$

$$\begin{aligned} \mathrm{z} &= (\alpha) + (\alpha^{n+1}) + (\alpha^{2n+1}) + (\alpha^2) + (\alpha^{n+2}) + (\alpha^{2n+2}) + \\ &\quad (\alpha^3) + (\alpha^{n+3}) + (\alpha^{2n+3}) + (\alpha^4) + (\alpha^{n+4}) + (\alpha^{2n+4}) \\ &= (\alpha) + (\alpha^2) + (\alpha^4) + (\alpha^8) + (\alpha^3) + (\alpha^6) + \\ &\quad (\alpha^9) + (\alpha^{12}) + (\alpha^7) + (\alpha^{11}) + (\alpha^{13}) + (\alpha^{14}) \ . \end{aligned}$$

Note that the supports of y and z satisfy the property characterizing idempotents: they are invariant under the Frobenius mapping.

Comments on Section 2.3 The link between diagonal equations and irreducible cyclic codes was extensively studied by WOLFMANN [148, 149]. Previously, HELLESETH [77] and TIETÄVÄINEN [136] studied this approach for finding the covering radius of codes. The problem of solving diagonal equations of type (11) is related to famous problems such as WARING's problem.

It is often efficient to consider an irreducible cyclic code in its primitive form. An application can be found in [150]. In [55], this point of view is decisive for the determination of the weight distributions of cosets of 2-error-correcting binary BCH codes. It is generalized in [56].

2.4 Affine-Invariant codes

In this section, we consider codes of $\mathcal{A}$ — i.e. of the field algebra of the primitive extended codes. Addition and multiplication in the field $\mathbf{F}$ involve natural transformations on codewords including the following *affine permutations*

$$\sigma_{u,v} \ : \ \sum_{g\in\mathbf{F}} x_g X^g \ \longmapsto \ \sum_{g\in\mathbf{F}} x_g X^{ug+v} \ , \quad u \in \mathbf{F}^*, \ v \in \mathbf{F} \ . \qquad (13)$$

The permutations $\sigma_{u,0}$ consist of shifting symbols unless the symbol is labelled by 0. It is exactly the shift on codewords punctured in the position "0". On the other hand we have clearly

$$\sigma_{1,v}(\mathrm{x}) = X^v \mathrm{x} \ .$$

Thus a code C, which is invariant under the permutations $\sigma_{u,v}$, is an extended cyclic code and an ideal of $\mathcal{A}$. Such a code is called *an affine-invariant code* .

We will develop a combinatorial approach to affine-invariant codes, by defining the *poset of affine-invariant codes*. Each affine-invariant code can be identified with one and only one antichain of the poset $(S, \preceq)$, $S = [0, n]$. This leads to a classification, which is purely combinatorial. But it is most surprising that a given antichain contains much information about the code that it defines. This will provide tools useful in applications. In particular, with this point of view, the connection with the general representation of the ideals of $\mathcal{A}$ is established. For instance, the principal ideals, which are extended cyclic codes, are easily characterized. Finally a result on maximal antichains, due to Griggs, can be applied.

By our approach we complete the algebraic study of Assmus and Key (Chapter XXX Section 4). We do not give the complete proofs of results because our aim is mainly to suggest another context or other extensions. Moreover some of them can be found in Chapter(Assmus-Key). The main references are [51] and [52]. The results (and terminology) on antichains are those of Griggs [73].

2.4.1 The poset of affine-invariant codes

Affine-invariant codes were characterized by Kasami et al. in [87]. The authors showed that an extended cyclic code is affine-invariant if and only if its defining set satisfies a certain combinatorial property. We will present this result (Theorem 2.14) in terms of a partial order.

Definition 2.13 *Let $S = [0, p^m - 1]$. The p-ary expansion of $s \in S$ is $\sum_{i=0}^{m-1} s_i p^i$, $s_i \in [0, p-1]$. We denote by $\preceq$ the partial order relation on S defined as follows:*

$$\forall \ s,t \in S \ : \quad s \preceq t \quad \Longleftrightarrow \quad s_i \leq t_i \ , \ \ i \in [0, m-1]$$

($s \prec t$ means $s \preceq t$ and $s \neq t$).
Then we can define the poset $(S, \preceq)$. When $s \preceq t$, s is said to be a

descendant of t and t to be an ascendant of s. We can define a maximal (resp. minimal) element of a subset of S, with respect to $\preceq$. Two elements, s and t, are not related when they are distinct and are such that $s \not\preceq t$ and $t \not\preceq s$. An antichain *of $(S, \preceq)$ is a set of non-related elements of S. In the usual terminology, $(S, \preceq)$ is said to be a product of chains of size p.*

Theorem 2.14 *Let us define the map*

$$\Delta \,:\, T \subset S \quad\longmapsto\quad \Delta(T) = \bigcup_{t \in T} \{s \in S,\ s \preceq t\}\ . \tag{14}$$

Let C be an extended cyclic code, with defining set T. Then C is affine-invariant if and only if $\Delta(T) = T$.

Let $T \subset S$. The *border* of T is the antichain I of $(S, \preceq)$ consisting of the minimal elements of the set $S \setminus T$. It is easy to check the following:

$$I = \{\ s \in S \setminus T \ \mid\ \Delta(s) \setminus \{s\} \subset T\ \} \tag{15}$$

where $\Delta(s) = \Delta(\{s\})$. For simplification we will often say *the border of the code C*, with defining set T, instead of the border of T. Many extended cyclic codes have the same border. However one and only one affine-invariant code corresponds to a given antichain, providing the classification of the affine-invariant codes via antichains of $(S, \preceq)$.

Theorem 2.15 *There is a one-to-one correspondance between antichains of $(S, \preceq)$ and affine-invariant codes of length p^m. Each antichain is the border of one and only one affine-invariant code.*

Proof: Let I be an antichain of $(S, \preceq)$ and define the following subset of S:

$$T = S \ \setminus\ \bigcup_{f \in I} \{\ s \in S \mid f \preceq s\ \} = \bigcap_{f \in I} \{\ t \in S \mid f \not\preceq t\ \}\ .$$

It is clear that the two definitions of T above are equivalent. By definition $\Delta(T) = T$ and I is the border of T. So we can define the affine-invariant code C with defining set T and border I.

Suppose now that a subset T' of S, such that $\Delta(T') = T'$, also has border I. It is impossible to have $s \in T'$ and $f \preceq s$, for some $f \in I$, since I is the border of T'. So T' is included in T. If there exists an $s \in T \setminus T'$, then T contains any descendant of s. In particular T contains a descendant of s which is in the border of T', a contradiction. Hence $T' = T$.

♦

When the defining set of any cyclic code is precisely described, it is easy to check if this code is affine-invariant or not. For instance, GRM codes and extended narrow-sense BCH codes are obviously affine-invariant. It is more difficult to determine the border of any affine-invariant code; generally one has to make do with numerical results, by using a computer. However, in some cases, it is possible to prove exactly what the border is. We present below two results: the borders of p-ary RM codes and the borders of extended RS codes. We give the proof of the first one; the proof of the second one, which is more technical, can be found in [52]. Note that the RM codes have, as borders, maximal antichains while the border of any extended RS code of length p^m cannot have more than m elements.

Proposition 2.16 *The border of the p-ary RM code of length p^m and order ν, denoted by $\mathcal{R}_p(\nu, m)$ with $0 \le \nu < m(p-1)$, is*

$$S_\mu = \{ \ t \in S \mid wt_p(t) = \mu \ \} \quad \textit{where} \quad \mu = m(p-1) - \nu \ .$$

Such an antichain S_μ is said to be a maximal antichain of constant rank.

Proof: GRM codes are defined in Definition 2.8. In the terminology of partial order, the p-weight of any $s \in S$ is said to be the *rank* of s. Two distinct elements with the same p-weight are not related, with respect to $\preceq$. So a set of elements of the same p-weight is an antichain, which is called *an antichain of constant rank* [73]. An antichain is said to be maximal if it is not included in a bigger antichain. Clearly, the antichain S_μ is maximal.

Recall that $wt_p(s)$ is the integer sum of the symbols of the p-ary expansion of s. The defining set T of $\mathcal{R}_p(\nu, m)$ is the set of those $s \in S$ satisfying $0 \le wt_p(s) < \mu$. Obviously, $s \preceq t$ implies $wt_p(s) \le wt_p(t)$.

Let $t \in S$ such that $wt_p(t) = \mu$. Any descendant s of t is in T, except t itself. So t is in the border of T. Conversely if a given t satisfies this last property, it cannot be such that $wt_p(t) > \mu$, because it cannot have a descendant whose p-weight is μ. So the border of T is exactly S_μ, completing the proof.

♦

Proposition 2.17 *Let $C(d)$ be the extended RS code of length p^m and designed distance d. It is a code over the field of order p^m and its defining set is the set of elements in the interval $[0, d-1]$ (see Definition 2.9).*

Let $(d_0,\ ...,\ d_{m-1})$ be the p-ary expansion of d and denote by k_0 the smallest k such that $d_k \neq 0$. Let us define $d^{(m-1)} = (d_{m-1}+1)p^{m-1}$ and for any k, $0 \leq k < m-1$,

$$d^{(k)} = (d_k+1)p^k \ + \sum_{i=k+1}^{m-1} d_i p^i \ .$$

Then the border of $C(d)$ is

$$I(d) = \{\ d\ \}\ \cup\ \{\ d^{(k)} \mid k_0 < k \leq m-1 \text{ and } d_k < p-1\ \}\ .$$

Note that the minimum distance of $C(d)$ is $d+1$, since the minimum distance of the RS code is exactly d.

Example 2.18 Denote by C the extension of the RS code with parameters $[127, 102, 26]$. The defining set of C is $[0, 25]$; the designed distance is $d = 26$. The minimum distance of C is 27 (see later Property 2.20). With the notation of Proposition 2.17, we have $k_0 = 1$ and the border of C is

$$I(d) = \{\ d,\ d^{(2)},\ d^{(5)},\ d^{(6)}\ \}\ .$$

where

$$\begin{array}{rcl} d & = & (0,\ 1,\ 0,\ 1,\ 1,\ 0,\ 0) = 26 \\ d^{(2)} & = & (0,\ 0,\ 1,\ 1,\ 1,\ 0,\ 0) = 28 \\ d^{(5)} & = & (0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0) = 32 \\ d^{(6)} & = & (0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1) = 64\ . \end{array}$$

We pointed out that the affine-invariant codes of length p^m can be classified, by considering the antichains of $(S, \preceq)$. There are special classes among these antichains as well as special classes of affine-invariant codes. In other words, and it is quite surprising, many properties of a given affine-invariant code can be deduced from its border. One aspect will be developed later in the description of "cyclic ideals" of $\mathcal{A}$. We now give some basic properties and two examples for illustration. The proofs, which are generally simple, can be found in [52], [21] or [54]. Recall that $n = p^m - 1$ and $S = [0, n]$.

Property 2.19 Let I be an antichain of $(S, \preceq)$. Denote by T the subset of S such that $\Delta(T) = T$ and whose border is I. Let u divide m (u may be 1 or m). *Then $p^u I = I$ if and only if $p^u T = T$ (modulo n).*

Actually this means that the class of antichains satisfying $p^u I = I$ corresponds to the class of affine-invariant codes over $\mathbf{k}$, where $\mathbf{k}$ is the finite field of order p^u.

Property 2.20 Let C be an affine-invariant code with defining set T and border I. Let C^* be the cyclic code whose extended code is C. The cardinality of the largest interval contained in T is called the *BCH bound* of C. Let δ be the smallest element of I. *Then $[0, \delta - 1] \subset T$ and δ is the BCH bound of C.* This property provides a lower bound for the minimum distance of C. Indeed the minimum distance of C^* is lower-bounded by δ, since $[1, \delta - 1]$ is contained in the defining set of C^*. Since C is affine-invariant, its minimum distance is lower-bounded by $\delta + 1$. Note that the BCH bound of C^* could be $\delta + 1$, but no more.

Property 2.21 Let C be an affine-invariant code with defining set T and border I. The dual code $C^\perp$ is also affine-invariant. Denote by $I^\perp$ its border and by $T^\perp$ its defining set. Let us define *the maximal set M* of T (or of C) as the set of maximal elements of T, with respect to $\preceq$.

Obviously *M is an antichain. As well as the border, the maximal set of T uniquely defines the affine-invariant code C. Moreover $M = n - I^\perp$ and, conversely, $I = n - M^\perp$.*

Property 2.22 This property is an application of Property 2.21; we keep the same notation. The code C is *self-orthogonal*, i.e. $C \subset C^\perp$, if and only if its border satisfies

$$\text{for all } s \text{ in } I \text{ and for all } t \text{ in } I \text{ then } t \notin \Delta(n - s) \ . \tag{16}$$

In other words *the class of antichains of $(S, \preceq)$ satisfying (16) corresponds to the class of affine-invariant self-orthogonal codes of length p^m.*

It is well-known that a ternary code is 3-divisible (i.e. any codeword has a weight divisible by 3) when it is self-orthogonal. Hence, *when $p = 3$, an antichain I which satisfies (16) and $3I = I$ (modulo n) defines one and only one 3-divisible ternary affine-invariant code.*

Example 2.23 Consider the extended BCH code of length 16 with designed distance 5, say C. First suppose that C is binary. The defining set is

$$T = \{\ 0,\ 1,\ 2,\ 4,\ 8,\ 3,\ 6,\ 9,\ 12\ \}.$$

By writing the 2-ary expansions of these elements we obtain

$$T = \left\{ \begin{array}{llll} (0\ 0\ 0\ 0) & & & \\ (1\ 0\ 0\ 0) & (0\ 1\ 0\ 0) & (0\ 0\ 1\ 0) & (0\ 0\ 0\ 1) \\ (1\ 1\ 0\ 0) & (0\ 1\ 1\ 0) & (1\ 0\ 0\ 1) & (0\ 0\ 1\ 1) \end{array} \right\}$$

It is easy to check that the border I is exactly the 2-cyclotomic coset of 5:

$$I = \{\ 5 = (1\ 0\ 1\ 0),\ 10 = (0\ 1\ 0\ 1)\ \}\ .$$

Suppose now that C is a code over $GF(4)$. The defining set is $T' = \{\ 0,\ 1,\ 4,\ 2,\ 8,\ 3,\ 12\ \}$ and the border is obviously $I' = \{\ 5,\ 6,\ 9,\ 10\ \}$. Note that $2I = I$ and $2I' \neq I'$, whereas $4I = I$ and $4I' = I'$ (modulo 15). For both codes, the smallest element of the border is 5, the designed distance. That illustrates Properties 2.19 and 2.20.

Example 2.24 Let $p = 3$ and $m = 3$; so $S = [0, 26]$. Consider the 3-cyclotomic coset modulo 26 containing 7. It is the antichain

$$I = \{\ 7,\ 21,\ 11\ \} = \{\ (1\ 2\ 0),\ (0\ 1\ 2),\ (2\ 0\ 1)\ \}\ .$$

Hence we have

$$n - I = \{\ 19,\ 5,\ 15\ \} = \{\ (1\ 0\ 2),\ (2\ 1\ 0),\ (0\ 2\ 1)\ \}\ .$$

It is easy to check that I satisfies (16): there is no $t \in I$ which is a descendant of some $u \in n - I$. Therefore the affine-invariant code C, whose border is I, is self-orthogonal. Its BCH bound is 7, implying that its minimum distance is at least 8. It is at least 9, since C is 3-divisible (see Property 2.22).

The defining set of C is the set of s such that $t \not\preceq s$, for all $t \in I$. That is:

$$T = \left\{ \begin{array}{lllll} (0\ 0\ 0) & (1\ 0\ 0) & (2\ 0\ 0) & (0\ 1\ 0) & (1\ 1\ 0) \\ (2\ 1\ 0) & (0\ 2\ 0) & (0\ 0\ 1) & (1\ 0\ 1) & (0\ 1\ 1) \\ (1\ 1\ 1) & (0\ 2\ 1) & (0\ 0\ 2) & (1\ 0\ 2) & \end{array} \right\}$$

One deduces that the maximal set of C is the antichain

$$M = \{\ 5,\ 15,\ 19,\ 13\ \} = \{\ (2\ 1\ 0),\ (0\ 2\ 1),\ (1\ 0\ 2),\ (1\ 1\ 1)\ \}\ .$$

The maximal set of the dual of C is $M^{\perp} = n - I$. It is clear that $M^{\perp} \subset T$, implying $T^{\perp} \subset T$. This again shows that C is self-orthogonal. The border of the dual of C is the antichain

$$I^{\perp} = n - M = \{\ (0\ 1\ 2),\ (2\ 0\ 1),\ (1\ 2\ 0),\ (1\ 1\ 1)\ \}\ .$$

2.4.2 Affine-invariant codes as ideals of $\mathcal{A}$

Recall that the ambient space is $\mathcal{A} = \mathbf{k}[\{\mathbf{F}, +\}]$ where $\mathbf{k}$ is any subfield of the field $\mathbf{F}$ of order p^m. Note that p-ary codes can be defined in this ambient space – or more generally p^e-ary codes, p^e dividing the order of $\mathbf{k}$. In other words a p-ary code is a code which has a generator matrix with coefficients in $GF(p)$.

Let x be any element of $\mathcal{A}$. The p^{th} power of x, where p is the characteristic of $\mathcal{A}$, is as follows:

$$\mathrm{x}^p = \left(\sum_{g \in \mathbf{F}} x_g X^g \right)^p = \sum_{g \in \mathbf{F}} x_g^p X^{pg} = \left(\sum_{g \in \mathbf{F}} x_g^p \right) X^0 = \left(\sum_{g \in \mathbf{F}} x_g \right)^p X^0\ .$$

Thus x is either invertible, when $\sum_{g \in \mathbf{F}} x_g \neq 0$, or nilpotent, when $\sum_{g \in \mathbf{F}} x_g = 0$. The *radical* of the algebra $\mathcal{A}$ is the set of nilpotent elements of $\mathcal{A}$. It is clearly an ideal of $\mathcal{A}$, the unique maximal ideal of $\mathcal{A}$. We will denote it by $\mathcal{P}$; the rth power of the ideal $\mathcal{P}$ will be denoted by $\mathcal{P}^r$. Recall that *powers of the radical of $\mathcal{A}$ are the p-ary Reed-Muller codes*:

$$\mathcal{P}^r = \mathcal{R}_p(m(p-1) - r, m)\ ,\quad 1 \leq r \leq m(p-1)\ . \tag{17}$$

The proof of this important property, as well as an extensive study on the ideals $\mathcal{P}^r$, can be found in the chapter(Assmus-Key) (Section 4). Our notation is slightly different; note $\mathcal{A}$ is used instead of $\mathbf{R}$ and $\mathcal{P}$ instead of $\mathbf{M}$.

Any element (or any subset) of $\mathcal{A}$ has a "position" in the decreasing sequence provided by ideals $\mathcal{P}^r$. This is a new parameter we will call *the depth:* x $\in \mathcal{A}$ *has depth r if and only if* x $\in \mathcal{P}^r \setminus \mathcal{P}^{r+1}$. Similarly the *depth of any ideal U of $\mathcal{A}$* is r if and only if U is contained in $\mathcal{P}^r$ and not in $\mathcal{P}^{r+1}$.

Our purpose here is to describe the affine-invariant codes by a set of generators. Any ideal of $\mathcal{A}$ is a sum of principal ideals. For any element x of $\mathcal{A}$, we will denote by (x) the principal ideal generated by x. The next definition and Theorem 2.26 were introduced by LAUBIE in [97].

Definition 2.25 *Let U be an ideal of $\mathcal{A}$ and let V be a subset $\{ \mathrm{u}_1, \ldots, \mathrm{u}_\ell \}$ of U. The set V is said to be a generator system of U if*

$$U = (\mathrm{u}_1) \ + \ \ldots \ + \ (\mathrm{u}_\ell) \ .$$

Moreover V is said to be minimal when the cardinality k of any generator system of U satisfies $\ell \leq k$. In this case we will say that ℓ is the size of the ideal U.

Theorem 2.26 *Let U be an ideal of $\mathcal{A}$. For any $\mathrm{x} \in U$, denote by $\overline{\mathrm{x}}$ the image of x in the quotient vector-space $U/\mathcal{P}U$. Then the following statements are equivalent:*

(i) $\{ \mathrm{u}_1, \ldots, \mathrm{u}_\ell \}$ *is a minimal generator system of U.*

(ii) $\{ \overline{\mathrm{u}}_1, \ldots, \overline{\mathrm{u}}_\ell \}$ *is a basis of $U/\mathcal{P}U$.*

Note that $\mathcal{P}U$ is the ideal generated by the products xy, $\mathrm{x} \in \mathcal{P}$ and $\mathrm{y} \in U$.

The main consequence of this theorem is that any generator system of any ideal U of $\mathcal{A}$ contains a minimal generator system. More precisely, one has a method for finding the size of any ideal.

Principal ideals are simply the ideals of size 1. In the general case it is not so easy to determine the size. However, for affine-invariant codes, *the size is deduced from the border.*

Theorem 2.27 *Let U be an affine-invariant code with defining set T and border I. Let θ be the cardinality of I. Then θ is the size of the ideal U.*

Sketch of proof: The complete proof is given in [52]. First consider the ideal $\mathcal{P}U$. As $\mathcal{P}$ and U are affine-invariant, $\mathcal{P}U$ is affine-invariant. It is sufficient to see that for $\mathrm{x} \in \mathcal{P}$ and $\mathrm{y} \in U$

$$\sigma_{u,0}(\mathrm{xy}) = \sigma_{u,0}(\mathrm{x})\sigma_{u,0}(\mathrm{y}) \ .$$

Let $\overline{T}$ be the defining set of $\mathcal{P}U$. Then we have the following property:

$$\overline{T} = T \cup I \ .$$

Then the dimension of U is equal to the dimension of $\mathcal{P}U$ plus θ. It remains to find θ elements in U, linearly independant and providing a basis of $U/\mathcal{P}U$.

We will indicate how this basis can be constructed. Let U^* be the cyclic code whose extension is U. We consider the usual generator matrix of U^*, whose rows are the generator polynomial and their shifts (see Chapter 1, Theorem 5.2.). By extending each row of this matrix, we obtain a basis of U. Let x be the first extended row — i.e. the extension of the generator polynomial of the cyclic code U^*. The extension of the ith row is the image of x by the affine-permutation $\sigma_{\alpha^i,0}$. Then the set

$$\{\ \mathrm{x},\ \sigma_{\alpha,0}(\mathrm{x}),\ \sigma_{\alpha^2,0}(\mathrm{x}),\ \ldots,\ \sigma_{\alpha^{\theta-1},0}(\mathrm{x})\ \}$$

is a minimal generator system of U.

♦

An immediate consequence of this theorem is the characterization of affine-invariant codes which are principal ideals of $\mathcal{A}$ — i.e. affine-invariant codes of size 1.

Corollary 2.28 *Let q be the order of the alphabet field* **k***.*

An affine-invariant code is a principal ideal if and only if its border has only one element. More precisely, the border contains only one element δ, satisfying $q\delta \equiv \delta$ modulo n.

Example 2.29 As an example, *the class of extended RS codes which are principal ideals* is easily deduced from Proposition 2.17. Indeed such a code $C(d)$ must have as border the set $\{d\}$, where d is its designed distance. So, in Proposition 2.17, d must be such that the set

$$\{\ d^{(k)}\ |\ k_0 < k \leq m-1 \text{ and } d_k < p-1\ \}$$

is empty. It is equivalent to say that d has the following form

$$d = d_{k_0}p^{k_0} + \sum_{k=k_0+1}^{m-1}(p-1)p^k\ ,\quad d_{k_0} \in [1, p-1]\ ,\quad k_0 \in [0, m-2]\ . \qquad (18)$$

By convention, $d = d_{k_0}p^{k_0}$ when $k_0 = m-1$. *There are $m(p-1)$ principal extended RS codes, one and only one for each depth.*

For instance, consider the RS code with parameters $[2^m-1, 2^{m-1}, 2^{m-1}]$ over $GF(2^m)$. Then the extended code, $C(d)$ with $d = 2^{m-1}$, is such that d satisfies (18). So $C(d)$ is a principal ideal. The code $C(d)$ has parameters $[2^m, 2^{m-1}, 2^{m-1}+1]$. Its defining set is $[0, 2^{m-1}-1]$ and its maximal set is

d	border	d	border
1^*	$cl(1)$	23^*	$cl(23) \cup cl(27) \cup cl(29) \cup cl(43)$
3^*	$cl(3) \cup cl(5) \cup cl(9)$	27^*	$cl(27) \cup cl(29) \cup cl(43)$
5^*	$cl(5) \cup cl(9)$	29^*	$cl(29) \cup cl(43)$
7	$cl(7) \cup cl(9)$	31	$cl(31) \cup cl(43)$
11^*	$cl(11) \cup cl(13) \cup cl(19) \cup cl(21)$	43^*	$cl(43)$
13^*	$cl(13) \cup cl(19) \cup (21)$	47^*	$cl(47) \cup cl(55)$
15	$cl(15) \cup cl(19) \cup cl(21)$	55^*	$cl(55)$
19^*	$cl(19) \cup cl(21)$	63^*	$cl(63)$
21	$cl(21) \cup cl(27)$		

Table 1: Borders of the extended binary BCH codes of length 128; d is the designed distance of the BCH code; $cl(i)$ denotes the 2-cyclotomic coset containing i; the asterisk indicates that the border is an antichain of constant rank.

simply $\{2^{m-1} - 1\}$. From Property 2.21, the border of the dual code also contains only one element, which is

$$(2^m - 1) - (2^{m-1} - 1) = 2^{m-1} .$$

The code $C(d)$ and its dual have the same border, implying that $C(d)$ is self-dual. The binary image of such self-dual codes, with short lengths, appear in [120] and [121] for a new construction of the binary Golay code and of an extremal self-dual code of length 64.

On the other hand the results of Griggs on maximal antichains can be applied here to the determination of affine-invariant codes of maximal size. These codes are among the p-ary RM codes.

Theorem 2.30 *Let U be an affine-invariant code and denote by $t(U)$ the size of U. Let S_j, $1 \leq j \leq m(p-1)$, be the maximal antichain of constant rank which is the border of $\mathcal{P}^j$. Denote by $|S_j|$ the cardinality of S_j. Let λ be the median p-weight in $S = [0, p^m - 1]$:*

$$\lambda = \left\lfloor \frac{m(p-1)}{2} \right\rfloor$$

Then $t(U) \leq |S_\lambda|$. Moreover if $t(U) = |S_\lambda|$ then U is a p-ary RM code. That is:

- *if $m(p-1)$ is even then $U = \mathcal{P}^{\lambda}$;*
- *if $m(p-1)$ is odd then U is either $\mathcal{P}^{\lambda}$ or $\mathcal{P}^{\lambda+1}$.*

Note that $\lfloor a \rfloor$ denotes the integer part of some real number a.

Proof: It was proved by Griggs in [73] that the maximal size for an antichain of $(S, \preceq)$ is exactly the size of S_λ. Moreover if $m(p-1)$ is even, S_λ is the unique antichain of this size. If $m(p-1)$ is odd then we have $p=2$, m odd, and $\lambda = (m-1)/2$; the size of S_λ is exactly the size of $S_{\lambda+1}$ since these sizes are respectively

$$\binom{m}{(m-1)/2} \quad \text{and} \quad \binom{m}{(m+1)/2} \ .$$

The antichains S_λ and $S_{\lambda+1}$ uniquely define the affine-invariant codes $\mathcal{P}^{\lambda}$ and $\mathcal{P}^{\lambda+1}$. Note that $\mathcal{P}^{\lambda+1}$ is the self-dual doubly-even RM code.
♦

Let U be an affine-invariant code with border I. We have proved that the size of U is the cardinality of I. On the other hand, the depth of U is easily obtained. It is

$$\min \ \{ \ wt_p(s) \mid s \in I \ \} \ ,$$

because if there is an $s \in I$ which has p-weight μ then U cannot be contained in $\mathcal{P}^{\mu+1}$ – i.e. the defining set of U does not contain the defining set of $\mathcal{P}^{\mu+1}$ (see Proposition 2.16).

If all elements in I have the same p-weight, then I is an antichain of constant rank. This is the case for principal ideals and for p-ary Reed-Muller codes. The extended RS codes defined from an antichain of constant rank can be easily obtained from Proposition 2.17 (see another proof in [50]). Moreover several extended BCH codes have this property. As an example we give in Table 1 the borders of the extended BCH codes of length 128. The class of extended BCH codes which are principal is described in [53]. It is proved that the true minimum distance of these BCH codes is exactly the designed distance. It is important to notice that, by studying a special class of ideals, some results on parameters of some BCH codes are then obtained. When the alphabet field is a prime field, all principal affine-invariant codes are extended BCH codes. To conclude we give an example over the field of order 5.

Example 2.31 Consider BCH codes of length $5^3 - 1$ over $GF(5)$. Denote by $B^*(d)$ such a code with designed distance d. Let $B(d)$ be the extended code. The codes $B(d)$, which are principal ideals, are defined from antichains $\{d\}$ such that $5d = d$ modulo 124. Then the 5-ary expansion of d must have the following form: $d = \delta(1 + 5 + 5^2)$, $\delta \in [1, 4]$.

Let C be any affine-invariant code with border $\{d\}$, where d has the form above. Let T be the defining set of C. Then $t \in T$ if and only if t is not an ascendant of d, with respect to $\preceq$. That is

$$T = \{\ t \mid t \neq d \text{ and } d \not\preceq\ t\ \}\ .$$

Since the 5-ary expansion of d is $(\delta,\ \delta,\ \delta)$, the condition $t \in T$ means that there is a representative of the 5-cyclotomic coset of t which is smaller than d. Thus T is the defining set of the extension of the BCH code $B(d)$ — i.e. $C = B(d)$.

Then the four affine-invariant codes, which are principal, are extended BCH codes $B(d)$ with $d \in \{31, 62, 93, 124\}$ (if $d = 124$ the code is trivial). The dimensions of these codes are respectively $(5 - \delta)^3$, $\delta \in [1, 4]$. The minimum distance of $B^*(d)$ is d and the minimum distance of $B(d)$ is $d + 1$ (see [53, Theorem 2]).

Comments on Section 2.4 At the end of this section, we indicated more properties of affine-invariant codes which are properties of antichains. There are others examples: it was proved in [21] that the automorphism group of an affine-invariant code can be determined from the knowledge of its border and of its maximal set only. Another example is given in [54], where the antichains defining self-dual affine-invariant codes are studied (only for codes over $GF(2^r)$). The affine-invariant codes whose border is an antichain of constant rank appear as a special class. However, except when the size is 1, no new result (on weights, dimension, ...) are derived.

Affine-invariant codes are of most interest when the combinatorial properties of the defining sets of cyclic codes are considered. There is a natural question: is it possible, maybe with another partial order, to define other special classes? We have in mind the work providing bounds on the minimum distance (see Chapter 1, Section 6). On the other hand, is the development similar when repeated-root cyclic codes, constructed from affine-invariant codes, are considered?

To conclude we want to mention the role of the multiplication of the algebra $\mathcal{A}$ in the study of primitive codes. For instance, Theorem 2.26 can be applied because it is possible to determine the defining set of the code $\mathcal{P}U$. More generally, one can characterize any code UV where U and V are affine-invariant codes. This is because the value $\phi_s(\mathrm{xy})$, for some s, can be calculated from $\phi_s(\mathrm{x})$ and $\phi_s(\mathrm{y})$ (see in Chapter(Assmus-Key), Section 4.3.).

3 On parameters of cyclic codes.

This section deals with famous open problems. For instance it is well-known that the *minimum distance* of a given cyclic code is generally not known. A fortiori *weight enumerators* of cyclic codes are generally not known. The study of *weight enumerators*, *complete* or not, is crucial in coding theory. A lot of open problems arise from the difficulty of obtaining results on the number or on the form of a set of codewords of a given weight.

The main part of this section is devoted to the question of the form of codewords. We develop connections with two algebraic problems: the solvability of some systems of algebraic equations and the existence of certain kinds of polynomials on finite fields (Section 3.1 and 3.2). Above all, we want to emphasize the significant role of tools derived from symbolic calculus, as has appeared in recent works. We want also to point out that several classical problems of the theory of finite fields are involved.

In Sections 3.3 and 3.4, our main purpose is to illustrate the hardness of any question on weight enumerators by discussing simple specific problems. We have chosen, at first, two well-known hard open problems: the minimum distance of binary narrow-sense BCH codes and the weight enumerators of binary RM codes.

We later treat the weight enumerators of cyclic codes with few zeros, especially of binary cyclic codes with two zeros which appear to be the simplest cyclic codes involved in several applications (see an example in Section 4.1). The determination of the weight enumerator of such a code remains an open problem except when the code is *optimal* in a certain sense. Our aim is to recall and explain the main tools which were used by Kasami for proving the unicity of the weight enumerator of these optimal codes. The work of Kasami, based on the MacWilliams transform and the Pless identities, is still fundamental for any approach with a view toward classifying cyclic codes with few zeros.

Section 3.4.3 is a short paragraph devoted to irreducible cyclic codes –

i.e. the duals of the cyclic codes with one zero. Note that to say “j zeros” for any q-ary cyclic code means that the defining set of this code is the union of exactly j q-cyclotomic cosets.

Section 3 is completed by short comments on the automorphism group of cyclic codes and on the question of their asymptotic behaviour.

3.1 Codewords and Newton identities

In this section we introduce the *Newton identities*, restricting ourself to the context of cyclic codes – however the reader can easily see that they can be defined in a more general context. By using Newton identities, one can put in a concrete form the definition of words of a given code, whose weights are less than or equal to a fixed value. Our purpose is to explain (and we will do that as one goes along) why this form is “concrete” and how it can be exploited. We wish to show that Newton identities are a tool of great interest for describing a set of codewords, particularly for codewords of cyclic codes. This section is based on the recent work of Augot [5][6].

Taking any codeword c, say $(c_1, \ldots, c_n)$, its *support* is the set

$$supp(\mathrm{c}) = \{\ i \mid c_i \neq 0\ \}.$$

We consider here codewords of length n whose supports are contained in a finite field $\mathbf{F}$, with respect to the ambient space $\mathcal{M} = \mathbf{k}[\{G^*, \times\}]$ (see §2.2); recall that G^* is the subgroup of order n of the multiplicative group of the splitting field $\mathbf{F}$ of $X^n - 1$.

We can then study, as well as codewords, subsets of $\mathbf{F}$ and polynomials in the ring $\mathbf{F}[X]$. Recall that such a polynomial is said to *split in* $\mathbf{F}$ when it can be written as a product of linear factors in $\mathbf{F}[X]$.

Definition 3.1 *Let* $\mathrm{x} = \sum_{g \in G^*} x_g(g)$ *be a codeword in* $\mathcal{M}$ *of weight* w*. The support of* x *is said to be its set of locators. That is*

$$supp(\mathrm{x}) = \{\ g_1, \ldots,\ g_w\ \} = \{\ g \in G^* \mid x_g \neq 0\ \}\ .$$

The locator polynomial of x *is the polynomial over* $\mathbf{F}$ *defined as follows :*

$$\sigma_{\mathrm{x}}(X) = \prod_{i=1}^{w} (1 - g_i X).$$

The coefficients of $\sigma_{\mathrm{x}}(X)$ are the elementary symmetric functions of the locators g_i, $1 \le i \le w$. These are for any j, $1 \le j \le w$,

$$\sigma_j = (-1)^j \sum_{1 \le i_1 < i_2 < \ldots < i_j \le w} g_{i_1} g_{i_2} \ldots g_{i_j} \ .$$

The power sum functions of the locators of x *are:*

$$A_i = \sum_{k=1}^{w} g_k^i \quad , \quad i \ge 0 \ .$$

Note that the locators of a codeword are, by definition, distinct elements.

The definition of the locator polynomial is in conformity with the definition of the extended codeword (see (7)). Indeed the support of extended codewords is contained in $G = G^* \cup \{0\}$. If such a support contains "0", the polynomial $\sigma_{\mathrm{x}}(X)$ is multiplied by 1 and the power sum functions are also unchanged. Actually we assume that a codeword and its extension have the same locator polynomial.

The following properties can be easily proved. Our notation is that of Definition 3.1; q is the order of the alphabet field and α is an nth root of unity.

Proposition 3.2 *Let* $\mathrm{x}^{(k)}$ *be the* k*th-shift of* x. *Denote by* $\sigma_j^{(k)}$ *the coefficients of the locator polynomial of* $\mathrm{x}^{(k)}$ *and by* $A_i^{(k)}$ *its power sum functions. Then*

(i) $A_{qi} = A_i^q$, $A_{i \ mod \ n} = A_i$ *and* $A_i^{(k)} = \alpha^{ik} A_i$.

(ii) *The support of* $\mathrm{x}^{(k)}$ *is* $\{ \alpha^k g_1, \ldots, \alpha^k g_w \}$ *and*

$$\sigma_{\mathrm{x}^{(k)}}(X) = \sigma_{\mathrm{x}}(\alpha^k X) \quad , \ i.e. \ \sigma_j^{(k)} = \alpha^{kj} \sigma_j \ .$$

There are two natural questions. What is the form of the locator polynomial of this or that codeword of a given cyclic code ? Is a given polynomial a possible locator polynomial ? The use of the *Newton identities* is the most natural tool for attacking these questions. We can write simply an algebraic system of equations over the splitting field $\mathbf{F}$ whose solutions could correspond to the codewords.

Note that a codeword whose symbols are from $\{0, 1\}$ can be identified with its support and then with its locator polynomial. Moreover for such a codeword the coefficients of the MS polynomials are exactly the power sums of the locators. The Newton identities are usually viewed in this context while those introduced by Theorem 3.5 are said to be the *generalized Newton identities*. We begin by giving the usual form which is very useful in practice, mainly in the binary case, as will appear in the next example.

Theorem 3.3 *Let* $\mathrm{x} \in \mathcal{M}$ *be a codeword of weight* w*, with locators* $g_1, \dots, g_w$*. Then the coefficients of the locator polynomial and the power sum functions of* x *are linked by the Newton identities, i.e. with notation of Definition 3.1, the following identities hold:*

$$\begin{array}{l} A_1 + \sigma_1 = 0 \\ A_2 + \sigma_1 A_1 + 2\sigma_2 = 0 \\ \dots\dots\dots\dots \\ A_w + \sigma_1 A_{w-1} + \dots + \sigma_{w-1} A_1 + w\sigma_w = 0 \end{array} \tag{19}$$

and for $j > w$*,*

$$A_j + \sigma_1 A_{j-1} + \dots + \sigma_w A_{j-w} = 0 \ . \tag{20}$$

Proof: The logarithmic derivative of $\sigma_{\mathrm{x}}(X)$, with respect to X, is

$$\frac{\sigma'_{\mathrm{x}}(X)}{\sigma_{\mathrm{x}}(X)} = \sum_{i=1}^{w} \frac{-g_i}{1 - g_i X}$$

But the formal series of $(1 - g_i X)^{-1}$ is $\sum_{\ell=0}^{\infty} g_i^{\ell} X^{\ell}$. So we have

$$\frac{\sigma'_{\mathrm{x}}(X)}{\sigma_{\mathrm{x}}(X)} = \sum_{i=1}^{w} -g_i \sum_{\ell=0}^{\infty} g_i^{\ell} X^{\ell} = \sum_{\ell=0}^{\infty} \left(\sum_{i=1}^{w} -g_i^{\ell+1} \right) X^{\ell} = \sum_{\ell=0}^{\infty} -A_{\ell+1} X^{\ell} \ .$$

This yields

$$\sigma'_{\mathrm{x}}(X) = \left(\sum_{\ell=0}^{\infty} -A_{\ell+1} X^{\ell} \right) \left(\sum_{i=0}^{w} \sigma_i X^i \right)$$

giving

$$\sum_{j=1}^{w} j \ \sigma_j X^{j-1} = \sum_{j=0}^{\infty} \left(\sum_{\ell+i=j} -A_{\ell+1} \sigma_i \right) X^j \ .$$

By equating coefficients we obtain

$$\begin{aligned} j\,\sigma_j &= -\sum_{i=0}^{j-1} A_{j-i}\,\sigma_i \quad , \quad \text{for } j \le w \ , \\ 0 &= \sum_{i=0}^{w} A_{j-i}\,\sigma_i \quad , \quad \text{for } j > w \ . \end{aligned}$$

♦

Example 3.4 Let C be the binary cyclic code of length $n = 2^m - 1$ with defining set T, $T = cl(3) \cup cl(5)$, where $cl(i)$ is the 2-cyclotomic coset of i modulo n. By using Newton identities, we will prove the following property:

> *The code C has minimum distance 3 if and only if 3 divides m. In this case its set of minimum weight codewords consists of the word whose locator polynomial is $1 + X + X^3$ and of its shifts. When 3 does not divide m, the code C has minimum distance at least four.*

Out notation is that of Theorem 3.3. Clearly the minimum distance of C is at least two. Suppose that there is a codeword x of weight two or three in C. We begin by using the first three Newton identities

$$\begin{aligned} &A_1 + \sigma_1 \ = \ 0 \\ &A_3 + A_2\sigma_1 + A_1\sigma_2 + \sigma_3 \ = \ 0 \\ &A_5 + A_4\sigma_1 + A_3\sigma_2 + A_2\sigma_3 \ = \ 0 \ . \end{aligned} \tag{21}$$

By shifting we can take $A_1 = 1$ and by definition of C, we have $A_3 = A_5 = 0$. First suppose that there is a codeword of weight two, i.e. $\sigma_3 = 0$. So by substitution in (21) we obtain

$$\sigma_1 = A_1 = 1 \ \ , \ \ 1 + \sigma_2 = 0 \ \text{ and } \ 1 = 0$$

(note that $A_{2k} = A_k^2$). The third identity produces a contradiction, implying that codewords of weight 2 do not exist. Suppose now that there is a codeword of weight three. In the same way, we obtain

$$\sigma_1 = A_1 = 1 \ \ , \ \ 1 + \sigma_2 + \sigma_3 = 0 \ \text{ and } \ 1 + \sigma_3 = 0 \ ,$$

implying $\sigma_3 = 1$ and $\sigma_2 = 0$. Then the locator polynomial is here unique, up to a shift; we obtain $\sigma_{\rm x}(X) = 1 + X + X^3$. But this polynomial splits in the field of order 2^m if and only if 3 divides m. So if 3 does not divide m, the minimum distance is at least four.

Suppose now that 3 divides m and compute the A_i which are not already known. By replacing the σ_i by their values, we have the following identities

$$A_j = A_{j-1} + A_{j-3} \quad , \quad j \geq 5 \ . \tag{22}$$

We must prove that they are satisfied. Set $I = \{3, 5, 6\}$, the cyclotomic coset of 3 modulo 7. It is easy to check, by induction on j, that the solution

$$A_j \ = \ \begin{cases} 0 & \text{if } \ j \bmod 7 \in I \\ 1 & \text{otherwise} \end{cases} \tag{23}$$

works when 3 divides m. Note that $A_0 = 1$, since A_0 is the sum modulo 2 of the three non zero symbols of the word. So we have

$$A_0 = A_1 = A_2 = A_4 = 1 \quad \text{and} \quad A_3 = A_5 = A_6 = 0 \ ,$$

showing that (23) is satisfied for $j < 7$. Now we have just to see that $A_j = A_{j \ mod \ 7}$; according to (22) one only have to check the seven equations

$$A_{j=7k+s} = A_{(j-1) \ mod \ 7} + A_{(j-3) \ mod \ 7} = A_s \ , \quad 0 \leq s \leq 6 \ .$$

Finally the codewords of weight three of C correspond to the locator polynomials

$$1 \ + \ \alpha^k X \ + \ (\alpha^k X)^3 \quad , \quad k \in [0, 2^m - 2] \ ,$$

where α is a primitive root of the field of order 2^m.

We are going to state the general form of Newton identities. This form is clearly more interesting if we want to treat non binary codewords. Indeed it will turn out that the MS polynomial is as important as the locator polynomial for the description of the solutions of the algebraic system defined from the Newton identities.

Theorem 3.5 *Let* x $\in \mathcal{M}$ *be a codeword of weight* w. *Let* $\Lambda_1, \ldots, \ \Lambda_n$ *be the coefficients of the MS polynomial of* x *and denote by* $\sigma_0, \ldots, \ \sigma_w$ *the coefficients of the locator polynomial of* x *(note that* $\sigma_0 = 1$*). Then the* σ_i *and the* Λ_i *are linked by the generalized Newton identities – i.e. the following identities hold:*

$$\forall \ j \geq 0 \ , \quad \Lambda_{j+w} + \sigma_1 \Lambda_{j+w-1} + \ldots + \sigma_w \Lambda_j = 0 \ . \tag{24}$$

Proof: First observe that by definition (see (1) and (3)) we have for $0 \leq \ell < n$

$$\Lambda_\ell = \sum_{g \in G^*} x_g g^\ell = \sum_{i=1}^{w} x_{g_i} g_i^\ell$$

where $g_1, \ldots, g_w$ are the locators of x. Moreover if $\ell \geq n$ then $\Lambda_\ell = \Lambda_{\ell \ mod \ n}$.

Now from Definition 3.1, $\sigma_{\mathrm{x}}(1/g_i) = 0$ for $i = 1, \ldots, w$. Thus, for any i and any $j \geq 0$, we obtain

$$x_{g_i} g_i^{j+w} \sigma_{\mathrm{x}}(1/g_i) = \sum_{k=0}^{w} x_{g_i} g_i^{j+w-k} \sigma_k = 0 \ ,$$

implying

$$\sum_{i=1}^{w} \sum_{k=0}^{w} x_{g_i} g_i^{j+w-k} \sigma_k = \sum_{k=0}^{w} \Lambda_{j+w-k} \sigma_k = 0 \ .$$

♦

Consider the ring $\mathbf{F}[Y]$, $Y = \{Y_1, \ldots, Y_\ell\}$, of polynomials with coefficients in $\mathbf{F}$ and with ℓ indeterminates. Taking $f_i \in \mathbf{F}[Y]$, $1 \leq i \leq s$, we can define the algebraic system

$$\mathcal{S} = \{ \ f_1(Y) = 0, \ \ \ldots, \ \ f_s(Y) = 0 \ \} \ .$$

The set of solutions of $\mathcal{S}$ is

$$V(\{f_1, \ldots, f_s\}) = \{ \ Y \in \mathbf{F}^\ell \mid f_i(Y) = 0, \ \ 1 \leq i \leq s \ \} \ .$$

If I denotes the ideal generated by $\{f_1, \ldots, f_s\}$, we have obviously $V(I) = V(\{f_1, \ldots, f_s\})$.We are saying that *any system $\mathcal{S}$ defines an ideal I in* $\mathbf{F}[Y]$ *and any solution Y of $\mathcal{S}$ satisfies $f(Y) = 0$ for all $f \in I$.*

We will now consider the ring $\mathbf{F}[\Lambda_0, \ldots, \Lambda_{n-1}, \sigma_1, \ldots, \sigma_w]$ and the algebraic system provided from a given cyclic code C by the Newton identities.

Definition 3.6 *Let the field* $\mathbf{F}$ *be the splitting field of $(X^n - 1)$. Let $q = p^r$, where p is the characteristic of the ambient space $\mathcal{M}$. Let C be a cyclic code in $\mathcal{M}$ with defining set T. We define the system $\mathcal{S}_C(w)$, where the Λ_i and* *the σ_i are the indeterminates, as follows:*

$$\mathcal{S}_C(w) = \begin{cases} \Lambda_{w+1} + \Lambda_w\sigma_1 + \cdots + \Lambda_1\sigma_w = 0, \\ \Lambda_{w+2} + \Lambda_{w+1}\sigma_1 + \cdots + \Lambda_2\sigma_w = 0, \\ \vdots \\ \Lambda_{n+w} + \Lambda_{n+w-1}\sigma_1 + \cdots + \Lambda_n\sigma_w = 0, \\ \forall i \in [0, n-1], \quad \Lambda_{qi \bmod n} = \Lambda_i^q, \\ \forall i \in [0, n-1], \quad \Lambda_{i+n} = \Lambda_i, \\ \forall i \in T, \quad \Lambda_i = 0. \end{cases} \tag{25}$$

The system $\mathcal{S}_C(w)$ defines an ideal in the ring $\mathbf{F}[\Lambda_0, \ldots, \Lambda_{n-1}, \sigma_1, \ldots, \sigma_w]$.

Theorem 3.7 *Let C be a cyclic code in $\mathcal{M}$ with defining set T. Then we have the following properties.*

(i) *If the code C contains a codeword* x *of weight less than or equal to w, then the system $\mathcal{S}_C(w)$ has at least one solution $(\Lambda_0, \ldots, \Lambda_{n-1}, \sigma_1, \ldots, \sigma_w)$, where the Λ_i are the coefficients of the MS polynomial of* x *and the σ_i are the coefficients of the locator polynomial of* x.

(ii) *If the system $\mathcal{S}_C(w)$ has solutions then the corresponding n-tuples $(\Lambda_0, \ldots, \Lambda_{n-1})$ are the coefficients of the MS polynomials of the codewords of C of weight less than or equal to w.*

(iii) *Let $(\Lambda_0, \ldots, \Lambda_{n-1}) \in \mathbf{F}^n$ and denote by S the set of w-tuples $(\sigma_1, \ldots, \sigma_w)$ such that $(\Lambda_0, \ldots, \Lambda_{n-1}, \sigma_1, \ldots, \sigma_w)$ is a solution of $\mathcal{S}_C(w)$. Assume that S is not empty and then denote by* x *the codeword of C whose MS polynomial has as coefficients the Λ_i.*

Then $(\sigma_1, \ldots, \sigma_w)$ is in S if and only if the locator polynomial of x *divides the polynomial $1 + \sum_{i=1}^{w} \sigma_i X^i$. Moreover S is an affine space of dimension $w - w_0$, where w_0 is the weight of* x.

Proof: **(i)** Suppose that C contains a codeword of weight $w_0 \leq w$. Let x be this codeword, $\Lambda_0, \ldots, \Lambda_{n-1}$ the coefficients of its MS polynomial and $\sigma_1, \ldots, \sigma_{w_0}$ the coefficients of its locator polynomial. From Theorem 3.5 and from the definition of the MS polynomial, it is clear that $\mathcal{S}_C(w)$ is satisfied for these Λ_i and these σ_i. Note that this solution is such that $\sigma_i = 0$ for $w_0 < i \leq w$, when $w_0 < w$. We can say that *the existence of solutions of*

$\mathcal{S}_C(w)$ is a necessary condition for the existence of codewords of weight less than or equal to w in C.

(ii) Suppose that the algebraic system $\mathcal{S}_C(w)$ has a solution $(\Lambda_0, \ldots, \Lambda_{n-1}, \sigma_1, \ldots, \sigma_w)$ and consider only the Λ_i. The equations

$$\Lambda_{qi \bmod n} = \Lambda_i^q \quad , \quad i \in [0, n-1]$$

imply that $\Lambda_0, \ldots, \Lambda_{n-1}$ are the coefficients of the MS polynomial of a codeword x of $\mathcal{M}$ (the MS polynomial has values in $\mathbf{k}$). Furthermore x belongs to C because $\Lambda_i = 0$ for all $i \in T$ (see Theorem 2.3). It remains to prove that $w_0 \leq w$, where w_0 is the weight of x.

We now write that (25) is satisfied for the solution $(\Lambda_0, \ldots, \Lambda_{n-1}, \sigma_1, \ldots, \sigma_w)$:

$$\begin{pmatrix} \Lambda_n & \Lambda_{n-1} & \cdots & \Lambda_{w+1} & \cdots & \Lambda_1 \\ \Lambda_{n+1} & \Lambda_n & \cdots & \Lambda_{w+2} & \cdots & \Lambda_2 \\ \vdots & \vdots & & \vdots & & \vdots \\ \Lambda_{2n-1} & \Lambda_{2n-2} & \cdots & \Lambda_{w+n} & \cdots & \Lambda_n \end{pmatrix} \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ \sigma_1 \\ \vdots \\ \sigma_w \end{pmatrix} = 0.$$

Since $\Lambda_{i+n} = \Lambda_i$, the matrix above is exactly the matrix $\mathcal{C}(\mathrm{x})$ of Theorem 2.5. From this theorem we know that the rank of this matrix is w_0. Since $\mathcal{C}(\mathrm{x})$ is a circulant matrix, we have

$$\begin{pmatrix} \Lambda_n & \Lambda_{n-1} & \cdots & \Lambda_{w+1} & \cdots & \Lambda_1 \\ \Lambda_1 & \Lambda_n & \cdots & \Lambda_{w+2} & \cdots & \Lambda_2 \\ \vdots & \vdots & & \vdots & & \vdots \\ \Lambda_{n-1} & \Lambda_{n-2} & \cdots & \Lambda_w & \cdots & \Lambda_n \end{pmatrix} \begin{pmatrix} 0 & 0 & \cdots & 1 \\ \vdots & \vdots & & \sigma_1 \\ 0 & 1 & & \vdots \\ 1 & \sigma_1 & & \sigma_w \\ \sigma_1 & \sigma_2 & & 0 \\ \vdots & \vdots & & \vdots \\ \sigma_w & 0 & \cdots & 0 \end{pmatrix} = 0.$$

It appears that each column of $\mathcal{C}(\mathrm{x})$ is in the vector-space generated by the last w columns of $\mathcal{C}(\mathrm{x})$. Hence the rank of $\mathcal{C}(\mathrm{x})$, which is w_0, is less than or equal to w. Moreover it is clear that, fixing $\Lambda_0, \ldots, \Lambda_{n-1}$, the set of solutions of $\mathcal{S}_C(w)$ is an affine space of dimension $w - w_0$.

(iii) Let $(\Lambda_0, \ldots, \Lambda_{n-1}) \in \mathbf{F}^n$ and set

$$S = \left\{ (\sigma_1, \ldots, \sigma_w) \;\middle|\; \begin{array}{l} (\Lambda_0, \ldots, \Lambda_{n-1}, \sigma_1, \ldots, \sigma_w) \\ \text{is a solution of } \mathcal{S}_C(w) \end{array} \right\}$$

Assuming that S is not empty, we have at least one $\mathrm{x} \in C$ whose MS polynomial has the Λ_i as coefficients. We have shown in proving **(ii)**, that the weight w_0 of x satisfies $w_0 \leq w$ and that S has dimension $w - w_0$. Now set

$$S' = \{ \ (\sigma_1, \ldots, \sigma_w) \mid 1 + \sum_{i=1}^{w} \sigma_i X^i \equiv 0 \pmod{\sigma_{\mathrm{x}}(X)} \ \} \ ,$$

where $\sigma_{\mathrm{x}}(X)$ is the locator polynomial of x. Since the degree of σ_{x} is w_0, S' is an affine space of dimension $w - w_0$ too; so it is sufficient to prove that $S' \subset S$. Take $(\sigma_1, \ldots, \sigma_w) \in S'$ and denote by $\sigma(X)$ the polynomial $1 + \sum_{i=1}^{w} \sigma_i X^i$. Since $\sigma_{\mathrm{x}}(X)$ divides $\sigma(X)$, any root of σ_{x} is a root of σ, providing

$$\sigma(1/g_i) \ = \ 0 \ \ , \ \ i \in [1, w_0]$$

where $g_1, \ldots, g_{w_0}$ are the locators of x. We remark that only this property is needed in the proof of Theorem 3.5, for proving that the σ_i and the Λ_i satisfy (24). By using the same method, we obtain for any $j \geq 0$:

$$x_{g_i} g_i^{j+w} \sigma(1/g_i) = \sum_{k=0}^{w} x_{g_i} g_i^{j+w-k} \sigma_k = 0 \ ,$$

implying

$$\sum_{i=1}^{w_0} \sum_{k=0}^{w} x_{g_i} g_i^{j+w-k} \sigma_k = \sum_{k=0}^{w} \left(\sum_{i=1}^{w_0} x_{g_i} g_i^{j+w-k} \right) \sigma_k = \sum_{k=0}^{w} \Lambda_{j+w-k} \sigma_k = 0 \ .$$

So $\mathcal{S}_C(w)$ is satisfied for these σ_i and for the Λ_i corresponding to the codeword x of C; hence $(\sigma_1, \ldots, \sigma_w) \in S$. We have proved that $S = S'$, completing the proof of **(iii)**. Note that the coefficients of the polynomial $\sigma_{\mathrm{x}}(X)$ itself provide an element of S.

♦

It is important to notice that the existence of solutions of $\mathcal{S}_C(w)$ insures the existence of codewords of weight $w_0 \leq w$ in C (see (ii)). Moreover such a codeword x, which is uniquely defined by its MS polynomial, is such that its locator polynomial generates an affine-subspace S, of dimension $w - w_0$, included in the ideal of solutions of $\mathcal{S}_C(w)$: *each solution of* $\mathcal{S}_C(w)$ *provides an* $\mathrm{x} \in C$ *and a subspace* S*;* S *"contains" one and only one* $\mathrm{x} \in C$ *and several other solutions of* $\mathcal{S}_C(w)$. Whenever $w_0 = w$, the subspace S contains one and only one solution of $\mathcal{S}_C(w)$ corresponding to a unique codeword of C of weight w. This is always satisfied when the minimum distance of C is lower-bounded by w. Thus we have an important corollary of Theorem 3.7 concerning the minimum distance of C.

Corollary 3.8 *Let* C *be a cyclic code in* $\mathcal{M}$ *whose minimum distance* δ *satisfies* $\delta \geq w$*. Then the minimum distance of* C *is exactly* w *if and only if the system* $\mathcal{S}_C(w)$ *has at least one solution* $(\Lambda_0, \ldots, \Lambda_{n-1}, \sigma_1, \ldots, \sigma_w)$*. For any such solution the codeword* x*, whose MS polynomial is* $\sum_{s=0}^{n-1} \Lambda_{n-s} X^s$*, is a codeword of* C *of weight* w*. The* σ_i *are the coefficients of the locator polynomial of* x*. The number of codewords of weight* w *in* C *is equal to the number of solutions of* $\mathcal{S}_C(w)$*.*

The theory of *Gröbner bases* (see [16][68]) gives tools for solving the systems $\mathcal{S}_C(w)$. The idea is to construct a basis of the ideal generated by the polynomials occuring in the system. The aim is to obtain a reduced system with few equations or with equations which induce a description of the set of solutions. In order to do so, it is necessary to have a computer and a package for computing Gröbner bases.

This point of view, for finding minimum weight codewords in a code, was first developed by AUGOT in his thesis [5]. When it is possible to compute the Gröbner basis of the system $\mathcal{S}_C(w)$, the set of solutions is thereby described by a small set of equations – more precisely, it is almost always the case. The most important is the possibility to prove that the system has no solutions. In many situations, it is the only known way for proving that a lower bound on the minimum distance of a given code is not reached. *The system has no solutions if and only if its Gröbner basis is reduced to* $\{1\}$ – since $1 = 0$ is impossible. Otherwise we not only know the number of solutions but also some algebraic properties that these solutions satisfy. According to Corollary 3.8, this method is of most efficiency when w is the minimum distance of C. Several examples are given in [5][6]; one of them is the following.

Example 3.9 The field of order 32 is denoted by $\mathbf{F}$. Let $\mathcal{Q}$ be the *binary quadratic residue code of length* 31. It is the cyclic code with defining set

$$T = cl(1) \cup cl(5) \cup cl(7) \ .$$

The minimum distance is known to be 7. The Gröbner basis for $\mathcal{S}_{\mathcal{Q}}(7)$ was obtained by using a computer. It is the following set of polynomials

$$\left\{\begin{array}{lll} \sigma_7 + {\Lambda_{11}}^4{\Lambda_3}^{29} + {\Lambda_{11}}^2{\Lambda_3}^{26} & \sigma_6 + {\Lambda_3}^2 & \sigma_5 + \Lambda_{11}{\Lambda_3}^{29} \\ \sigma_4 + {\Lambda_{11}}^4{\Lambda_3}^{28} + {\Lambda_{11}}^2{\Lambda_3}^{25} & \sigma_3 + \Lambda_3 & \sigma_2 + \Lambda_{11}{\Lambda_3}^{28} \\ \Lambda_{15} + {\Lambda_{11}}^3{\Lambda_3}^{25} + {\Lambda_3}^5 & \sigma_1 & {\Lambda_3}^{31} + 1 \\ {\Lambda_{11}}^5 + {\Lambda_{11}}^4{\Lambda_3}^{14} + {\Lambda_{11}}^2{\Lambda_3}^{11} + \Lambda_{11}{\Lambda_3}^{25} + {\Lambda_3}^8 & & \end{array}\right\} .$$

Denote by A a value of $(\Lambda_0 \ , \dots \ , \Lambda_{30} \ , \sigma_1, \dots , \ \sigma_7)$ in $\mathbf{F}^{38}$; A is a solution of $\mathcal{S}_{\mathcal{Q}}(7)$ if and only if $f(A) = 0$, for any polynomial f belonging to the set above. Note that in the Gröbner basis only one indeterminate for each set $\{\Lambda_i, \ \Lambda_{2i} \dots\}$ appears; this is because of the conditions $A_{2i \ mod \ 31} = A_i^2$ in $\mathcal{S}_{\mathcal{Q}}(7)$. Moreover we have also in $\mathcal{S}_{\mathcal{Q}}(7)$ the equations $\Lambda_1 = 0$, $\Lambda_5 = 0$ and $\Lambda_7 = 0$, (by definition of $\mathcal{Q}$). Finally we have ten expressions with ten indeterminates, $(\Lambda_3 \ , \Lambda_{11} \ , \Lambda_{15} \ , \sigma_1, \dots , \ \sigma_7)$.

Each value in $\mathbf{F}^{10}$ of these indeterminates which is such that the ten expressions are zero gives us a solution of $\mathcal{S}_{\mathcal{Q}}(7)$. A solution is here a triple

$$(a, b, c) \in \mathbf{F}^3 \ \text{ with } \ \Lambda_3 = a, \ \Lambda_{11} = b \ , \Lambda_{15} = c \ ,$$

which is available; the values of the σ_i are deduced. In accordance with Corollary 3.8, there is a one-to-one correspondance between the solutions of $\mathcal{S}_{\mathcal{Q}}(7)$ and the codewords of weight 7 in $\mathcal{Q}$. Moreover, by using the Gröbner basis, we can say more about the set of minimum weight codewords:

1. There are $31 \times 5 = 155$ solutions. They correspond to the roots of the system :

$$ {\Lambda_{11}}^5 + {\Lambda_{11}}^4{\Lambda_3}^{14} + {\Lambda_{11}}^2{\Lambda_3}^{11} + \Lambda_{11}{\Lambda_3}^{25} + {\Lambda_3}^8 = 0 \ , \quad {\Lambda_3}^{31} + 1 = 0 \ . \tag{26}$$

   We consider above the two equations which have only Λ_3 and Λ_{11} as indeterminates.

   For each value of $(\Lambda_3 \ , \Lambda_{11})$, we deduce the values of Λ_{15} and of the σ_i from the other equations:

$$\Lambda_{15} = {\Lambda_{11}}^3{\Lambda_3}^{25} + {\Lambda_3}^5, \ \sigma_1 = 0, \ \sigma_2 = \Lambda_{11}{\Lambda_3}^{28}, \ \dots$$

   For any fixed value $a \in \mathbf{F}^*$ of Λ_3, we are sure that the first equation of (26), say

$$E(\Lambda_{11}) = 0 \ \text{ where } \ E(\Lambda_{11}) = {\Lambda_{11}}^5 + {\Lambda_{11}}^4 a^{14} + {\Lambda_{11}}^2 a^{11} + \Lambda_{11} a^{25} + a^8 \ ,$$

has five solutions in $\mathbf{F}$; indeed each root of E provides a solution which must be in $\mathbf{F}$, by definition of $\mathcal{S}_{\mathcal{Q}}(7)$ (see Theorem 3.7, **(ii)**). It remains to check that these five solutions are always pairwise distinct. Consider the derivative of $E(\Lambda_{11})$, with respect to Λ_{11}; it is the polynomial

$$\Lambda_{11}^4 + a^{25} = (\Lambda_{11} + a^{8\times 25})^4 = (\Lambda_{11} + a^{14})^4 \ .$$

But $E(a^{14}) = a^8$ and a cannot be zero, implying that $E(\Lambda_{11})$ has no multiple roots.

So there are 155 codewords of weight 7 in $\mathcal{Q}$.

2. The codewords of weight 7 do not belong to any cyclic subcode of $\mathcal{Q}$. First we have no equation $\Lambda_i = 0$, $i = 3, 11, 15$, implying that the set of codewords of weight 7 is not contained in a cyclic subcode. Can such a codeword be in a cyclic subcode?

   One easily proves that Λ_3 cannot be equal to 0 and Λ_{11} too. Indeed $\Lambda_3^{31} = 1$ yields $\Lambda_3 \neq 0$. On the other hand, from the first equation of (26), $\Lambda_{11} = 0$ would imply $\Lambda_3 = 0$, a contradiction. Finally suppose that $\Lambda_{15} = 0$. Then

$$\Lambda_{15} + {\Lambda_{11}}^3 {\Lambda_3}^{25} + {\Lambda_3}^5 = 0 \implies \Lambda_{11}^3 = \Lambda_3^{11} \ .$$

   By replacing in the first equation of (26), we obtain

$$\Lambda_{11}^5 + \Lambda_{11}^7\Lambda_3^3 + \Lambda_{11}^5 + \Lambda_{11}^7\Lambda_3^3 + \Lambda_3^8 = \Lambda_3^8 = 0 \ ,$$

   a contradiction. Thus we can conclude that there is no codeword of weight 7 in some cyclic subcode.

3. There is no idempotent — i.e. no codeword of weight 7 whose MS polynomial has binary coefficients. Indeed it is impossible to have $\Lambda_3 = 1$ and $\Lambda_{11} = 1$ and we have proved that $\Lambda_3 \neq 0$ and $\Lambda_{11} \neq 0$.

It is important to notice that for each solution (a, b, c) we are sure that the corresponding polynomial $1 + \sum_{i=2}^{7} \sigma_i X^i$ is the locator polynomial of a codeword. It means that this polynomial splits in $\mathbf{F}$ and has seven distinct roots. We point out that by means of the Gröbner basis of $\mathcal{S}_{\mathcal{Q}}(7)$ *one obtains precisely the class of polynomials corresponding to the minimum weight codewords of $\mathcal{Q}$.*

Comments on Section 3.1 Example 3.4 summarizes the efficiency of Newton identities. On the one hand the identities must be satisfied for a given weight w and for a given defining set T (i.e. some A_i are equal to zero). If a contradiction appears in the identities, then there is no codeword of weight w in the code of defining set T. On the other hand the method can produce immediately (by hand) the full set of codewords of a given weight for an infinite class of codes. Of course it is not generally the case. Moreover the method, which uses the form (19)(20) of the Newton identities, works only for codewords whose symbols are in $\{0, 1\}$. But a lot of information can be obtained in this way.

In the binary case the usual form allows us to treat any codeword. Note that the set of minimum weight codewords of binary Reed-Muller codes was first described by Kasami et al. by means of the Newton identities [90]. There are many recent applications as, for instance, the minimum distance of some BCH codes [9], codewords of minimum weight of some self-dual binary codes [54] or covering radius of some BCH codes [61]. The Newton identities can be used for the description of codewords of a large class of codes. Recent results are given in [34] concerning cyclic codes over Z_4.

The use of Newton identities for decoding is well-known (see [111, p. 273] and, for instance, [32]). We want also to cite several recent works on decoding or on decoding up to the minimum distance as, for instance, [60][67] and [131]. The use of Gröbner bases for decoding is discussed in [59] and an extensive study by de Boer and Pellikan is in [31].

Unfortunately any method, for decoding or for codeword description, which consists of computing the Gröbner basis of the system $\mathcal{S}_C(w)$ is restricted by the high complexity of Buchberger's algorithm. It is, however, the best known algorithm at the moment [98].

3.2 Special locator polynomials

This section naturally follows the preceding, concerning the description of codewords of cyclic codes. The basic idea is still to define tools for finding solutions in some system of type $S_C(w)$. In Section 3.1 we started from the concept of locator polynomials and next emphasized the significant role of MS polynomials. Now we come back to the characterization of the locator polynomials of codewords of a given cyclic code. We give here basic material and recall that little is known about a question which is connected with the determination of the splitting field of some class of polynomials.

Idempotents in $\mathcal{R}_n$ are studied in Chapter 1, §5. In our ambient space $\mathcal{M} = \mathbf{k}[\{G^*, \times\}]$ they are the codewords e which satisfy

$$\left(\sum_{g \in G^*} e_g(g) \right)^2 = \sum_{g \in G^*} e_g(g) \ . \qquad (27)$$

From the multiplication in $\mathcal{M}$, that is equivalent to

$$\sum_{uv=g} e_u e_v = e_g \quad , \quad g \in G^* \ .$$

Recall that α is a primitive nth root of unity and q is the order of the alphabet field $\mathbf{k}$. We know from Corollary 5.19 of Chapter 1 that any idempotent has the following form

$$\mathrm{e} = \sum_{s \in I} e_{\alpha^s} \sum_{i \in cl(s)} (\alpha^i) \qquad (28)$$

where I is a system of representatives of the q-cyclotomic cosets modulo n and $cl(s)$ is the coset of s. When $q = 2$ any codeword of the form (28) is an idempotent.

Proposition 3.10 *Let* x $\in \mathcal{M}$. *Then* x *has the form (28) if and only if its MS polynomial $M_{\mathrm{x}}(X)$ has coefficients in* $\mathbf{k}$. *If* x *has the form (28), its locator polynomial $\sigma_{\mathrm{x}}(X)$ has coefficients in* $\mathbf{k}$.

When $q = 2$, i.e. $\mathbf{k}$ *is the field of order two,* x *is an idempotent if and only if it satisfies one of these three following conditions*

(i) x *has the form (28);*

(ii) $M_{\mathrm{x}}(X)$ *is a polynomial of* $\mathbf{k}[X]$*;*

(iii) $\sigma_{\mathrm{x}}(X)$ *is a polynomial of* $\mathbf{k}[X]$.

Proof: Notation is that of Section 2.2. We must prove that x has the form (28) if and only if

$$(\rho_j(\mathrm{x}))^q = \rho_j(\mathrm{x}) \ , \quad 0 \leq j \leq n \ . \qquad (29)$$

Applying the inverse Fourier transform, x has the form (28) if and only if its MS polynomial satisfies $M_{\rm x}(g) = M_{\rm x}(g^q)$, for all $g \in G^*$. By definition this is equivalent to $M_{\rm x}(X^q) = M_{\rm x}(X)$ which means

$$\sum_{s=0}^{n-1} \rho_{n-s}({\rm x})\ X^s = \sum_{s=0}^{n-1} \rho_{n-s}({\rm x})\ X^{qs \bmod n} \ ,$$

which is equivalent to $\rho_j({\rm x}) = \rho_{qj}({\rm x})$, for all j. As $\rho_{qj}({\rm x}) = (\rho_j({\rm x}))^q$, this is exactly (29).

On the other hand the locator polynomial of x is in $\mathbf{k}[X]$ if and only if it is a product of some minimal polynomials on $\mathbf{k}$. That means that the support of x corresponds to a union of q-cyclotomic cosets modulo n. This property is satisfied when x has the form (28).

When $q = 2$, we know that the form (28) characterizes the set of idempotents. Since it is a binary codeword, x can be identified to its support. So $\sigma_{\rm x}(X) \in \mathbf{k}[X]$ if and only if x has the form (28). We have previously proved that **(i)** is equivalent to **(ii)** for any q, completing the proof.
♦

Example 3.11 The minimal polynomials correspond to the simplest idempotents. Consider the following polynomial which is irreducible over $GF(2)$:

$$\sigma(X) = 1 + X + X^2 + X^3 + X^5 = \prod_{i=0}^{4}(1 - \beta^{2^i} X) \ .$$

Its splitting field is $GF(2^5)$ and, since 31 is prime, any such polynomial is primitive; $\sigma(X)$ is the minimal polynomial of β^{-1}, which is a primitive root of $GF(32)$.

Now we want to know the smallest binary cyclic code of length 31 containing the codeword x whose locators are the β^{2^i}. In other words, we want to determine the cyclic code where x is the primitive idempotent. We must compute the coefficients A_i of the MS polynomial of x, for $i \in \{1, 3, 5, 7, 11, 15\}$ – a system of representatives of the 2-cyclotomic cosets $cl(i)$ modulo 31.

Since x is an idempotent, one can obtain this result without computer, by simply writing the Newton identities (given in Theorem 3.3) and replacing the values of the coefficients of the locator polynomial: $\sigma_1 = 1$, $\sigma_2 = 1$, $\sigma_3 = 1$, $\sigma_4 = 0$ and $\sigma_5 = 1$. We obtain

$$A_1 = 1 \ , \quad A_3 = 1 \ , \quad A_5 = 0 \ ,$$

and

$$A_j = A_{j-1} + A_{j-2} + A_{j-3} + A_{j-5} \ , \quad j \geq 6 \ .$$

Using the recursive formula above, one finds $A_7 = 1$, $A_{11} = 0$ and $A_{15} = 0$. So x is the primitive idempotent of the cyclic code C whose defining set is

$$T = cl(5) \cup cl(11) \cup cl(15) \ .$$

Moreover the minimum distance of C is 5 and x is a minimum weight codeword of C. Indeed $wt(\mathrm{x}) = 5$ and $20, 21, 22$ and 23 are in T, proving that the minimum distance is at least 5.

We are going to define the codewords of BCH codes by means of a set of special polynomials. Furthermore we will notice that some such polynomials correspond to the idempotents which are minimal weight codewords of some BCH codes.

Theorem 3.12 *Let $\{g_1, \ldots, g_w\}$ be a set of locators in the field $\mathbf{F}$ of characteristic p. Denote by $\sigma(X)$ the associated locator polynomial and by A_i, $i \geq 0$, the power sum functions of these locators. Let δ be a positive integer less than or equal to w. Then the coefficients σ_r of $\sigma(X)$ satisfy*

$$1 \leq r < \delta \ \ \textit{and} \ \ r \not\equiv 0 \pmod{p} \quad \Longrightarrow \quad \sigma_r = 0$$

if and only if $A_1 = A_2 = \ldots = A_{\delta-1} = 0$.

Proof: This is an immediate application of Theorem 3.3. The first w Newton identities are:

$$\begin{array}{lcl} I_1 & : & A_1 + \sigma_1 = 0 \\ I_2 & : & A_2 + \sigma_1 A_1 + 2\sigma_2 = 0 \\ & & \ldots\ldots\ldots \\ I_r & : & A_r + \sum_{i=1}^{r-1} A_{r-i}\sigma_i + r\sigma_r = 0 \\ & & \ldots\ldots\ldots\ldots \\ I_w & : & A_w + \sum_{i=1}^{w-1} A_{w-i}\sigma_i + w\sigma_w = 0 \ . \end{array}$$

Suppose that $A_1 = A_2 = \ldots = A_{\delta-1} = 0$. Then for any $r < \delta$, I_r is reduced to $r\sigma_r = 0$. Hence if p does not divide r then σ_r must be zero.

Conversely suppose that the condition on the σ_r is satisfied. Then we can prove, by induction on r, that $A_r = 0$ for $r < \delta$:

- From I_1 we have $A_1 = 0$.
- Suppose that $A_1 = A_2 = \ldots = A_{r-1} = 0$. Then the identity I_r is reduced to $A_r + r\sigma_r = 0$, where either $r \equiv 0 \pmod p$ or $\sigma_r = 0$. Hence $A_r = 0$.

♦

It is clear that the theorem above is related to the BCH bound. Actually it gives the "polynomial form" of any codeword of any BCH code of designed distance δ on $\mathbf{k}$, which has symbols from $\{0,1\}$. The following corollary is obvious, since the locators of any codeword of the BCH code of designed distance δ satisfy $A_1 = \cdots = A_{\delta-1} = 0$.

Corollary 3.13 *Let the ambient space be $\mathcal{M}$ (the characteristic is p). Let $B(\delta)$ be the BCH code of length n and designed distance δ. Consider any polynomial*

$$\sigma(X) = 1 + \sum_{1<r<\delta,\ p|r} \sigma_r X^r + \sum_{r=\delta}^{w} \sigma_r X^r \quad , \quad \sigma_r \in \mathbf{F},\ \sigma_w \neq 0\ , \qquad (30)$$

where $\mathbf{F}$ is the splitting field of $X^n - 1$. Then $\sigma(X)$ is the locator polynomial of a codeword of weight w of $B(\delta)$, whose symbols are from $\{0,1\}$, if and only if it splits in $\mathbf{F}$ and their roots are w distinct nth roots of unity.

Corollary 3.13 gives the form of the locator polynomial of any codeword of any binary BCH code. More precisely, let us denote by $B(\delta)$ a binary BCH code of length $2^m - 1$ and designed distance δ. Then $B(\delta)$ has true minimum distance δ if and only if there exists a polynomial

$$\sigma(X) = 1 + \sum_{i=1}^{(\delta-1)/2} \sigma_{2i} X^{2i} + \sigma_\delta X^\delta \qquad (31)$$

which has δ distinct roots in $\mathbf{F}$, the finite field of order 2^m. This property leads to the determination of the order of the splitting field of the polynomials of the form (31).

Such a polynomial corresponds to an idempotent if and only if its coefficients are in $GF(2)$. Augot and Sendrier proposed in [10] an algorithm for computing the extension degree of the splitting field of such *idempotent*

δ	m
3	2, 3
5	4, 5, 6
7	3, 4, 7, 10
9	6, 8, 9, 10, 14, 15, 21
11	5, 6, 8, 11, 21, 28
13	8, 9, 10, 12, 13, 14, 21, 22, 33, 35
15	4, 5, 6, 7, 9, 26, 33, 39
17	8, 9, 10, 12, 14, 15, 17, 21, 35, 39, 44, 52, 55, 65, 66, 77
19	8, 9, 10, 12, 15, 19, 21, 28, 34, 35, 39, 51, 52, 65, 66, 77, 91
21	6, 7, 8, 9, 10, 11, 15, 38, 51, 57, 68, 85
23	6, 8, 10, 11, 14, 15, 21, 23, 35, 51, 52, 57, 65, 68, 76, 85, 95, 117, 119
25	8, 10, 12, 13, 15, 18, 21, 22, 25, 28, 33, 46, 57, 68, 69, 76, 77, 95, 102, 119, 133, 153
27	6, 7, 8, 9, 10, 13, 15, 33, 44, 55, 68, 69, 76, 85, 92, 115, 187
29	10, 12, 14, 15, 16, 18, 21, 25, 26, 27, 29, 35, 39, 44, 66, 68, 69, 76, 77, 92, 95, 99, 102, 114, 115, 153, 161, 171, 187, 209, 221, 715
31	5, 6, 8, 9, 14, 21, 31, 39, 44, 52, 58, 77, 87, 92, 119, 161, 209, 221, 247, 374 , 561
33	10, 11, 12, 15, 16, 17, 18, 21, 27, 28, 39, 52, 62, 76, 87, 91, 92, 93, 95, 114, 115, 116, 133, 138, 145, 171, 175, 207, 247, 322
35	9, 10, 12, 14, 15, 16, 17, 21, 22, 25, 33, 35, 52, 65, 77, 78, 87, 91, 92, 93, 95, 114, 116, 124, 138, 143, 145, 152, 155, 203, 253, 299, 494, 741
37	8, 10, 12, 14, 15, 18, 19, 21, 27, 33, 34, 37, 44, 51, 52, 55, 65, 77, 78, 92, 93, 115, 116, 117, 119, 124, 138, 143, 155, 161, 174, 175, 203, 207, 217, 261, 299, 506
39	8, 9, 10, 12, 13, 15, 19, 21, 25, 28, 33, 35, 44, 51, 55, 68, 74, 77, 85, 111, 115, 116, 119, 124, 138, 145, 174, 186, 187, 217, 319, 322, 391, 406
41	10, 12, 14, 15, 16, 18, 21, 25, 26, 27, 35, 38, 39, 41, 44, 51, 57, 65, 66, 68, 77, 91, 99, 111, 116, 119, 124, 133, 138, 148, 155, 174, 184, 185, 186, 207, 209, 261, 279, 319, 341, 374, 377, 391, 437, 759, 1615, 2431
43	7, 8, 11, 12, 15, 18, 20, 27, 39, 43, 50, 52, 57, 65, 68, 76, 82, 85, 95, 102, 111, 115, 116, 123, 124, 138, 145, 148, 153, 174, 185, 186, 207, 221, 261, 279, 310, 377, 403, 437, 782, 1173
45	8, 9, 10, 11, 12, 14, 15, 21, 23, 25, 35, 39, 52, 57, 65, 68, 76, 85, 86, 91, 102, 119, 123, 124, 129, 133, 145, 148, 155, 164, 174, 186, 205, 217, 222, 247, 259, 403, 442, 493, 754
47	8, 9, 10, 12, 15, 21, 22, 23, 28, 33, 35, 47, 52, 55, 68, 76, 77, 78, 91, 95, 102, 114, 119, 123, 129, 133, 143, 148, 155, 164, 172, 174, 185, 186, 205, 215, 22 1, 222, 287, 325, 407, 425, 434, 493, 494, 518, 527, 551, 741, 806, 1131, 1209, 1885, 3553
49	10, 12, 14, 15, 16, 18, 21, 25, 27, 33, 35, 44, 46, 49, 52, 55, 65, 68, 69, 76, 78, 85, 94, 95, 102, 114, 117, 119, 129, 141, 143, 145, 148, 153, 164, 171, 172, 174, 186, 187, 203, 209, 215, 222, 232, 246, 248, 261, 279, 287, 299, 301, 333, 369, 407, 442, 481, 527, 551, 589, 663, 741, 986, 1131, 1209, 1479, 1771, 2387, 3059, 4199

Table 2: Binary BCH codes of length $2^m - 1$ and designed distance δ whose true minimum distance is exactly δ (see §3.2, following (31)).

polynomials. In this way they gave the true minimum distance of many BCH codes of relatively large length and dimension.

These results are presented in Table 2. Recall that extended primitive BCH codes are affine-invariant. So it is sufficient to find an idempotent either of weight δ or of weight $\delta + 1$ to ensure that the true minimum distance is δ. The codes $B(\delta)$ listed in Table 2 have this property. For every δ, $3 \leq \delta \leq 49$, a list of values of m is given. The result is precisely: *for any value of m, in the list, the true minimum distance of the BCH code of length $2^m - 1$ and designed distance δ is exactly δ.* Note that this property holds for the BCH codes of length $2^{km} - 1$, and designed distance δ, for any m in this list and for any k. This is because the idempotent of weight δ (or $\delta + 1$) corresponds to a polynomial of the form (31) which splits in $GF(2^m)$ and then in $GF(2^{km})$.

On the other hand, there is a "classical" class of lacunary polynomials: the class of polynomials of the form

$$f(X) = c + \gamma_0 X + \gamma_1 X^q + \ldots + \gamma_k X^{q^k} \tag{32}$$

with coefficients in some extension field of $\mathbf{k}$, the field of order q. These polynomials are usually called *affine polynomials* as their roots form an affine space of dimension k over $\mathbf{k}$. When $c = 0$ the roots form a vector space and $f(X)$ is said to be *a linear polynomial.* The reader can refer to [102, pp. 108-120] for basic properties. Since the derivative of $f(X)$ is reduced to γ_0 (modulo q), the roots of $f(X)$ have multiplicity one if and only if $\gamma_0 \neq 0$. So $\gamma_0 \neq 0$ is necessary if we want to consider $f(X)$ as a locator polynomial.

Now we want to give some equivalent representations of affine spaces. As the zeros of $f(X)$ form an additive structure, our ambient space is now the algebra $\mathcal{A}$. We consider only primitive codewords, i.e. $n = p^m - 1$, and the multiplicative group of $\mathcal{M}$ will be $\mathbf{F}^*$ ($\mathbf{F}$ is the field of order p^m).

Assume that the affine polynomial $f(X)$ splits in $\mathbf{F}$ with roots of multiplicity one. Then $f(X)$ can be identified to the codeword of $\mathcal{A}$ whose support is the affine space of their roots and whose symbols are from $\{0, 1\}$. More precisely define the codewords of the form

$$\mathrm{x} = \lambda X^h \sum_{g \in V_k} X^g \quad , \quad \lambda \in \mathbf{k} \ , \tag{33}$$

where V_k is a subspace of $\mathbf{F}$ of dimension k over $\mathbf{k}$. Such a codeword can be identified with an affine polynomial whose roots are the elements of the affine space $h + V_k$, up to scalar multiplication. In the next proposition, we characterize the locator polynomial of any codewords x of the form (33) (in the sense of Definition 3.1).

Proposition 3.14 *Let the ambient space be $\mathcal{A}$. Let $\delta = q^k - 1$, $\delta < n$, and set*

$$\mathcal{I}_k = \{ \ q^k - q^j \mid j \in [0, k-1] \ \} \ .$$

Define the polynomial of degree δ ($\sigma_\delta \neq 0$):

$$\sigma(X) \ = \ 1 \ + \sum_{i \in \ \mathcal{I}_k} \sigma_i X^i \quad , \quad \sigma_i \in \mathbf{F} \ .$$

Denote by v_i the roots of $\sigma(X)$ and set $g_i = v_i^{-1}$. Then **(i)** *and* **(ii)** *are equivalent.*

(i) *$\sigma(X)$ splits in $\mathbf{F}$ with roots of multiplicity one.*

(ii) *$\sigma(X)$ is the locator polynomial of the codewords of the form (33) such that $h = 0$ and V_k is the set $\{0, g_1, \ldots, g_\delta\}$.*

Proof: We simply observe that the polynomial

$$f(X) = X^{q^k} \sigma(X^{-1}) = X^{q^k} + \sum_{j=0}^{k-1} \gamma_j X^{q^j} \ ,$$

where $\gamma_j = \sigma_i$ with $i = q^k - q^j$, is a linear polynomial. Clearly, **(i)** holds if and only if $f(X)$ has q^k distinct roots in $\mathbf{F}$ and that means that the set of the roots of $f(X)$ is the support of a codeword of the form (33) with $V_k = \{0, g_1, \ldots, g_\delta\}$ and $h = 0$. It is equivalent to say that $\sigma(X) = \prod_{i=1}^{\delta}(1 - g_i X)$, where $\{0, g_1, \ldots, g_\delta\}$ is a subspace of dimension k of $\mathbf{F}$, i.e. it has exactly property **(ii)**.
♦

We defined the GRM codes in Section 2.2 and keep the same notation (see Definition 2.8). Recall that considering GRM codes of length $p^m - 1$ over the alphabet field of order q, $q = p^r$, the order is in the range $[1, m'(q-1) - 1]$ where $m = rm'$; the GRM code of order ν is denoted by $\mathcal{R}_q(\nu, m)$. It is quite easy to prove that the codewords of the form (33), whose weight is q^k, belong to the set of minimum weight codewords of the GRM code of order ν, $\nu = (m' - k)(q - 1)$. A proof is given in Chapter(Assmus-Key). It was first proved by Kasami et al. by using the following property [91, Theorem 9].

Theorem 3.15 *Let V_k be any subspace of* $\mathbf{F}$ *of dimension k over* $\mathbf{k}$. *Then the power sum functions*

$$A_i = \sum_{v \in V_k} v^i \ , \quad i \in [1, p^m - 1] \ ,$$

are zero when the q-weight of i is less than $k(q-1)$ – i.e. when i is in the defining set of $\mathcal{R}_q(\nu, m)$, $\nu = (m' - k)(q-1)$.

By using this theorem and the usual Newton identities, the authors described the set of minimum weight codewords of binary Reed-Muller codes. We want to show that their result can be expanded by using the generalized Newton identities. Note that the set of minimum weight codewords of any GRM code was described in another way (see comments in Section 3.2).

Lemma 3.16 *Let $\delta = q^k - 1$; $\mathcal{I}_k$ is defined in Proposition 3.14. Let* x *be a codeword of the punctured GRM code $\mathcal{R}^*_q(\nu, m)$, $\nu = (m' - k)(q-1)$. Then the MS polynomial of* x *is such that $\rho_s(\mathrm{x}) = 0$ for any $1 \le s < \delta$ and*

$$s \in [1, \delta - 1] \ , \quad s \notin \mathcal{I}_k \quad \Longrightarrow \quad \rho_{s+\delta}(\mathrm{x}) = 0$$

(see (1) for the definition of ρ_s).

Proof: Recall that the defining set of $\mathcal{R}^*_q(\nu, m)$ is the set

$$T_\nu = \{ \ s \in [0, q^{m'} - 1] \mid wt_q(s) < k(q-1) \ \} \ .$$

A codeword x is in $\mathcal{R}^*_q(\nu, m)$ if and only if $\rho_s(\mathrm{x}) = 0$ for all $s \in T_\nu$.

First observe that $\delta = \sum_{i=0}^{k-1} (q-1) q^i$. Clearly $wt_q(\delta) = k(q-1)$ and any $s < \delta$ is such that $wt_q(s) < k(q-1)$ – i.e. s is in T_ν and then $\rho_s(\mathrm{x}) = 0$. Therefore

$$2\delta = 2q^k - 2 = (q-2) + \sum_{i=1}^{k-1} (q-1) q^i + q^k \ ,$$

providing $wt_q(2\delta) = k(q-1)$; note that 2δ, as δ, is not in T_ν.

Set $t = \delta + s$ with $s \in [1, \delta - 1]$. It remains to prove that t is in T_ν whenever $s \notin \mathcal{I}_k$. We easily deduce, from the form of the q-ary expansion of 2δ, that any $t < 2\delta$ has a q-weight less than or equal to $k(q-1)$. Suppose that $wt_q(t) = k(q-1)$. The general form of such a t, $\delta < t < 2\delta$, is

$$t = \sum_{i=0}^{k-1} t_i q^i + \epsilon q^k \ , \quad \epsilon \in \{0, 1\} \ , \quad t_i \in \{q-2, \ q-1\} \ ,$$

where $\epsilon = 1$ (since $t \neq \delta$) and $t_0 = q-1$ (since $t \neq 2\delta$). More precisely $wt_q(t) = k(q-1)$ yields that one and only one t_j, $j > 0$, must be equal to $q-2$ – i.e. $t = \delta + q^k - q^j$, with $j \in [1, k-1]$.

We have proved that the set of those t, $\delta \leq t \leq 2\delta$, such that $wt_q(t) = k(q-1)$ is the set of those t which satisfy: $t = \delta + s$ with $s \in \mathcal{I}_k \cup \{0\}$.

Finally when $s \in [1, \delta-1]$ and $s \notin \mathcal{I}_k$, we have $wt_q(\delta+s) < k(q-1)$ meaning $\delta + s \in T_\nu$, completing the proof.

♦

Lemma 3.17 *Denote by C the GRM code $\mathcal{R}_q^*(\nu, m)$ of length $n = q^{m'} - 1$, $\nu = (m'-k)(q-1)$. Let $\delta = q^k - 1$ and let $\mathcal{S}_C(\delta)$ be the system (25), written for the codewords of weight δ of C. The defining set is T_ν. Then any solution $(\Lambda_1, \ldots, \Lambda_n, \sigma_1, \ldots, \sigma_\delta)$ of $\mathcal{S}_C(\delta)$ satisfies the following statements.*

(i) $\Lambda_1 = \Lambda_2 = \ldots = \Lambda_{\delta-1} = 0$.

(ii) *If $s \in [1, \delta-1]$ and $s \notin \mathcal{I}_k$, then $\Lambda_{\delta+s} = 0$ and $\sigma_s = 0$.*

(iii) *If $s \in \mathcal{I}_k$, then $\sigma_s = \Lambda_{\delta+s}/\Lambda_\delta$.*

Proof: Recall that $\mathcal{I}_k$ is the set of the $q^k - q^j$, $j \in [0, k-1]$. Statement **(i)** and a part of statement **(ii)** are immediately deduced from Lemma 3.16. Indeed it was proved that the defining set of C contains $[1, \delta-1]$ and any $s + \delta$ such that $s \in [0, \delta-1]$ and $s \notin \mathcal{I}_k$. Now we write the first Newton identities, taking into account the condition $\{ \Lambda_i = 0 \ , \ i \in [0, \delta-1] \ \}$.

$$\begin{array}{lll}
I_1 & : & \Lambda_{\delta+1} + \Lambda_\delta \sigma_1 = 0 \\
I_2 & : & \Lambda_{\delta+2} + \Lambda_{\delta+1}\sigma_1 + \Lambda_\delta \sigma_2 = 0 \\
 & & \cdots\cdots\cdots \\
I_s & : & \Lambda_{\delta+s} + \sum_{i=1}^{s} \Lambda_{\delta+s-i}\sigma_i = 0 \\
 & & \cdots\cdots\cdots\cdots\cdots \\
I_{2\delta-1} & : & \Lambda_{2\delta-1} + \Lambda_{2\delta-2}\sigma_1 + \ldots + \Lambda_\delta \sigma_{\delta-1} = 0
\end{array}$$

There are other Λ_i which are zero because the full condition is $\{ \Lambda_i = 0 \ , \ i \in T_\nu \ \}$. The proof follows by simply replacing some Λ_i by zero in the system above.

We proceed by induction on s. Since we do not treat trivial GRM codes, it is clear that $1 \notin \mathcal{I}_k$. So $\Lambda_{\delta+1} = 0$ and I_1 gives $\sigma_1 = 0$. Now we assume the following hypothesis, say H_r: *for $r \in [0, s-1]$, if $r \notin \mathcal{I}_k$ then $\sigma_r = 0$ else $\sigma_r = \Lambda_{\delta+r}/\Lambda_\delta$.* Consider every term $\Lambda_{\delta+s-i}\sigma_i$, $i < s$, of the identity I_s. We have:

- If $i \notin \mathcal{I}_k$ then $\sigma_i = 0$ from H_i.
- If $i \in \mathcal{I}_k$ then $i = q^k - q^j$, j in the range $[0, k-1]$. As $i < s < q^k - 1$, $s - i < q^j - 1$ with $q^j - 1 < q^{k-1}$. Hence $s - i \notin \mathcal{I}_k$ implying $\Lambda_{\delta+s-i} = 0$.

So the identity I_s is in fact $\Lambda_{\delta+s} + \Lambda_\delta \sigma_s = 0$. If $s \notin \mathcal{I}_k$ then $\Lambda_{\delta+s} = 0$ and $\sigma_s = 0$, otherwise $\sigma_s = \Lambda_{\delta+s}/\Lambda_\delta$. Note that $\Lambda_\delta = 0$ is impossible because this would imply that all the Λ_i are zero (one can also say that the BCH bound would be strictly greater than δ).

♦

Theorem 3.18 *The minimum weight codewords of the punctured GRM code $\mathcal{R}_q^*(\nu, m)$, $\nu = (m' - k)(q-1)$, are the codewords of weight $\delta = q^k - 1$ whose locators are the nonzero elements of some subspace V_k of $\mathbf{F}$ of dimension k and whose symbols are from $\{0, 1\}$, up to scalar multiplication. These are in the algebra $\mathbf{k}[\{\mathbf{F}^*, \times\}]$ precisely the codewords*

$$\mathrm{x} = \lambda \sum_{g \in \ V_k^*} (g) \quad , \quad \lambda \in \mathbf{k} \ . \tag{34}$$

The locator polynomial is

$$\sigma_{\mathrm{x}}(X) = 1 \ + \sum_{\substack{s = q^k - q^j \\ j \in [0, k-1]}} \frac{\rho_{\delta+s}(\mathrm{x})}{\rho_\delta(\mathrm{x})} X^s \ . \tag{35}$$

The minimum weight codewords of $\mathcal{R}_q(\nu, m)$ are the codewords of $\mathcal{A}$ of weight q^k which are of the form (33).

Proof: This is an application of Corollary 3.8. In Lemma 3.17 we studied the solutions of the system $\mathcal{S}_C(\delta)$, where $C = \mathcal{R}_q^*(\nu, m)$ and δ is the minimum weight of C. We know that in this case the set of the solutions of $\mathcal{S}_C(\delta)$ is the set of the minimum weight codewords of C. For any solution the Λ_i are the coefficients of the MS polynomial, and the σ_i are the coefficients of the locator polynomial of such a word. So we have proved that any minimum weight codeword of C has a locator polynomial of the form (35).

On the other hand, we know from Proposition 3.14 that the roots of such a polynomial are the non zero elements of some subspace V_k of $\mathbf{F}$ of dimension k. Moreover we know that any codeword of the form (34) is a minimum weight codeword of $\mathcal{R}^*_q(\nu,m)$. So the symbols of the minimum weight codewords are from $\{0,1\}$, up to a scalar multiplication. Indeed two minimum weight codewords which have the same support are obtained one from the other by scalar multiplication. The set of the minimum weight codewords of C is the set of codewords of the form (34).

GRM codes are affine-invariant codes. Hence the minimum weight codewords of $\mathcal{R}_q(\nu,m)$ are the codewords of $\mathcal{A}$ of weight q^k which are either an extension of any minimum weight codeword of $\mathcal{R}^*_q(\nu,m)$ or any translation of these extended codewords. They are the codewords X^hx, where x is the extension of a minimum weight codeword of $\mathcal{R}^*_q(\nu,m)$ and $h \in \mathbf{F}$. These are exactly the codewords of the form (33).
♦

Comments on Section 3.2 Our purpose is to emphasize, with an elementary presentation, that any property of polynomials on finite fields can apply to the description of codewords of cyclic codes. We have chosen to present the best known polynomials concerned with codewords of cyclic codes. They are more or less lacunar and this property, evidently, gives simplifications for solving the algebraic systems of type (25).

It appears in [10] that binary narrow-sense BCH codes often have a minimum weight codeword which is an idempotent, and the authors ask for a theoretical explanation of their numerical results.

In Theorem 3.15, the values of some power sum functions are given for codewords whose supports are vector spaces. The result, due to Kasami et al. [91], is based on a report from Pele [122]. Note that there is no other general result on the other power sum functions of these codewords. We remark that Theorem 3.18 gives the form of the coefficients of the locator polynomials of codewords whose supports are vector spaces.

Denote by W the set of the minimum weight codewords of the binary BCH code of length 2^m-1 and minimum distance $2^{m-2}-1$. It was proved that W is equal to the set of the minimum weight codewords of the punctured Reed-Muller code $\mathcal{R}^*_2(2,m)$ [9][41]. It is probably an exception which, however, could happen also for some non binary primitive BCH codes. We know that the p-ary Reed-Muller codes (extended or not) are generated by their minimum weight codewords (see Chapter(Assmus-Key) and also [3]). This leads to the general problem: for which other cyclic codes does this property hold ?

The number of minimum weight codewords of GRM codes was obtained by Delsarte, Gœthals and MacWilliams [64]. At the beginning of their proof, the authors *hasten to point out that it would be very desirable to find a more sophisticated and shorter proof.* Another description of the set of minimum weight codewords was proposed in [20], but the proof used the cardinality of this set. We cannot say, at present, if our method which leads to the description of the set of minimum weight codewords of GRM codes of some orders (Theorem 3.18) can be generalized to GRM codes of any order. Furthermore we are not sure that it can provide a proof shorter than the preceding. Actually our aim is merely to illustrate the use of Newton identities and then to suggest other applications.

3.3 On the minimum distance of BCH codes

The BCH codes are, for many reasons, considered as the *most important* cyclic codes. They are presented in Chapter 1 and appear in several others (Tietaveinen-Huffman-Brualdi.Litsyn.Pless) because of their connection with many open problems. In this section we want to present recent numerical results on the true minimum distance of primitive binary BCH codes and their duals. Actually there are few theoretical results for the pionering work of Berlekamp [22, 23] and Kasami et al. [87, 88, 89, 90, 93]. In this context there is a challenge which consists in the improvement of the numerical results. This is a good way for testing the efficiency of algorithms for finding minimum weight codewords in a given code. But above all the numerical results could suggest interesting conjectures.

Recall that BCH codes are defined in Section 2.2 (Definition 2.9). In this section we consider binary BCH codes of length $2^m - 1$; we will always assume that the designed distance is the smallest representative of its 2-cyclotomic coset.

In the previous section we have pointed out that the problem of finding the minimum distance of BCH codes is connected with the existence of some kinds of polynomials. In Section 2.4 we indicated that the group algebra approach can lead to applications on minimum distance of non binary BCH codes. On the other hand the Weil bound is an interesting tool for studying the duals (see Theorem 3.21). In the binary case this bound is actually the so-called Carlitz-Ushiyama bound:

Theorem 3.19 *Denote by $B(\delta)$ the binary BCH code of length $2^m - 1$ and designed distance δ with $\delta = 2t + 1$. Assume that*

$$2t - 1 \; < \; 2^{\lceil m/2 \rceil} \; + \; 1 \; .$$

Then the weight w of any codeword in $B^{\perp}(\delta)$ satisfies

$$2^{m-1} - 2^{m/2}(t-1) \leq w \leq 2^{m-1} + 2^{m/2}(t-1) \; .$$

Note that w must be even.

The BCH bound is generally a good bound for BCH codes since one can say that the true minimum distance is roughly close to the BCH bound. It is easy to find examples of non primitive binary BCH codes whose minimum distance exceeds the BCH bound (see [111, p.205] and [47, 84]).

When the codes are binary and primitive, it is usually conjectured that the true minimum distance d does not exceed $\delta + 4$, δ being the designed distance. Kasami and Tokura first proved that d can exceed δ [93, 1969]. This result was obtained by means of the divisibility of the RM codes. They have shown that *for any $m > 6$, m different from 8 and 12, there are some binary BCH codes of length $2^m - 1$ and designed distance δ such that $d > \delta$.* Quite recently Augot et al. completed the table of the minimum distance of BCH codes of length 255 [9, 1991]. By using Newton identities they proved that two such codes have true minimum distance $\delta + 2$. These are the BCH codes with designed distance 59 and 61. At the moment the case $m = 12$ remains open.

On the other hand the true minimum distances of BCH codes of length 511 are not all known. The more recent results are due to Canteaut and Chabaud [38]. In their paper, a probabilistic algorithm for finding small-weight words in any linear code is presented; this algorithm applies successfully to the determination of the minimum distance of some BCH codes.

The BCH codes of length $n = 511$, dimension k and designed distance δ are listed in Table 3. The true minimum distance is denoted by d. When d is known, we indicate the paper where the result can be found. We want to conclude by some comments on the results presented in this table.

- The value of d is not known for six codes. These are the BCH codes with designed distance

$$59 \; , \quad 61 \; , \quad 75 \; , \quad 77 \; , \quad 85 \text{ and } \; 107.$$

k	δ	d	in	k	δ	d		in
502	3	3	[89]	241	73	73		[123]
493	5	5	[89]	238	75	≥ 75		—
484	7	7	[89]	229	77	≥ 77		—
475	9	9	**	220	79	79		*
466	11	11	[89]	211	83	83		*
457	13	13	[76]	202	85	≥ 85		—
448	15	15	[89]	193	87	87		***
439	17	17	**	184	91	91		*
430	19	19	*	175	93	95	#	[93]
421	21	21	[123]	166	95	95		[89]
412	23	23	[89]	157	103	103		*
403	25	25	[76]	148	107	≥ 107		—
394	27	27	[89]	139	109	111	#	[93]
385	29	29	***	130	111	111		[89]
376	31	31	[89]	121	117	119	#	[93]
367	35	35	[123]	112	119	119		[89]
358	37	37	***	103	123	127	##	*
349	39	39	*	94	125	127	#	[93]
340	41	41	***	85	127	127		[89]
331	43	43	***	76	171	171		**
322	45	45	*	67	175	175		**
313	47	47	[89]	58	183	183		**
304	51	51	***	49	187	187		**
295	53	53	*	40	191	191		[89]
286	55	55	[89]	31	219	219		[123]
277	57	57	*	28	223	223		[89]
268	59	≥ 59	—	19	239	239		[89]
259	61	≥ 61	—	10	255	255		[89]
250	63	63	[89]					

#	$d = \delta + 2$
##	$d = \delta + 4$
*	new result obtained by Newton's identities [9]
**	new result obtained by an exhaustive search [9]
***	new result obtained with a probabilistic algorithm [38]

Table 3: The binary narrow-sense BCH codes of length 511, §3.3.

- Most results are due to KASAMI et al.. Theorem 1 of [89] applies to a large class of BCH codes. It is obtained by studying the intersection of BCH codes with shortened RM codes.

- Four codes have minimum distance $\delta + 2$; this is due also to KASAMI et al. by using the 4-divisibility of the RM code of order four [93].

  By using Newton identities, it was established that the BCH code of designed distance 123 has minimum distance 127 [9]. Taking into account several numerical results, we conjecture that *any BCH code of length $2^m - 1$ and designed distance $\delta = 2^{m-2} - r$, $r = 3$ or 5 has true minimum distance greater than δ.*

- We have $511 = 7 \times 73$. Consider B, a BCH code of length 511 whose designed distance is $\delta = 7 \times \delta_2$. For any available value of δ_2, the BCH code of length 73 and designed distance δ_2 has true minimum distance δ_2. Hence B has true minimum distance δ. There is a similar property when the designed distance is $\delta_1 \times 73$. All these results can be derived from a general one which can be found in [123, p.278]. Note that the general context is the study of *cyclic product codes* [70, 103].

- The true minimum distances

  $$d \;=\; 19,\; 39,\; 45,\; 53,\; 57,\; 79,\; 83,\; 91,\; 103,$$

  are obtained by finding an idempotent of weight d or $d+1$ in the code [9].

- The true minimum distances 13 and 25 were computed by considering a “shortened code” [76].

- When $\delta \leq 9$ one can also deduce d from [111, Theorem 2, p.259]. This general theorem, easily proved, shows that BCH codes with small designed distance δ have true minimum distance δ.

On the other hand, the CARLITZ-USHIYAMA bound (CU bound) gives an interesting estimation of the minimum distance of the dual $B^{\perp}(\delta)$ of the BCH code $B(\delta)$ of length $2^m - 1$ and designed distance δ. However this bound is trivial when

$$\delta \geq 2^{\lceil m/2 \rceil} \;+\; 3 \;.$$

δ	Theoretical bound	Schaub's bound
3	128	128*
5	112	112*
7	96	96*
9	80	88
11	64	64
13	48	64
15	32	60
17 , 19	24	42
21	24	40
23, 25, 27	24	32
29	16	28
31	16	26
37	14	22
39	12	22
43, 45	12	20
47, 51, 53	12	16
55, 59	12	?
61, 63, 85	8	?
87, 91, 95, 111	6	?
119, 127	4	?

Table 4: Lower bounds for the minimum distance of duals of binary BCH codes of length 255 and designed distance δ (see § 3.3).

Moreover it seems to be really significant only when the dimension of the dual is small. The Weil bound, which can be used for any cyclic code, has these drawbacks.

A recent study, due to Augot and Levy-dit-Vehel gives us new numerical results on the minimum distance of duals of primitive BCH codes [11]. In this paper the best known theoretical bound is checked by using a new algorithm which is based on Theorem 2.5. The theoretical bound is determined from the CU bound (the Weil bound for non binary codes) and from the results of Levy-dit-Vehel. In [100, 101], she determined the divisibility of duals of primitive BCH codes and gave new lower bounds for duals of large dimension (when the other bounds do not work). On the other hand an algorithmic method, due to Massey and Schaub, called *the rank-bounding algorithm* [115, 127], was implemented. The results on duals of primitive BCH codes are *surprisingly higher than all previously known bounds* [11][100].

As an example we give in Table 4 the lower bound on the minimum distance of binary codes $B^{\perp}(\delta)$ of length 255. The symbol "*" means that the bound is the true minimum distance. The sign "?" means that the rank-bounding algorithm fails; it cannot compute the bound. The CU bound does not work for $\delta > 19$. When $\delta \leq 19$ the theoretical lower bound is "combinatorial", based on the Roos bound [101]. One can see that for $13 \leq \delta \leq 53$ the rank-bounding algorithm produces a lower bound widely higher than the theoretical lower bound. Generally the numerical results obtained in this way show that the approximation of the minimum distance of the duals of primitive BCH codes remains an open problem.

Comments on Section 3.3 In this section we pointed out the interest in some recent numerical observations concerning specific difficult questions; they induce or strengthen several conjectures. The general problem is, however, the determination of the weight enumerators of any BCH code.

The most recent numerical results on the weight distributions of BCH codes are due to Desaki, Fujiwara and Kasami [65]. By using an original algorithm, the authors obtain all weight enumerators of extended binary primitive BCH codes of length 128. They observe that the extended BCH code of length 128 and dimension k has the same weight distribution as the dual of the extended BCH code of dimension $128 - k$, when $k = 29, 36, 43, 64, 85, 92, 99$.

There is a lot of work on the CU bound, the Weil bound and their applications to cyclic codes. This subject is treated in Chapter(Tietavainen). The recent work of RODIER [126] on duals of binary primitive BCH codes is also explained in that chapter.

3.4 On the weight enumerators

To find new tools for the study of weight enumerators is a classical research problem in coding theory. We wish to show that it is a motivating subject by presenting some fundamental tools through famous unsolved problems and examples. These tools – in particular, the MacWilliams transform, the Pless identities, invariant theory and Gauss sums – provide important, but partial, results. So it appears that it is necessary to find new tools or original methods combining several tools in order to solve a number of essential problems.

We assume that the basic presentation, given in Chapter 1 (Section 10), is known.

We would like to introduce this section by recalling two important theorems. The first one, due to MCELIECE [105], provides an algorithm for the determination of the divisibility of any given p-ary cyclic code; an application will be presented in Section 3.4.3 (Proposition 3.35). The second one gives a lower bound and an upper bound for the weights of cyclic codes. It comes from the results of WEIL and SERRE on the number of rational points of algebraic curves and was adapted by WOLFMANN to the case of cyclic codes [146]; the use of this theorem is explained in the next example.

Theorem 3.20 *Let C be a cyclic code of length n over $\mathbf{k}$ where $\mathbf{k}$ is a prime field of order p. Let T be the defining set of C and denote by U the set $\{\ s \in [0, n-1] \mid s \notin T\ \}$. Suppose that $0 \notin U$. Let w be the smallest integer satisfying*

1. *$w \equiv 0 \pmod{p-1}$, and*

2. *there are w elements of U (with repetition allowed), say $u_1, \ldots,\ u_w$, such that the sum $\sum_{i=1}^{w} u_i$ equals 0 modulo n. Note that any element may occur t times, $t \leq p-1$.*

Then for any $\mathrm{c} \in C$, the weight of c satisfies

$$wt(\mathrm{c}) \equiv 0 \pmod{p^{\lambda}}\ ,\quad \lambda = \frac{w}{p-1} - 1\ .$$

Moreover there is a c *in* C *such that* $wt(\mathrm{c}) \not\equiv 0 \pmod{p^{\lambda+1}}$. *In other words, the code* C *is* p^{λ}*-divisible and not* $p^{\lambda+1}$*-divisible*

Theorem 3.21 *Let* C *be a cyclic code of length* n *over* $\mathbf{k}$*, the field of order* q*. Set* $n\nu = q^{m'} - 1$*, where* $q^{m'}$ *is the order of* $\mathbf{F}$*, the splitting field of* $X^n - 1$*. Let* T *be the defining set of* C *and let* $T^{\perp}$ *be the defining set of* $C^{\perp}$*. Denote by* $\mathcal{J}$ *a set of representatives of the cyclotomic cosets of* q *modulo* n *belonging to* $T^{\perp}$*. Let* θ *be the biggest element in* $\mathcal{J}$*.*

If every element of $\mathcal{J}$ *is prime to* p*, then the non-zero weights* w *of* C *satisfy :*

(i) *If* $0 \in T$ *then*

$$\left| w - \frac{q^{m'-1}(q-1)}{\nu} \right| \leq \frac{(\theta\nu - 1)(q-1)}{2\nu q} \lfloor 2q^{\frac{m'}{2}} \rfloor \ .$$

(ii) *If* $0 \notin T$ *then*

$$\left| w - \frac{q^{m'-1}(q-1) - 1}{\nu} \right| \leq \frac{(\theta\nu - 1)(q-1)}{2\nu q} \lfloor 2q^{\frac{m'}{2}} \rfloor \ .$$

Example 3.22 In order to explain the use of Theorem 3.21, we study the dual C of the ternary BCH $[80, 68, 5]$ code. Thus $q = 3$, $n = 3^4 - 1 = 80$ ($\nu = 1$ and $m' = 4$) and the defining set of $C^{\perp}$ is

$$T^{\perp} = \{1, 3, 9, 27\} \cup \{2, 6, 18, 54\} \cup \{4, 12, 36, 28\} \ .$$

The defining set of C is the set of those t such that $n - t \notin T^{\perp}$; in particular $0 \in T$. The set $\mathcal{J}$ is a system of representatives of the cyclotomic cosets included in $T^{\perp}$; each representative must be prime to 3. Clearly the best choice, producing the best bound, is $\mathcal{J} = \{1, 2, 4\}$, implying $\theta = 4$. According to Theorem 3.21 **(i)**, the non zero weights w of C satisfy

$$2.3^3 - 2.3^2 \frac{2(4-1)}{6} \leq w \leq 2.3^3 + 2.3^2 \frac{2(4-1)}{6}$$

giving $36 \leq w \leq 72$. These bounds are attained. By using the coding package of MAGMA we obtain the weight enumerator of C, say $W(x, y)$,

$$\begin{aligned} W(x,y) &= x^{80} + 800x^{44}y^{36} + 26720x^{35}y^{45} + 77220x^{32}y^{48} \\ &\quad +108000x^{29}y^{51} + 154880x^{26}y^{54} + 112320x^{23}y^{57} \\ &\quad +37800x^{20}y^{60} + 13600x^{17}y^{63} + 100x^{8}y^{72} \ . \end{aligned}$$

Note that C is self-orthogonal; therefore it is 3-divisible. The Weil bound gives an excellent result; this is because the dimension of $C^{\perp}$ is small, as we noticed in Section 3.3.

3.4.1 The Reed-Muller codes

The weight enumerators of GRM codes are not known. This fundamental problem is heavily connected with many open problems on primitive codes and on related discrete objects.

In particular few weight enumerators of binary Reed-Muller codes are known. The weight enumerators of the RM codes of orders one and two are known. As $\mathcal{R}_2(m-\nu-1,m)$ is dual to $\mathcal{R}_2(\nu,m)$, the weight enumerators of $\mathcal{R}_2(m-2,m)$ and of $\mathcal{R}_2(m-3,m)$ are also known (see Theorem 13.3 of Chapter 1). It is an old problem to find the weight enumerators of $\mathcal{R}_2(\nu,m)$, $3 \le \nu \le m-4$.

Carlet pointed out that it is as difficult to find a general characterization of the weights in the RM code of order three as it is to obtain one in the RM codes of any order [39]. In any case it seems that the problem is to find a good formulation. Such a formulation was found for the self-dual RM codes.

Assume that m is odd and set $\tau = (m-1)/2$. The code $\mathcal{R}_2(\tau,m)$ is equal to its dual since $m-\tau-1=\tau$. On the other hand the divisibility of RM codes is well-known to be $2^{\lceil m/\nu \rceil -1}$, where ν is the order (see a proof in Chapter(tietav-honkala) Theorem 4.17). So all weights in $\mathcal{R}_2(\tau,m)$ are divisible by four – i.e. *$\mathcal{R}_2(\tau,m)$ is a doubly-even self-dual code.* The general form of weight enumerators of doubly-even binary self-dual codes is known from the work of Gleason. We have for $\mathcal{R}_2(\tau,m)$ the following result.

Theorem 3.23 *Let ϕ_8 and ϕ_{24} be respectively the weight enumerator of the extended Hamming code and the weight enumerator of the extended Golay code:*

$$\phi_8 = x^8 + 14x^4y^4 + y^8$$

and

$$\phi_{24} = x^{24} + 759\ (x^{16}y^8 + x^8y^{16}) + 2576\ x^{12}y^{12} + y^{24}\ .$$

Then the weight enumerator of $\mathcal{R}_2(\tau,m)$, $\tau=(m-1)/2$ and m odd, is of the form

$$W_m(x,y) = a_0\phi_8^{2^{m-3}} + a_1\phi_8^{2^{m-3}-3}\phi_{24} + \ldots + a_i\phi_8^{2^{m-3}-3i}\phi_{24}^{i} + \ldots + a_r\phi_8\phi_{24}^{r}\ , \quad (36)$$

where $r = (2^{m-3} - 1)/3$ *and the* a_i *are numbers to be determined. Now, setting* $t = (m+1)/2$*, the coefficients* b_i *of* $W_m(x,y)$ *satisfy:*

1. *if* $i \not\equiv 0 \pmod 4$*, then* $b_i = 0$,
2. $b_1 = b_2 = \ldots = b_{2^t-1} = 0$*, and*
3. *if* $2^t \leq s < 2^{t+1}$ *and* $s \notin \{\ 2^{t+1} - 2^j \mid 2 \leq j \leq t\ \}$*, then* $b_s = 0$.

Proof: Recall the notation of $W_m(x,y)$:

$$W_m(x,y) = \sum_{i=0}^{2^m} b_i\ x^{n-i}y^i$$

where b_i is the number of codewords of weight i in $\mathcal{R}_2(\tau, m)$. As the code is 4-divisible, any b_i such that $i \not\equiv 0 \pmod 4$ is zero. Formula (36) is due to Gleason [69]. We have written his general formula only for length 2^m. Note that 3 divides $2^{m-3} - 1$ because m is odd.

The minimum weight of $\mathcal{R}_2(\tau, m)$ is 2^t, $t = m - \tau = (m+1)/2$. This may be deduced from the BCH bound, implying the second condition on the b_i. The third one is deduced from a general result of Kasami [92] (see comments in Section 3.4.1).

♦

The weight enumerators of the self-dual RM codes are not known for $m \geq 9$. In the following example we will show how one can determine $W_m(x,y)$ for lengths 32 and 128 by means of the previous theorem.

Example 3.24 First recall that $\mathcal{R}_2(1,3)$ is the extended Hamming code and then $W_3(x,y)$ is exactly $\phi_8(x,y)$. The code $\mathcal{R}_2(2,5)$ is a $[32,16,8]$ self-dual code; we obtain from (36):

$$\begin{aligned} W_5(x,y) &= a_0\phi_8^4 + a_1\phi_8\phi_{24} \\ &= a_0(x^8 + 14x^4y^4 + y^8)^4 + a_1(x^8 + 14x^4y^4 + y^8) \\ &\quad (x^{24} + 759x^{16}y^8 + 2576x^{12}y^{12} + 759x^8y^{16} + y^{24}) . \end{aligned}$$

Since there is only one codeword of weight zero, we have $a_0 + a_1 = 1$. Moreover the code has no codeword of weight four and the coefficient of $x^{28}y^4$ is $14(4a_0 + a_1)$. This leads to $a_0 = -1/3$ and $a_1 = 4/3$, giving

$$W_5(x,y) = x^{32} + 620\,x^{24}y^8 + 13888\,x^{20}y^{12} + 36518\,x^{16}y^{16} + 13888\,x^{12}y^{20} + 620\,x^8y^{24} + y^{32} .$$

Note that we have proved again that the weight enumerator of all doubly-even self-dual $[32,16,8]$ codes is unique. Actually this code is extremal and this property holds for any extremal doubly-even self-dual code (see Section 10 of Chapter 1).

The code $\mathcal{R}_2(3,7)$ is a $[128,64,16]$ doubly-even self-dual code with weight enumerator of the following form:

$$W_7(x,y) = a_0\phi_8^{16} + a_1\phi_8^{13}\phi_{24} + a_2\phi_8^{10}\phi_{24}^2 + a_3\phi_8^7\phi_{24}^3 + a_4\phi_8^4\phi_{24}^4 + a_5\phi_8\phi_{24}^5 \ ,$$

where $a_0, \ldots, a_5$ are not known. By using this formula, is it possible to determine all the coefficients b_i of the polynomial $W_7(x,y)$?

We have $b_0 = 1$ and, according to Theorem 3.23, $b_4 = b_8 = b_{12} = b_{20} = 0$. Moreover, the number b_{16} of minimum weight codewords of $\mathcal{R}_2(3,7)$ is 3309747 (see [111, Chapter 13, Theorem 9]). By computing the corresponding coefficients in $W_7(x,y)$ we obtain successively:

$$a_0 = 1 - a_1 - \ldots - a_5 \ \ , \quad a_1 = 16/3 - 2a_2 - 4a_3 - 3a_4 - 5a_5 \ ,$$

$$a_2 = 4084/441 - 3a_3 - 6a_4 - 10a_5 \ \ , \quad a_3 = 17944/3087 - 4a_4 - 10a_5 \ ,$$

$$a_4 = 46568/46305 - 79a_5/20 \ , \quad a_5 = 5628589/5445468 \ .$$

We solved the equations on the b_i by using a symbolic computation software. The coefficients of $W_7(x,y)$ are given in Table 5. As we have determined $W_7(x,y)$, we know the weight enumerators of all RM codes of length 128. Indeed the other RM codes of length 128 are those of order one and two and their duals.

Comments on Section 3.4.1 Our main reference on self-dual codes is [111, chapter 19], where an extensive study of the work of Gleason is given. See also Chapter 1 and Chapter(sloane). The self-dual affine-invariant codes are studied in [54] (for characteristic 2 only). Generally an extended cyclic code which is self-dual is doubly-even (see a proof in [99]). For this reason, it is clear for us that there is no self-dual binary extended narrow-sense BCH code. In a recent paper, the weight distributions of binary extended narrow-sense BCH codes of length 128 are given [65]. Hence the extended $[128,64,22]$ BCH code is formally self-dual.

Kasami and Tokura determined in [92] the number of codewords of weight w, $d \leq w < 2d$, of any RM code of minimum weight d (see also [111,

weights	number of words	weights	number of words
16, 112	3309747	44, 84	50059881835741
24, 104	2144705388	48, 80	94150059881835741
28, 100	9507508544	52, 76	549678173926151424
32, 96	37527010290	56, 72	1920946561829079256
36, 92	19957889171264	60, 68	4051419446028441984
40, 88	94150059881835741	64	5194232755773662458

Table 5: Weight enumerator of the binary self-dual Reed-Muller code of length 128.

chapter 15]). However this knowledge is not sufficient for determining the weight enumerator of the self-dual RM code $\mathcal{R}_2(4,9)$ of length 512 using the method of Example 3.24. In this case the number of indeterminates is 21 while we know the value of only 16 coefficients b_i in $W_9(x,y)$. Are there other invariants, like ϕ_8 and ϕ_{24}, especially for weight enumerators of RM codes ?

The weight enumerators of RM codes of length 2^m, $m \leq 8$, are known. They are studied and given in [143]. The most recent result on RM codes of length 2^9 is due to Sugita et al. who have determined the weight enumerator of $\mathcal{R}_2(3,9)$ (see [135] and their references). Since the dual of $\mathcal{R}_2(3,9)$ is $\mathcal{R}_2(5,9)$, only the weight enumerator of $\mathcal{R}_2(4,9)$, the self-dual code, remains unknown.

Little is known about weight enumerators of GRM codes except their divisibilities and the set of their minimum weight codewords. Can the result of Kasami and Tokura [92] be generalized ? Note however that the weight enumerator of any GRM code of order two was given by McEliece [104]. For the minimum weight codewords of GRM codes, see comments in Section 3.2.

On the *relatives* of GRM codes (see [64] and Chapter(Assmus-Key)), we want to mention the *projective GRM codes*. Sorensen has studied their parameters in [133]; in particular he gave their minimum distances. Moreover he proved that some of these codes are cyclic, describing precisely a subclass of cyclic projective GRM codes.

3.4.2 On cyclic codes with two zeros

In this section we consider binary codes of length $n = 2^m - 1$. Recall that the field of order 2^m, the support field, is denoted by $\mathbf{F}$ and that α is a primitive nth root of the unity. Moreover codes are *cyclic and have only two zeros, i.e. the defining set is composed of two distinct* 2*-cyclotomic cosets modulo* n. For short we will say $T = \{r, s\}$ for such a defining set, where r and s are the coset representatives, and the code with defining set T will be denoted by $C_{r,s}$.

This section is concerned with the classification of the codes $C_{r,s}$ by means of their minimum distance. Our aim is to recall that this classification is not yet achieved; furthermore the determination of the weight enumerators appears as a most difficult problem. At the moment the known tools, that we will present in proving Theorem 3.30, are efficient only for the characterization of codes which are *optimal* in a certain sense. We begin by showing that the minimum distance of the codes $C_{r,s}$ cannot be more than 5.

Theorem 3.25 *Let $n = 2^m - 1$, $m \geq 4$. Let $C_{r,s}$ be the binary cyclic code with defining set $\{r, s\}$ and minimum distance d. Then we have*

(i) $2 \leq d \leq 5$ *and*

(ii) $d = 2$ *if and only if* $gcd(r, s, n) > 1$.

Proof: The parity check matrix of $C_{r,s}$ has the form

$$\mathcal{H} = \begin{bmatrix} 1 & \alpha^r & \alpha^{2r} & \dots & \alpha^{(n-1)r} \\ 1 & \alpha^s & \alpha^{2s} & \dots & \alpha^{(n-1)s} \end{bmatrix} .$$

The dimension k of $C_{r,s}$ satisfies $k \geq n - 2m$. As there is no zero column in $\mathcal{H}$, $d \geq 2$.

On the other hand, the sphere packing bound gives $d \leq 6$ (see Chapter 1, Section 2) and the existence of an $[n, k, d]$ code obviously induces the existence of an $[n - 1, k, d - 1]$ code. Assuming $d = 6$, we could construct a $[2^m - 2, k, 5]$ code with $k \geq 2^m - 1 - 2m$. But such a code does not exist (see [33]). Finally $2 \leq d \leq 5$ completing the proof of **(i)**.

The code $C_{r,s}$ contains a codeword of weight 2 if and only if two columns of $\mathcal{H}$ are equal; one can easily check that this is equivalent to $gcd(r, s, n) > 1$. ♦

Considering the codes $C_{1,\ell}$, van Lint and Wilson presented another proof of this last theorem and gave a further result: *if $gcd(\ell, n) > 1$ and m is odd, the minimum distance of $C_{1,\ell}$ is at most four* [141, Theorem 12].

We remark that the minimum distance of codes with defining set $\{1, \ell\}$ is clearly dependent upon properties of affine subspaces of dimension two, a fact that we noticed in the comments of Section 3.2. Indeed denote by V a subset of four distinct elements of $\mathbf{F}$; if $\sum_{v \in V} v = 0$ then V is a 2-dimensional affine subspace of $\mathbf{F}$; it is a linear subspace when V contains 0. So Theorem 3.25 and the result above are related to the values of the ℓth power sum functions of the affine subspaces of dimension two and can be rewritten as follows

Corollary 3.26 *The minimum distance of $C_{1,\ell}$ is at most five. It is three or four if and only if there is an affine subspace V of $\mathbf{F}$ of dimension 2 satisfying $\sum_{v \in V} v^\ell = 0$. This is always the case when $gcd(\ell, n) \neq 1$ and m is odd.*

The purpose of van Lint and Wilson in [141] is to prove that cyclic codes with only two zeros are generally bad. According to Theorem 3.25, "bad" means that $d \leq 4$. In [142], the same authors use a deep theorem of algebraic geometry for studying the special case $\ell = 7$. They proved that the minimum distance is less than or equal to 4 when $m \geq 18$. It was later shown that this property holds when $m < 18$, unless $m = 5$, by computing some codewords of weight four [6]. The method introduced in [142] was generalized by Janwa et al. [81, 82], providing a lot of results which strengthened the previous conjecture. By applying a form of Weil's theorem they showed that, for a large class of codes with defining set $\{1,\ \ell\}$, only a finite number could be "good". However the problem of finding codes with defining set $\{1,\ \ell\}$ and minimum distance five remains open. The known classes are the class of the Melas codes (see Example 3.27) and two famous other classes due to Kasami [87, 88]:

- The first one is composed of codes $C_{1,\ell}$ with $\ell = 2^i+1$ and $gcd(i, m) = 1$. Note that their duals are in $\mathcal{R}_2^*(2, m)$, the punctured RM code of order two (see an extensive study in [111, Chapter 15]). The Preparata codes are constructed by concatenating some of their cosets (see §4.3).

- The second one corresponds to those ℓ such that $\ell = 2^{2i} - 2^i + 1$ with $gcd(i, m) = 1$ (the proof for m even is actually due to Janwa et al.).

These classes are both of most interest when m is odd because they are composed of codes which are *optimal* in the following sense: the dual code has only three weights and the best minimum distance; the weight enumerator of the dual is unique, equal to those of the dual of the 2-error-correcting BCH code. *We have here exceptional objects which appear in other contexts*, as the study of parameters of sequences (see Chapter(Kumar-helleseth)) or the determination of cryptographic primitives with "good" properties (see Section 4.1).

The remainder of this section will be devoted to the characterization of these optimal objects. On the other hand the Melas codes, which have minimum distance 5 when m is odd, are never optimal as we show now.

Example 3.27 The Melas code M_m is the cyclic code of length $n = 2^m - 1$ with defining set $\{1, -1\}$. When m is odd, the minimum distance is 5; this can be proved by using the Hartmann–Tzeng bound (see Chapter 1, Theorem 6.3).

Indeed the defining set contains these three pairs:

$$(1,\ 2)\ ,\quad (2^{m-1}-1,\ 2^{m-1})\ ,\quad (-1,\ -2)\ ,$$

and so contains all the elements

$$1+i+jc\ ,\quad 0 \le i \le \delta - 2\ ,\quad 0 \le j \le s\ ,$$

where $\delta = 3$, $s = 2$ and $c = 2^{m-1} - 2$. Moreover $gcd(2^m - 1, c) = 1$, since $2^m - 1 = (2^{m-1} - 2) + (2^{m-1} + 1)$ implies $gcd(2^m - 1, c) = gcd(2^m - 1, 2^{m-1} + 1)$, and it is well-known that $2^r + 1$ is prime to $2^m - 1$, for any r, when m is odd. Finally the HT bound is equal to $\delta + s = 5$; this yields that the minimum distance is exactly five.

When m is even the minimum distance of the codes M_m is three, since it contains the codeword whose locators are

$$1\ ,\quad \alpha^{\lambda}\ ,\quad \alpha^{2\lambda} \quad \text{with} \quad \lambda = \frac{2^m - 1}{3}\ ,$$

the three non zero elements of the field of order four. On the other hand the dual of M_m has "many" weights. This was established by Lachaud and Wolfmann [94] (see more in Section 3.4.3).

Now we come back to the optimal codes. We will focus on the exceptional properties of the codes of length $2^m - 1$, m odd, with defining set

$$\{\ 1,\ 2^{2i} - 2^i + 1\ \}\ ,\quad gcd(i, m) = 1\ , \tag{37}$$

in proving Theorem 3.32 later. These codes are equivalent to codes of type $C_{r,s}$, $r = 2^i + 1$ and $s = 2^{3i+1}$; the dual of $C_{r,s}$ is then contained in the RM code of order 2. KASAMI proved that such codes are optimal in a more general context, the determination of the weight enumerator of a number of cyclic subcodes of the RM code of order 2 [88, Remark 3].

To prove that these codes $C_{r,s}$ are optimal necessitates the use of several classical tools; it is interesting to notice that, at the moment, the optimality can be proved only for subcodes of $\mathcal{R}^*(2,m)$ – as we will show in the proof. We have chosen the elements of the proof in [87][88] or [141] because we want to present different methods which could apply to a large class of codes. The restriction "m odd" is necessary here but not generally.

The main part of the proof is obtained by means of the first *Pless power moments*. The ℓth-power moments, derived from MacWilliams identities, were given by PLESS in [124]. We need to recall the first four power moments, for codes whose minimum distance is at least 3, and a fundamental theorem (see also Chapter 1, §10).

Lemma 3.28 *Let C be any linear code of length n and dimension k. Let $C^\perp$ be the dual code. Let us denote by a_w (resp. b_w), $w \in [0,n]$, the number of codewords of weight w in C (resp. in $C^\perp$). Assume that $b_1 = b_2 = 0$ – i.e. the minimum distance of $C^\perp$ is at least three. Then the first four power moments of the weight distribution of C (and $C^\perp$) are:*

$$\begin{aligned}
\sum_{w=0}^{n} w a_w &= 2^{k-1} n \\
\sum_{w=0}^{n} w^2 a_w &= 2^{k-2} n(n+1) \\
\sum_{w=0}^{n} w^3 a_w &= 2^{k-3}(n^2(n+3) - 3!\; b_3) \\
\sum_{w=0}^{n} w^4 a_w &= 2^{k-4}(n(n+1)(n^2+5n-2) + 4!\; (b_4 - n b_3)) \; . \qquad (38)
\end{aligned}$$

Our notation is that of Lemma 3.28.

Theorem 3.29 [Theorem 10.7, Chapter 1] *Let S be a subset of $[1,n]$ containing s elements. Then the weight distributions of C and $C^\perp$ are uniquely determined by $b_1, b_2, \ldots, b_{s-1}$ and the a_i with $i \notin S$.*

The next theorem is actually due to KASAMI [87, Theorem 13]. We give a more general presentation, including codes of any dimension.

Theorem 3.30 *Let C be any linear code of length n and dimension k where $n = 2^m - 1$ and m is odd. Suppose that C does not contain the all-one vector. Assume that the dual code $C^\perp$ has minimum distance at least three. Let us denote by a_w (resp. b_w), $w \in [0, n]$, the number of codewords of weight w in C (resp. in $C^\perp$). Let w_0 be the smallest w such that*

$$a_w + a_{2^m - w} \neq 0 \ , \quad 0 \ < \ w \ < \ 2^{m-1} \ .$$

The dimension of C cannot satisfy $k < m$; for $k \geq m$ we have the following statements.

(i) *If $k \geq 2m$ then w_0 satisfies*

$$w_0 \ \leq \ 2^{m-1} - 2^{(m-1)/2} \ .$$

Moreover if equality holds, then $b_3 = b_4 = 0$, $k = 2m$ and the weight distribution of C is the same as the weight distribution of the dual of the double-error-correcting BCH code, which is

Weight	*Number of words*
0	1
$2^{m-1} - 2^{(m-1)/2}$	$(2^m - 1)(2^{m-2} + 2^{(m-3)/2})$
2^{m-1}	$(2^m - 1)(2^m + 1)$
$2^{m-1} + 2^{(m-1)/2}$	$(2^m - 1)(2^{m-2} - 2^{(m-3)/2})$

(ii) *If $m \ \leq \ k \ < \ 2m$, then the minimum distance of $C^\perp$ is at most four. Moreover if $w_0 \ \geq \ 2^{m-1} - 2^{(m-1)/2}$, then*

$$b_3 + b_4 \leq \left((2^{m-1} - 1)(2^{3m-3} - 2^{k+m-3})\right) / (3.2^{k-1}) \ . \qquad (39)$$

Proof: We consider the identities $I_\ell = \sum_{w=1}^{n} (w - 2^{m-1})^\ell a_w$. Since for ℓ even

$$(w - 2^{m-1})^\ell = ((2^m - w) - 2^{m-1})^\ell \ ,$$

we have for any even ℓ that

$$I_\ell = \sum_{w=1}^{n} (w - 2^{m-1})^\ell a_w = \sum_{w=w_0}^{2^{m-1}-1} (w - 2^{m-1})^\ell (a_w + a_{2^m - w}) \ . \qquad (40)$$

Note that the codeword of weight zero is not taken into account in the sum above; on the other hand, by hypothesis, C does not contain the all-one codeword.

The values of I_2 and I_4 are simply obtained by using the four power moments given by (38). We do not develop all the computations, indicating the way only. Recall that $\sum_{w=1}^{n} a_w = 2^k - 1$.

$$\begin{aligned} I_2 &= 2^{2m-2}\sum_{w=1}^{n} a_w - 2^m \sum_{w=1}^{n} w a_w + \sum_{w=1}^{n} w^2 a_w \\ &= 2^{2m-2}(2^k-1) - 2^m 2^{k-1} n + 2^{k-2} n(n+1) \ , \end{aligned}$$

$$\begin{aligned} I_4 &= \sum_{w=1}^{n} \left(2^{4m-4} a_w - 2^{3m-1} w a_w + 3.2^{2m-1} w^2 a_w - 2^{m+1} w^3 a_w + w^4 a_w \right) \\ &= 2^{4m-4}(2^k-1) - 2^{3m+k-2} n + 3.2^{2m+k-3} n(n+1) - 2^{m+k-2}(n^2(n+3) - 3!\ b_3) \\ &\quad +2^{k-4}(n(n+1)(n^2+5n-2) + 4!\ (b_4 - n b_3)) \ . \end{aligned}$$

We replace n by $2^m - 1$ and obtain

$$I_2 = 2^{k+m-2} - 2^{2m-2} \tag{41}$$

and

$$I_4 = 2^{k+m-4}(3.2^m - 2) - 2^{4m-4} + 3.2^{k-1}(b_3 + b_4) \ . \tag{42}$$

Now we consider by (40)

$$I_4 - 2^{m-1} I_2 = \sum_{w=w_0}^{2^{m-1}-1} (w - 2^{m-1})^2 \left((w-2^{m-1})^2 - 2^{m-1}\right)(a_w + a_{2^m - w}) \ . \tag{43}$$

Note that $|w - 2^{m-1}| \le 2^{(m-1)/2}$ implies that the wth term above is less than or equal to zero. From (41) and (42) we have

$$I_4 - 2^{m-1} I_2 = (2^{m-1} - 1)(2^{k+m-3} - 2^{3m-3}) + 3.2^{k-1}(b_3 + b_4) \ . \tag{44}$$

When $k < m$, the value of I_2 is strictly negative which is impossible, proving that C cannot satisfy the hypothesis of the theorem.

(i) Suppose that $k \ge 2m$. Then, from (44), the value of $I_4 - 2^{m-1} I_2$ cannot be negative. In the sum (43), the terms corresponding to those w satisfying

$2^{m-1} - 2^{(m-1)/2} < w < 2^{m-1}$ are negative. Thus we have proved that the value of w_0 is at most $2^{m-1} - 2^{(m-1)/2}$.

When $w_0 = 2^{m-1} - 2^{(m-1)/2}$, the only possibility is $I_4 - 2^{m-1}I_2 = 0$ (see (43)). We deduce from (44) that $k = 2m$ and $b_3 + b_4 = 0$. Therefore C has dimension $2m$ and $C^\perp$ has minimum distance at least five; moreover only three a_w are unknown which correspond to

$$w = 2^{m-1} \pm 2^{(m-1)/2} \quad \text{or} \quad w = 2^{m-1} \ .$$

Now we apply Theorem 3.29. As $b_1 = b_2 = 0$ and the a_w are unknown for only three values of w, the weight enumerator of C (and of $C^\perp$) is unique. Since the 2-error-correcting BCH code satisfies our hypothesis, its weight polynomial is the solution.

(ii) If $k = m$, then $I_2 = 0$, proving that C has only one weight, $w = 2^{m-1}$, – i.e. the code C has the same weight distribution as the simplex code.

Assume that $m \leq k < 2m$. There is no linear code with parameters $[2^m - 2, k' \geq 2^m - 2m - 1, 5]$ [33]. If there exists a linear $[2^m - 1, 2^m - 2m, 5]$ code then we can construct a linear $[2^m - 2, 2^m - 2m - 1, 5]$ code, a contradiction. So the minimum distance of $C^\perp$ is at most four.

When $w_0 \geq 2^{m-1} - 2^{(m-1)/2}$, the value of $I_4 - 2^{m-1}I_2$ must be less than or equal to zero (see (44)), giving condition (39) on $b_3 + b_4$ and completing the proof.
♦

Corollary 3.31 *The hypotheses are those of Theorem 3.30. Furthermore $k = 2m$.*

When C is a subcode of $\mathcal{R}^*(2, m)$, the punctured RM code of order two, then w_0 equals $2^{m-1} - 2^{(m-1)/2}$ if and only if $b_3 = b_4 = 0$.

In other words, the weight enumerator of C is the same as the weight enumerator of the dual of the double-error-correcting BCH code if and only if C has minimum distance five.

Proof: The weight distribution of the code $\mathcal{R}^*(2, m)$ is well-known (see Theorem 13.3 of Chapter 1). In particular when m is odd, this code has no words of weight w such that $2^{m-1} - 2^{(m-1)/2} < w < 2^{m-1}$. Therefore this property holds for any subcode C of $\mathcal{R}^*(2, m)$. So in accordance with (43) and (44), we have

$$\begin{aligned} I_4 - 2^{m-1}I_2 &= \sum_{w=w_0}^{2^{m-1}-2^{(m-1)/2}} (w-2^{m-1})^2[(w-2^{m-1})^2-2^{m-1}](a_w+a_{2^m-w}) \\ &= 3.2^{k-1}(b_3+b_4)\ , \end{aligned}$$

where $(w-2^{m-1})^2-2^{m-1} \geq 0$ for any w in the range $[w_0, 2^{m-1}-2^{(m-1)/2}]$. Then $b_3+b_4=0$ means $a_w+a_{2^m-w}=0$ unless w is in $\{\ 2^{m-1}\pm 2^{(m-1)/2},\ 2^{m-1}\ \}$. ♦

Theorem 3.32 *Let $n=2^m-1$, where m is odd, $m>4$. Let $m=2t+1$ and $j\in[1,t]$ such that $gcd(j,m)=1$. Let C be the binary cyclic code of length n with defining set*

$$\{\ 2^j+1,\ 2^{3j}+1\ mod\ n\ \},$$

Then the minimum distance of C is five. Moreover the weight distribution of the dual code $C^\perp$ is exactly the weight distribution of the dual of the double-error-correcting BCH code (see Theorem 3.30).

Note that C is equivalent to the code whose defining set is given by (37).

Proof : Note that the value of $2^{3j}+1$ is to be considered modulo 2^m-1. Let us denote by d the minimum distance of C; we know from Theorem 3.25 that $d\leq 5$. First we remark that

$$2^{3j}+1=(2^j+1)(2^{2j}-2^j+1) \quad \text{with} \quad gcd(2^j+1,n)=1\ ,$$

since m is odd. Then the code C is equivalent to the code $C_{1,t}$, $t=2^{2j}-2^j+1$ (see (37)).

The dual of C is the cyclic code with defining set

$$\{\ 0,\ \ldots,\ n-1\ \}\setminus\left\{cl(2^m-2^j-1)\cup cl(2^m-2^{3j}-1)\right\}\ .$$

Recall that the defining set of $\mathcal{R}^*(2,m)$ is

$$\{\ s\in[0,n-1]\mid 0<wt_2(s)<m-2\ \}.$$

So $C^\perp$ is contained in $\mathcal{R}^*(2,m)$. Hence if we show that $d\geq 5$, then we can apply Corollary 3.31 and prove the theorem.

After the first proof of KASAMI it was proved that $d=5$ by VAN LINT and WILSON [141] and, more recently, by JANWA et al. [81].

We will briefly explain the proof given in [141, Theorem 17]. For any subset of $\mathbf{F}^*$, let $A = \{\alpha^{i_1},\ \ldots,\ \alpha^{i_u}\}$, denote by $M(A)$ the following matrix

$$M(A) = \begin{pmatrix} 1 & \alpha^{i_1} & \alpha^{2i_1} & \ldots & \alpha^{(n-1)i_1} \\ 1 & \alpha^{i_2} & \alpha^{2i_2} & \ldots & \alpha^{(n-1)i_2} \\ 1 & .. & .. & \ldots & .. \\ 1 & \alpha^{i_u} & \alpha^{2i_u} & \ldots & \alpha^{(n-1)i_u} \end{pmatrix}$$

For a fixed ℓ, consider the ranks of any ℓ columns of $M(A)$. We denote by $r(\ell, A)$ the minimum of these ranks. For any two subsets A and B, the *product* of A and B is denoted by AB. This is the set of the elements $\xi\nu$, $\xi \in A$ and $\nu \in B$. In accordance with [141, Theorem 5], every time we can find A and B such that AB is contained in the defining set of C, then we have the following property: there could be a codeword of weight ℓ in C only if ℓ satisfies

$$r(\ell, A) \ + \ r(\ell, B) \ \leq \ell \ .$$

Taking $A = \{\alpha^{2^j},\ \alpha^{2^{3j}}\}$ and $B = \{\alpha,\ \alpha^{2^{2j}},\ \alpha^{2^{4j}}\}$, it is easy to check that AB is contained in the defining set of C. Moreover it is clear that any two columns of $M(A)$ have rank two. It is proved in [141, Lemma 4] that any four columns of $M(B)$ have rank three. Now suppose that there exists a codeword x $\in C$ of weight ℓ, with $3 \leq \ell \leq 5$. Then for each value of ℓ we have $r(\ell, A) \geq 2$ and $r(\ell, B) \geq 3$, implying $\ell \geq 5$. We have proved that $d = 5$.

Since $C^\perp$ is in $\mathcal{R}^*(2, m)$ and the minimum distance of C is five, then the weight enumerator of $C^\perp$ is exactly the weight enumerator of the dual of the double-error-correcting BCH code, completing the proof.

♦

Explanation of Tables 6, 7 and 8 Our purpose is to illustrate this section by giving the minimum distance and the weight enumerators of the dual codes of all codes $C_{1,\ell}$ of length 511. Recall that $C_{1,\ell}$ is the binary cyclic code whose zero's are α, α^ℓ and their conjugates – α being a primitive root of $GF(2^9)$.

In Table 6, we give for each value of ℓ the minimum distance d of $C_{1,\ell}$ and a reference p_i denoting the weight enumerator of $C_{1,\ell}^\perp$. Since there are 60 2-cyclotomic cosets modulo 511, there are 59 codes $C_{1,\ell}$. Two such codes can only be equivalent under a multiplier, because 511 and $\varphi(511)$ are relatively prime (φ is the Euler function). This means that $C_{1,\ell}$ is equivalent to $C_{1,t}$

ℓ	d	wed	ℓ	d	wed	ℓ	d	wed	ℓ	d	wed	ℓ	d	wed
3	5	p_1	5	5	p_1	7	4	p_2	9	3	p_3	11	3	p_4
13	5	p_1	15	3	p_5	17	5	p_1	19	5	p_1	21	4	p_2
23	3	p_4	25	3	p_4	27	5	p_1	29	3	p_6	31	5	p_1
35	4	p_2	37	3	p_7	39	3	p_8	41	4	p_9	43	3	p_4
45	4	p_{10}	47	5	p_1	51	3	p_{11}	53	3	p_6	55	3	p_{12}
57	3	p_3	59	5	p_1	61	4	p_{13}	63	4	p_{14}	73	3	p_{15}
75	3	p_{16}	77	3	p_{17}	79	3	p_6	83	4	p_{18}	85	3	p_{19}
87	5	p_1	91	4	p_{20}	93	3	p_4	95	3	p_8	103	5	p_1
107	3	p_4	109	3	p_4	111	4	p_{13}	117	4	p_{18}	119	4	p_{21}
123	3	p_6	125	4	p_{10}	127	3	p_{19}	171	5	p_1	175	4	p_{22}
183	3	p_7	187	4	p_9	191	3	p_{11}	219	3	p_{23}	223	3	p_{12}
239	3	p_5	255	5	p_{24}									

Table 6: The codes $C_{1,\ell}$ of length 511; d is the minimum distance and wed designates the weight enumerator of the dual code. The weight enumerators p_i are given in Tables 7 and 8. These tables are explained at the end of Section 3.4.2.

if and only if $t = \ell^{-1}$ with $gcd(\ell, 511) = 1$, where the inverse is calculated modulo 511 (see Theorem 5.22 in Chapter 1).

The weight enumerators p_i are given in Table 7 (*list* 1) and Table 8 (*list* 2). One obtains, in all, 24 weight enumerators p_i, $1 \leq i \leq 24$.

Note that 12 codes have p_1 as weight enumerator; 5 of them, $C_{1,\ell}$ with $\ell \in \{3, 5, 13, 17, 47\}$, are duals of the known optimal codes previously described. The code $C_{1,19}$ corresponds to the Welsh conjecture, that we give below. Up to equivalence we have then all the optimal codes we expected. The only non optimal code with minimum distance 5 is $C_{1,255}$, the Melas code. This situation does not hold for $m > 9$. Other optimal codes and other non optimal codes with minimum distance 5 will appear.

To conclude we remark that other weight enumerators, such as p_4, appear several times. Note that the weight enumerators p_{15} and p_{23} have minimum weight greater than 240.

Comments on Section3.4.2 As we already said, the properties of the binary primitive codes with two zeros are linked with the properties of sequences (see a recent example in [35]); for instance codes with two zeros and

p_1	w	240	256	272						
	a_w	69496	131327	61320						
p_2	w	196	228	232	236	244	248	252	256	260
	a_w	73	511	9198	13797	13797	45990	64605	511	18396
	w	264	268	276	280	284				
	a_w	52122	29127	4599	4818	4599				
p_3	w	224	256	288						
	a_w	18396	229439	14308						
p_4	w	224	240	256	272	288				
	a_w	4599	55188	146657	55188	511				
p_5	w	224	232	236	240	244	248	252	256	260
	a_w	4599	4599	9198	9198	19929	22995	51100	37814	27594
	w	264	268	272	276	280				
	a_w	32193	9198	18396	13797	1533				
p_6	w	216	232	240	248	256	264	272	280	
	a_w	511	13797	27594	50589	76139	59787	27594	6132	
p_7	w	208	216	224	232	240	248	256	264	272
	a_w	1533	511	4599	10731	13797	50589	83804	68985	27594
p_8	w	232	240	248	256	264	272	280	288	
	a_w	15330	27594	50589	74606	55188	36792	1533	511	
p_9	w	224	232	240	248	256	264	272	280	312
	a_w	4599	4599	22995	70518	71540	50589	32193	4599	511
p_{10}	w	232	240	248	256	264	272	280		
	a_w	13797	18907	70518	79205	32193	41391	6132		
p_{11}	w	232	236	240	244	248	252	256	260	264
	a_w	15330	13797	4599	13797	18396	41902	42413	41391	27594
	w	268	272	276	292					
	a_w	13797	22995	4599	1533					
p_{12}	w	204	212	232	236	240	244	248	252	256
	a_w	511	1533	10731	13797	4599	13797	18396	36792	51611
	w	260	264	268	272	276				
	a_w	36792	32193	18396	13797	9198				
p_{13}	w	232	240	248	256	264	272	280	312	
	a_w	13797	27594	52122	76139	59787	27594	4599	511	

Table 7: The weight enumerators of the duals of the codes $C_{1,\ell}$ of length 511: *list* 1. The number of codewords of weight w is denoted by a_w. This table is explained at the end of Section 3.4.2.

p_{14}	w	196	228	236	240	244	248	252	256	260
	a_w	73	4599	4599	24528	27594	18396	41610	28105	36792
	w	264	268	272	276	280	300			
	a_w	27594	24528	9198	9198	4818	511			
p_{15}	w	244	256	260	276	292				
	a_w	1533	511	1533	511	7				
p_{16}	w	208	224	232	240	248	256	264	272	
	a_w	1533	1533	9198	28105	55188	56210	82782	27594	
p_{17}	w	196	216	220	228	232	236	244	248	252
	a_w	73	1533	1533	511	9198	13797	13797	36792	55407
	w	256	260	264	268	276	280			
	a_w	511	18396	64386	41391	4599	219			
p_{18}	w	224	232	240	248	256	264	272	280	312
	a_w	1533	4599	41391	55188	56210	68985	32193	1533	511
p_{19}	w	228	232	240	244	248	252	256	260	264
	a_w	9198	4599	13797	18396	36792	32704	30149	45990	22995
	w	268	272	280						
	a_w	24528	13797	9198						
p_{20}	w	196	228	232	236	244	248	252	256	260
	a_w	73	511	4599	18396	13797	59787	50808	511	18396
	w	264	268	276	280					
	a_w	38325	42924	4599	9417					
p_{21}	w	196	220	232	236	240	244	248	252	256
	a_w	73	1533	4599	4599	13797	36792	22995	37011	32704
	w	260	264	268	272	276	280	288	300	
	a_w	32193	22995	27594	13797	9198	219	1533	511	
p_{22}	w	196	232	236	240	244	248	252	256	260
	a_w	73	4599	13797	15330	27594	22995	27813	28105	50589
	w	264	268	272	280	284	300			
	a_w	22995	24528	18396	219	4599	511			
p_{23}	w	244	252	256	268	292				
	a_w	1533	511	511	1533	7				
p_{24}	w	234	236	238	240	242	244	246	248	250
	a_w	4599	9198	4599	4599	22995	10731	9198	22995	9198
	w	252	254	256	258	260	262	264	266	268
	a_w	13797	22995	10220	9709	18396	13797	13797	13797	4599
	w	270	272	274	276	278				
	a_w	9198	18396	9198	4599	1533				

Table 8: The weight enumerators of the duals of the codes $C_{1,\ell}$ of length 511: *list* 2. The number of codewords of weight w is denoted by a_w. This table is explained at the end of Section 3.4.2.

minimum distance three provide binary sequences which have *the trinomial property*. On the other hand we will give, in Section 4.1, an example of the involvement of codes with two zeros in some cryptographic problems.

To characterize new cyclic codes with two zeros which are optimal, even not optimal but with minimum distance five, remains a hard open problem. There are no results other than those of KASAMI. We want to mention the oldest conjecture, the so-called *conjecture of Welsh*: the codes $C_{1,\ell}$, of length $2^m - 1$, with

$$\ell = 2^t + 3 \quad \text{and} \quad m = 2t + 1 \ ,$$

have minimum distance five; furthermore they have the same weight enumerator as the 2-error-correcting BCH code.

The papers of JANWA et al. explain why generally the minimum weight of binary cyclic codes with two zeros is not more than four [81][82]. On the other hand, CHARPIN et al. introduced tools for the classification of primitive binary cyclic codes of distance three [58]: when the length is $2^m - 1$ where m is not a prime, one can characterize many such codes; in some cases it is possible to give exactly the number of codewords of weight three. However the whole description of cyclic codes of minimum distance three remains an open, and apparently, difficult problem.

A very difficult problem is the determination of the weight enumerator of cyclic codes with two zeros, even when codes whose minimum distance is known are considered. All numerical results show that the number of distinct weight enumerators for such codes increases with the length $2^m - 1$. On the other hand several codes have the same weight enumerator and are not equivalent. As an example, we treat the case $m = 9$ in Tables 6, 7 and 8 which are explained above.

Note that for cyclic codes whose duals are contained in the Reed-Muller code of order two, the classification is not achieved. We do not know the weight enumerator of any cyclic code whose zeros have the form $\alpha^{2^i+2^k}$; for instance such codes which have the same weight enumerator as the 3-error-correcting BCH code are not yet characterized (see [144]).

To conclude we want to mention possible extensions of the tools that we have presented to other codes and to odd characteristics.

3.4.3 On irreducible cyclic codes

Irreducible cyclic codes are also said to be minimal cyclic codes because they are the minimal ideals of the algebra $\mathcal{R}_n$ of cyclic codes of length n over $\mathbf{k}$.

More precisely an irreducible cyclic code is a cyclic code which has only one non zero (see Chapter 1, Theorem 5.25). We first present this definition in the ambient space $\mathcal{M} = \mathbf{k}[G^*]$, where $\mathbf{k}$ is the field of order q and G^* is the multiplicative group of order n over $\mathbf{k}$ (see §2.2). The splitting field of $X^n - 1$ is denoted by $\mathbf{F}$ and has order $q^{m'}$.

Definition 3.33 *Let α be an nth root of unity. Denote by $cl(t)$, $1 \leq t \leq n-1$, the q-cyclotomic coset modulo n containing t.*

An irreducible cyclic code C with parameters $[n, m']$ is a cyclic code of $\mathcal{M}$ whose defining set is of the form

$$\{ \ s \in [0, n-1] \mid s \notin cl(-k) \ \} \ ,$$

where $cl(-k)$ is assumed to have cardinality m'. Then the MS polynomial of C is

$$M_C(X) = \lambda X^k + \lambda^q X^{kq} + \cdots + \lambda^{q^{m'-1}} X^{q^{m'-1} k \ mod \ n} \ , \ \lambda \in \mathbf{F} \ .$$

Note that $M_C(X) = Tr(\lambda X^k)$ where Tr is the trace function from $\mathbf{F}$ to $\mathbf{k}$. Set $\beta = \alpha^k$; if β is an nth root of unity, then the codewords of C are the n-tuples

$$\big(\ Tr(\lambda), \ Tr(\lambda\beta), \ \ldots, \ Tr(\lambda\beta^{n-1}) \big) \ , \ \lambda \in \mathbf{F} \ .$$

The code C is said to be an irreducible cyclic code with parameters $[n, m']$ over $\mathbf{k}$ (it is defined up to equivalence).

Example 3.34 Let C be an irreducible binary cyclic code of length $n = 23$; since the splitting field of $X^{23} - 1$ is $GF(2^{11})$, the code C has parameters $[23, 11]$. The 2-cyclotomic cosets modulo 23 are $\{0\}$,

$$\{ \ 1, \ 2, \ 4, \ 8, \ 16, \ 9, \ 18, \ 13, \ 3, \ 6, \ 12 \ \}, \text{ and}$$
$$\{ \ 5, \ 10, \ 20, \ 17, \ 11, \ 22, \ 21, \ 19, \ 15, \ 7, \ 14 \ \} \ .$$

Taking $\{0\} \cup cl(1)$ as the defining set of C, the MS polynomial is $Tr(\lambda X)$, $\lambda \in GF(2^{11})$. Note that $cl(1)$ is the set of the quadratic residues in the finite field of order 23. According to Definition 2.10, C is the $[23, 11, 8]$ quadratic residue code. It is the subcode of codewords of even weights of the $[23, 12, 7]$ Golay code. Golay codes are extensively studied in Chapter 1; see in particular Example 6.9 in Chapter 1 for the determination of the minimum distance.

It is important to remember that any $[n, m']$ irreducible cyclic code over $GF(q)$ is isomorphic to the finite field $GF(q^{m'})$; although this correspondence has no connection with the Hamming weight, it places irreducible codes at the center of some work on finite fields. More generally the research on the weight enumerator of irreducible cyclic codes remains important because of the number of fundamental problems which are concerned with finite fields – see for instance the links with the diagonal equations in Section 2.3.

The most significant work is due to McEliece et al. who pointed out the existence of a close connection between irreducible cyclic codes and Gauss sums over finite fields [14, 106, 108]. The main result, which is obtained by means of a famous theorem of Davenport and Hasse, follows:

> *For any fixed prime p and for any positive integer k prime to p, denote by m the multiplicative order of p modulo k. Define the infinite sequence of irreducible cyclic codes C_j with parameters*
>
> $$[n_j, mj] \ , \quad n_j = (p^{mj} - 1)/k \ , \quad j \geq 1, \ \textit{on GF(p)} \ . \qquad (45)$$
>
> *Then the calculation of the corresponding sequence of weight enumerators is reduced to the single calculation of the weight enumerator of C_1.*

This work was inspired by the study of irreducible binary codes, due to Delsarte and Gœthals [63], in which the computation of the sequence of weight enumerators is obtained simply by multiplying (iteratively) the vector of weights by a corresponding circulant matrix. The main result in [63] is in the description of a class of irreducible binary codes in which only two weights occur. This is generalized in [14] leading to the conjecture that *any two-weight cyclic code is irreducible.* Little is known about irreducible cyclic codes with three weights; see [15] and recent results in[95].

Many numerical results can be found in the papers previously quoted and in [110].

Henceforth the "numerical" problem is to determine the weight enumerator of one code for each sequence (45). From a theoretical point of view, the study of any specific class is of great interest and one can say that few general results have been obtained. The first reference is the work of Helleseth et al. on an infinite class of irreducible cyclic codes with fixed block length [79]. As an example of an interesting construction, the connection with product codes is explained in [70].

The most recent result is due to LANGEVIN and ZANOTTI who have characterized a class of irreducible codes with *balanced weight distribution* – i.e. such that there is the same number of codewords for any non zero weight of the code. A description is given in [96] and [152]. Note that the number of nonzero weights must divide $p-1$, implying that there are no such binary codes except the simplex code.

On the other hand consider the class of binary irreducible codes $C^{(m)}$ of length $n = 2^m + 1$ and dimension $2m$. Clearly $2^m + 1 = (2^{2m} - 1)/(2^m - 1)$ where m is the order of 2 modulo $2^m - 1$. Then $C^{(m)}$ is the second code of the sequence of irreducible cyclic codes $C_t^{(m)}$ with parameters $[n_t, mt]$ where

$$n_t = \frac{2^{mt} - 1}{2^m - 1} = \frac{(2^m - 1)(2^{m(t-1)} + \cdots + 2^m + 1)}{2^m - 1} = (2^{m(t-1)} + \cdots + 2^m + 1) \ .$$

We give in Table 9 the weight enumerators of the codes $C^{(m)}$ for $5 \leq m \leq 10$.

A relationship between the weight enumerators of the code $C^{(m)}$ and of the Melas code of length $2^m - 1$ was established by TIERSMA in [125]. On the other hand, LACHAUD and WOLFMANN proved in [94] that the weights of the non zero words of $C^{(m)}$ are all the even integers w such that

$$\frac{2^m + 1}{2} - 2^{m/2} \leq w \leq \frac{2^m + 1}{2} + 2^{m/2} \ .$$

This description was obtained by giving an explanation of the links between the weights of Melas codes and some results on elliptic curves and Kloosterman sums over $GF(2^m)$. The problem of the complete determination of the weight enumerator of the Melas code remains open; any result on the number of words of a given weight could apply to the problem of the values of Kloosterman sums. The ternary Melas codes were studied in [147].

We conclude this section with an application of Theorem 3.20 to the divisibility of irreducible cyclic codes. Note that although we treat codes with the most simple set of non zeros, we can only improve the algorithm for computing divisibility. It is generally difficult to determine divisibility of a given infinite class of cyclic codes. One can see the next proposition as an illustration of this general open problem: *find a precise formula for divisibility of some class of cyclic codes.*

Proposition 3.35 *Let C be an $[n, m]$ irreducible cyclic code over $GF(p)$ with $n\mu = p^m - 1$. Set $\tau_j = lcm\,(wt_p(jn), p-1)$, $1 \leq j \leq \mu$. Define*

$$\tau = min \ \{ \ \tau_j \mid 1 \leq j \leq \mu \ \} \quad \textit{and} \quad \ell = \frac{\tau}{p-1} - 1 \ .$$

n=9	w	2	4	6								
m=3	a_w	9	27	27								
n= 17	w	6	8	10	12							
m=4	a_w	68	85	68	34							
n=33	w	12	14	16	18	20	22					
m=5	a_w	165	165	165	330	165	33					
n=65	w	26	28	30	32	34	36	38	40			
m=6	a_w	390	455	780	780	390	585	520	195			
n=129	w	54	56	58	60	62	64	66	68	70	72	74
m=7	a_w	903	903	1032	2709	903	1806	2709	903	1806	1806	903
n=257	w	114	116	118	120	122	124	126	128	130	132	134
m=8	a_w	2056	4112	2056	4626	6168	4112	8224	4112	4112	5140	4122
	w	136	138	140	142	144						
	a_w	4112	4112	5140	2056	1285						

n= 513	w	234	236	238	240	242	244	246	248	250
m=9	a_w	1539	4617	9234	18468	9234	4617	13851	13851	13851
	w	252	254	256	258	260	262	264	266	270
	a_w	18468	9747	9234	23085	13851	9234	23085	9234	10773
	w	272	274	276	278					
	a_w	23085	4617	9234	4617					
n= 1025	w	482	484	486	488	490	492	494	496	498
m= 10	a_w	12300	11275	30750	20500	30750	41000	41000	20500	41000
	w	500	502	504	506	508	510	512	514	516
	a_w	61500	20500	46125	41000	20500	41000	61500	30750	41000
	w	518	520	522	524	526	528	530	532	534
	a_w	51250	46125	51250	20500	20500	41000	51250	35875	20500
	w	536	538	540	542	544				
	a_w	20500	20500	30750	20500	5125				

Table 9: Weight enumerators of the irreducible binary cyclic codes of length $n = 2^m + 1$ and dimension $2m$, $4 \leq m \leq 10$ (see §3.4.3); a_w denotes the number of codewords of weight w.

Then C is p^{ℓ}-divisible and not $p^{\ell+1}$-divisible.

Proof: Let $\sum_{i=0}^{m-1} \nu_i p^i$ be the p-ary expansion of n; recall that $wt_p(n)$ is the integer sum $\sum_{i=0}^{m-1} \nu_i$, called the p-weight of n. Let U be the set of those $s \in [0, n-1]$ which are not in the defining set of C. According to Definition 3.33, we assume that $U = cl(-1)$, the p-cyclotomic coset of -1 modulo n. In accordance with Theorem 3.20, we have to determine the smallest integer r divisible by $p-1$ such that r elements of U, say $\{u_1, \ldots,\ u_r\}$, satisfy $\sum_{i=0}^{r} u_i = 0$ modulo n.

Set $r = \sum_{i=0}^{m-1} r_i$, meaning that the element $-p^i$ occurs r_i times – i.e. r_i elements of $\{u_1, \ldots,\ u_r\}$ are equal to $-p^i$. We know from Theorem 3.20 that $r_i \leq p-1$, for all i. Set $I_r = \sum_{i=0}^{m-1} r_i p^i$. Then we must have $I_r \equiv 0$ modulo n.

Clearly $I_r \equiv 0$ is satisfied for any r such that $I_r = jn$, $1 \leq j \leq \mu$. In this case r is exactly the p-weight of jn. We consider those r which are divisible by $p-1$ only. Then the smallest available r is equal to the smallest value of $lcm\,(wt_p(nj), p-1)$ and ℓ is determined.
♦

3.5 Automorphism groups of cyclic codes

Chapter(Huffman) deals with the general problem of automorphism groups of codes. We want to mention recent results on cyclic codes and briefly discuss open problems only.

Huffman has recently studied the automorphism groups of the extended generalized quadratic residue codes. He gave the full automorphism groups as groups of semi-affine transformations [80]. On the other hand the permutation groups of affine-invariant codes were characterized by Berger and Charpin [18] [21]. Berger proved later that the automorphism group is easily deduced [17]. All these results can be used now in other contexts, for example, the determination of the automorphism group of codes constructed from other codes such as repeated-root cyclic codes or concatenated codes. Another application could be the study of *non linear cyclic codes.* We will conclude this section with an example showing how to construct non linear affine-invariant codes.

The general problem of determining the automorphism group of any cyclic or extended cyclic code is a difficult problem. There is probably no general answer and the best way seems to be the study of special classes. One can mention first the irreducible cyclic codes (see a recent result on a special subclass in [153]). More generally there are no results on non primitive codes.

However, the results of [21] suggest the conjecture that the permutation group of any cyclic code will be generally small, i.e. the group $\mathcal{G}$ generated by the shift and some Frobenius mapping depending on the alphabet field. Indeed, even when the extended code is affine-invariant, it appears that many cyclic codes have $\mathcal{G}$ as permutation group. According to [21, Theorem 6], one can conjecture that, generally, cyclic codes of length $p^m - 1$, m prime, over $GF(p)$, either have $\mathcal{G}$ as automorphism group or are equivalent to a p-ary Reed-Muller code; on the other hand, interesting exceptions might appear.

More is known about equivalent cyclic codes. There is a general necessary and sufficient condition under which two cyclic codes could be equivalent (see Theorem 5.22 in Chapter 1). In particular when the length is a prime number, two cyclic codes can be equivalent by a multiplier only. The inequivalence of affine-invariant codes is now established; two affine-invariant codes cannot be equivalent unless under the Frobenius mapping [17].

Example 3.36 *It is very easy to construct non linear affine-invariant codes.* Our notation is that of Section 2.4; let the ambient space be $\mathcal{A} = \mathbf{k}[\{\mathbf{F}, +\}]$ where $\mathbf{k} = GF(p)$. Consider a coset of $\mathcal{P}^r$, the rth power of the radical, of the form

$$\mathrm{x} + \mathcal{P}^r \ , \quad \mathrm{x} \in \mathcal{P}^{r-1} \setminus \mathcal{P}^r. \tag{46}$$

Let us define the (generally) non linear code

$$C = \bigcup_{0 \le j \le n-1} sh_j(\mathrm{x}) + \mathcal{P}^r$$

where $sh_j(\mathrm{x})$ is the j-shift of x. For clarity, we denote by α a primitive root of $\mathbf{F}$ and consider the j-shift as multiplication by α^j in $\mathbf{F}$, the support field. We are going to prove that C *is invariant under the affine permutations* $\sigma_{u,v}$.

Let $\mathrm{z} \in C$, $\mathrm{z} = \mathrm{y} + \mathrm{y}'$, $\mathrm{y}' \in \mathcal{P}^r$ and $\mathrm{y} = sh_j(\mathrm{x})$ for some j. Recall that, according to (13),

$$\sigma_{u,v}(\mathrm{z}) = \sum_{g \in \mathbf{F}} z_g X^{ug+v} = \sum_{g \in \mathbf{F}} y_g X^{ug+v} + \sum_{g \in \mathbf{F}} y'_g X^{ug+v} \ .$$

We have $\sigma_{u,v}(\mathrm{z}) = \sigma_{u,v}(\mathrm{y}) + \sigma_{u,v}(\mathrm{y}')$. As the code $\mathcal{P}^r$ is affine-invariant, $\sigma_{u,v}(\mathrm{y}') \in \mathcal{P}^r$. Moreover, by construction, $\sigma_{u,v}(\mathrm{y}) = \sigma_{au,v}(\mathrm{x})$ where $a = \alpha^j$;

this shows that $\sigma_{u,0}(\mathrm{y})$ is a k-shift of x, with $u = \alpha^i$ and $k = i + j$. So we only have to prove that $\sigma_{1,v}(\mathrm{x})$ is in C. Observe that

$$\sigma_{1,v}(\mathrm{x}) = X^v\mathrm{x} = (X^v - 1)\mathrm{x} + \mathrm{x}$$

where $(X^v-1)\mathrm{x} \in \mathcal{P}^r$ since $(X^v-1) \in \mathcal{P}$ and $\mathrm{x} \in \mathcal{P}^{r-1}$. Hence $\sigma_{1,v}(\mathrm{x})$ is in the coset $\mathrm{x} + \mathcal{P}^r$, completing the proof. Note that we mainly used the following property: any coset of the form (46) is invariant under any translation. Recall that $\mathcal{P}^r$ is the p-ary Reed-Muller code of order $m(p-1) - r$.

3.6 Are all cyclic codes asymptotically bad ?

Whether or not there exist good linear codes which are also cyclic remains an open problem. The most recent result is due to Castagnoli et al. who reduced the problem, by proving that repeated-root cyclic codes cannot be asymptotically better than simple-root cyclic codes [46].

It has been known for a long time that BCH codes are asymptitocally bad (see Chapter 1, Theorem 7.7). Furthermore Kasami proved that any family of cyclic codes is bad if it has the property that the extended codes are affine-invariant – the proof given in [86] for binary codes can be easily generalized.

On the other hand, Berlekamp and Justesen have shown that certain concatenated codes are cyclic [24] thus obtaining an improved class of long binary cyclic codes. Many researchers consider that quadratic residues codes could be asymptotically good. This open problem is connected with the necessity of finding a good bound for the minimum distance of the QR codes.

4 Related problems.

In this section, we examine research problems in coding theory which are connected with the study of cyclic codes. Actually it is a large topic in which we have chosen three subjects, which seem currently of interest: cryptography, alternant codes and non linear codes.

Concerning cryptography, we recall the involvement of Reed-Muller codes in the description of some cryptographic primitives. More generally, the primitive binary cyclic codes are then implicated, as we will show by giving a specific example.

The class of *alternant codes* is closely related with generalized Reed-Solomon codes and contains BCH codes and Goppa codes. The class of Goppa codes includes the narrow-sense BCH codes (see [111, chapter 12]). The aim is to present basic elements about the links between Goppa codes and BCH codes, introducing some open problems on Goppa codes. Note that Goppa codes are proposed, as public-key, in the McEliece cryptosystem.

The last subject can be viewed as an example of the involvement of cyclic codes, and of their cosets, in the construction of other interesting codes. We treat the most famous non linear codes, the Preparata and Kerdock codes. We give an original result, a new proof of the formal duality of these codes based on the description of BACKER and on recent results about cosets of 2-error-correcting BCH codes. The use of the operations in the field algebra of primitive extended codes provides new properties and might suggest other constructions.

4.1 Some problems in cryptography

The connections between coding theory and cryptography are discussed in Chapter(Van-Tilborg), a large part of which is devoted to the use of error-correcting codes in some cryptosystems. The most famous is the McEliece public-key cryptosystem which uses binary Goppa codes. A priori cyclic codes are not designed for such cryptosystems because they are considered as easily recognizable codes. There are generally few cyclic codes for a given length and these codes have a "rich" structure (note that the class of repeated-root cyclic codes is not so simple). However one can mention that to determine if a given code is cyclic or not remains a difficult problem.

Many problems in cryptography lead to general problems in coding theory. For instance the *generalized Hamming weight* is mentioned in Chapter(Van-Tilborg) (see in Chapter 1, Section 3: *the weight hierarchy of a code*). The relation between *minimal codewords* and *secret sharing* is another example [116][117].

Cyclic codes are related to the study and the construction of cryptographic primitives, mainly through Reed-Muller codes because of the large field of applications of boolean functions and sequences in cryptography. There are a lot of recent papers about these applications; many are to be found in the proceedings of the conferences EUROCRYPT and CRYPTO.

It is well-known that any property of RM codes is a property of boolean functions. RM codes provide a natural way to quantify the *degree*, the *nonlinearity*, the *correlation-immunity* or the *propagation criterion* of a boolean function (see for instance [36][37][42][43][117][128]). Note that maximum nonlinearity coincides with the covering radius of the RM code of order one. We have here a strong connection with famous open problems: the covering radius is not known for the lengths 2^m, $m \geq 7$ and m odd; for m even, the maximal cosets corresponding to the *bent functions* are not yet classified – the most recent result is due to CARLET and GUILLOT [45].

In this context, it is clear that binary primitive cyclic codes could appear in some specific application. We want to illustrate our purpose by such an example which can be seen as an extension of Section 3.4.2, because cyclic codes with two zeros are involved. *We want to emphasize that in a very recent application the "old" work of* KASAMI [87] *is an important reference.*

Two cryptanalysis methods have been introduced in the literature devoted to DES-like cryptosystems, the *differential cryptanalysis* [27](1991) and the *linear cryptanalysis* [118](1994). CHABAUD and VAUDENAY showed later that these methods are basically linked; they deduce the definition of those classes of functions which are optimally resistant to both attacks [48]. The functions that oppose an optimum resistance to differential attacks are said to be *almost perfect nonlinear* (APN) functions. On the other hand the functions that oppose an optimum resistance to linear attacks are said to be *almost bent* (AB) functions. Any AB function is APN. We will describe such functions from a coding point of view.

Recall that $n = 2^m - 1$, $\mathbf{F}$ is the field of order 2^m, $\mathbf{k}$ is the field of order 2 and α is a primitive nth root of unity. From now on, m is odd and we consider a function F from $\mathbf{F}$ to $\mathbf{F}$ as a polynomial on $\mathbf{F}$ such that $F(0) = 0$.

Definition 4.1 *The function F is said to be APN if and only if all the equations*

$$F(x) \ + \ F(x+\gamma) \ = \ \beta \quad , \quad \gamma \in \mathbf{F} \ , \ \gamma \neq 0 \ , \ \beta \in \mathbf{F} \ , \tag{47}$$

have at most two solutions (that is one solution modulo γ). The function F is said to be AB if and only if the value of

$$\mu_F(\gamma,\beta) = \sum_{x\in\mathbf{F}} (-1)^{\beta\cdot F(x)+\gamma\cdot x} \tag{48}$$

is equal either to 0 *or to* $\pm 2^{\frac{m+1}{2}}$, *for any* γ *and* β *in* $\mathbf{F}$, $\beta \neq 0$. *Note that* $x \cdot y$ *is the dot product with respect to any chosen basis of the vector-space* $\{\mathbf{F}, +\}$.

Theorem 4.2 *Let* F *be a function on* $\mathbf{F}$ *such that* $F(0) = 0$. *Let us denote by* C_F *the linear binary code of length* n *defined by its parity check matrix*

$$\mathcal{H}_F = \left[\begin{array}{ccccc} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ F(1) & F(\alpha) & F(\alpha^2) & \dots & F(\alpha^{n-1}) \end{array} \right]$$

where each entry is viewed as a vector of $\mathbf{k}^m$. *The dual code is denoted by* $(C_F)^\perp$.
Then we have:

(i) the function F *is APN if and only if the code* C_F *has minimum distance five,*

(ii) the function F *is AB if and only if the weights of the non zero codewords of the code* $(C_F)^\perp$ *form the following set*

$$W = \{ \ 2^{m-1}, \ 2^{m-1} \pm 2^{(m-1)/2} \ \} \ .$$

Proof: Let u $= (u_0, \dots, u_{n-1})$ be a codeword – i.e. a vector of $\mathbf{k}^n$. By definition u $\in C_F$ if and only if it satisfies

$$\sum_{i=0}^{n-1} u_i \alpha^i \ = \ 0 \quad \text{and} \quad \sum_{i=0}^{n-1} u_i F(\alpha^i) \ = \ 0 \ . \tag{49}$$

It is clear that the minimum weight of C_F is at least 3 because we cannot have $\alpha^i = \alpha^j$ for $i \neq j$. The equation (47) can be rewritten as follows:

$$x \ + \ y \ = \ \gamma \qquad \text{and} \qquad F(x) \ + \ F(y) \ = \ \beta \ , \tag{50}$$

for any $\gamma \neq 0$ and β. Suppose that there exist two distinct pairs (x, y) and (x', y') which satisfy (50). Of course "distinct" means that we have here four distinct elements of $\mathbf{F}$. The existence of four such elements, for some γ and β, is equivalent to the existence of four elements satisfying

$$x \ + \ y \ + \ x' \ + \ y' \ = \ 0 \qquad \text{and} \qquad F(x) \ + \ F(y) \ + \ F(x') \ + \ F(y') \ = \ 0 \ .$$

In accordance with (49), it is equivalent to say that the code C_F has at least one codeword of weight three or four – the weight can be three if 0 is in the set $\{x,\ y,\ x',\ y'\}$. Note that the minimum distance cannot be more than 5, by using the argument of the proof of Theorem 3.25 (i): the non-existence of a $[2^m-1,k,6]$ linear code such that $k \geq 2^m-1-2m$. So we have proved (i).

Now set $f(x) = \beta \cdot F(x) + \gamma \cdot x$. Considering elements of $\mathbf{F}$ as vectors of $\mathbf{k}^m$, the function f is actually a linear combination of some rows of $\mathcal{H}_F$. Hence the numbers

$$\lambda_{\beta,\gamma} = \text{card } \{\ \alpha^i \mid f(\alpha^i) = 1\ \}$$

are the weights of the code $(C_F)^\perp$. But $\mu_F(\gamma,\beta) = 0$ means $\lambda_{\beta,\gamma} = 2^{m-1}$ and $\mu_F(\gamma,\beta) = \pm 2^{\frac{m+1}{2}}$ means

$$2\lambda_{\beta,\gamma} = 2^m \pm 2^{\frac{m+1}{2}} \qquad \text{— i.e.} \quad \lambda_{\beta,\gamma} = 2^{m-1} \pm 2^{\frac{m-1}{2}}\ .$$

According to the definition of the property AB (see (48)), we have proved (ii). Note that in (48) the values of $\mu_F(\gamma,0)$ are not considered. For our point of view they correspond to the codewords of $(C_F)^\perp$ which are generated by the first m rows of $\mathcal{H}_F$, that is the codewords of the *simplex code* which have weight 2^{m-1}.

♦

Our notation is that of Theorem 4.2.

Corollary 4.3 *If the function F is AB, then the dimension of the code $(C_F)^\perp$ equals $2m$ – i.e. the code C_F has dimension 2^m-2m-1.*

Proof: By definition, the dimension of $(C_F)^\perp$ is at most $2m$. Suppose that it is stricly less than $2m$. This means that there is at least one $\beta \neq 0$ and one γ such that $\beta \cdot F(x) + \gamma \cdot x = 0$ for any $x \in \mathbf{F}$. So $\mu_F(\gamma,\beta)$ equals 2^m, a contradiction.

♦

Corollary 4.4 *Assume that the function F is defined as follows*

$$F(x) = x^r\ ,\quad \text{card } \{\ r,\ 2r,\ \ldots, 2^{m-1}r \ mod\ n\ \} = m\ .$$

Denote by C_r the binary cyclic code of length n whose zeros are α, α^r and their conjugates.

Then F is APN if and only if C_r has minimum distance five. The function F is AB if and only if $(C_r)^\perp$ has only three nonzero weights, 2^{m-1} and $2^{m-1} \pm 2^{(m-1)/2}$. In this case the weight enumerator of $(C_r)^\perp$ is exactly the weight enumerator of the dual of the 2-error-correcting BCH code — given in Theorem 3.32.

Proof: By definition $\mathcal{H}_F$ is exactly the parity-check matrix of the binary cyclic code C_r. Note that the 2-cyclotomic coset of r is assumed to have cardinality m because, according to Corollary 4.3, this is a necessary condition if we want to construct AB functions.

♦

It is easy to see that the code C_F always contains a subcode which is a cyclic code. This is the code whose zeros are $\{\alpha, \alpha^{i_1}, \dots, \alpha^{i_\ell}\}$ when the polynomial form of $F(x)$ is

$$F(x) = \sum_{j=1}^{\ell} \lambda_j x^{i_j} \ , \ \lambda_j \in \mathbf{F} \setminus \{0\} \ .$$

More generally, the connections between APN/AB functions, bent functions and codes were recently studied in [44].

Differential and linear attacks are now “classical”, providing theoretical criterions for the security of DES-like ciphers. For instance, to replace the S-boxes used in DES with another function which resists both differential and linear cryptanalysis is a problem which is currently under discussion. This gives renewed interest to the properties of functions $x \longmapsto x^k$ on $\mathbf{F}$ – i.e. of cyclic codes with two zeros. Therefore, there is much current work related to these properties which will certainly lead to new results. The paper of Dobbertin [66] is such an example in which it is proved that the function $x \longmapsto x^k$, for $k = 2^t + 3$, is APN. Then the author has partially proved the Welsh conjecture (see comments in Section 3.4.2).

For applications in cryptography the functions which are one-to-one are of most interest. So APN permutations, even when they are not AB, are interesting. It seems that the main problem is to find codes C_F with “few” codewords of weight 4. This is connected with the problem of the weight enumerators of cosets of the codes C_F, in particular when C_F is a primitive cyclic code with two zeros. Note that the covering radius of codes like C_F is generally not known.

4.2 Cyclic codes and Goppa codes

The aim of this section is to give a basic account about the connections between Goppa codes and cyclic codes.

Goppa codes, which are often said to be *close to random codes*, can be viewed in the ambient space of primitive cyclic (or extended cyclic) codes. To study some properties of cyclic codes through Goppa codes is, in a certain sense, an overview. For instance, codewords of Goppa codes can be defined in several ways including MS-polynomials and locator polynomials – tools which were developed in the previous sections for cyclic codes.

On the other hand there is a *famous open problem* which is to recover the original structure of any Goppa code when only a permuted generator matrix is given. This is a possible way for breaking the McEliece public-key cryptosystem [107] but could be used in some other applications. Here knowledge of properties of cyclic codes, or of tools designed to the study of cyclic codes, might be useful.

The automorphism groups of Goppa codes are not known. It is conjectured that the group of such a code is generally trivial; furthermore one can say that there are few Goppa codes, extended or not, which are cyclic. As is explained in Chapter(Assmus-Key) *a code can be cyclic in many ways.* One must specify explicitly the cyclic structure we are referring to before comparing a given code to a cyclic code. That is particularly true for Goppa codes. It is easy to treat the cyclicity when the support is fixed, meaning that we consider the code in the ambient space $\mathbf{k}[\{G^*, \times\}]$, denoted by $\mathcal{M}$ in Section 2.2; the "shift" is precisely the multiplication of the cyclic group G^*. Otherwise the problem becomes the general problem of finding the automorphism group of Goppa codes.

We first recall that, with the above restricted point of view, it is easy to show that cyclic Goppa codes are BCH codes. We next point out that, however, there is a large class of *quasi-cyclic Goppa codes.* To conclude we explain the link between the class of Goppa codes and the minimum weight codewords of BCH codes by giving some applications of Corollary 3.13 (in the binary case).

We consider here *classical Goppa codes* in the sense of [74] (see also [111, Chapter 12] or [139, Chapter 8]). As previously the finite field of order q, $q = p^r$ and p a prime, is denoted by $\mathbf{k}$; $\mathbf{k}$ is the alphabet field. The support field is denoted by $\mathbf{F}$; it is an extension field of $\mathbf{k}$ of order p^m, r dividing

m – or $q^{m'}$, $m' = m/r$. Considering Goppa codes, the field $\mathbf{F}$ is called the *full support field*, because for such a code the support can be, with some restrictions, any subset of $\mathbf{F}$.

Definition 4.5 *Let $g(z)$ be a monic polynomial of degree t over $\mathbf{F}$. Let $n \geq 2$ and $L = \{\alpha_1, \ \ldots, \ \alpha_n\}$ be a set of n distinct elements of $\mathbf{F}$. Moreover $g(z)$ and L are such that*

$$g(\alpha_i) \neq 0 \ , \ 1 \leq i \leq n \ .$$

The Goppa code $\Gamma(L, g)$, of length n over $\mathbf{k}$, is the set of codewords c, *i.e. vectors $(c_1, \ \ldots, \ c_n)$ in $\mathbf{k}^n$, satisfying*

$$R_{\mathrm{c}}(z) = \sum_{i=1}^{n} \frac{c_i}{z - \alpha_i} \ \equiv \ 0 \pmod{g(z)} \ .$$

Before studying some properties of cyclicity, we want to recall that the dimension and the minimum distance of Goppa codes are not known. In both cases, only a bound is known which is generally considered as a good bound; note that the bound on the dimension is reached for an infinite class of Goppa codes of small dimension [138]. These bounds can be easily obtained from a parity check matrix of the code (as H in the proof of Proposition 4.7).

Proposition 4.6 *Let $\Gamma(L, g)$ be a Goppa code defined by Definition 4.5; let t be the degree of $g(z)$. Then the dimension k and the minimum distance d of $\Gamma(L, g)$ satisfy:*

$$k \geq n - m't \quad \text{and} \quad d \geq t + 1 \ .$$

Proposition 4.7 *If $g(z) = z^t$ the Goppa code $\Gamma(L, g)$ can be identified to a subcode of the narrow-sense BCH code of designed distance t and length $q^{m'} - 1$ over $\mathbf{k}$.*

Proof: The following matrix, where each entry is a column vector of length m' from $\mathbf{k}$, is a parity check matrix of the code $\Gamma(L, g)$.

$$H = \begin{bmatrix} g(\alpha_1)^{-1} & \ldots & g(\alpha_n)^{-1} \\ \alpha_1 g(\alpha_1)^{-1} & \ldots & \alpha_n g(\alpha_n)^{-1} \\ \ldots & \ldots & \ldots \\ (\alpha_1)^{t-1} g(\alpha_1)^{-1} & \ldots & (\alpha_n)^{t-1} g(\alpha_n)^{-1} \end{bmatrix}$$

Assume that $g(z) = z^t$. For clarity, let $\alpha_i^{-1} = \beta_i$, for all i. By replacing in H, we obtain

$$H = \left[\begin{array}{lll} \alpha_1^{-t} & \dots & \alpha_n^{-t} \\ \alpha_1^{-(t-1)} & \dots & \alpha_n^{-(t-1)} \\ \dots & \dots & \dots \\ \alpha_1^{-1} & \dots & \alpha_n^{-1} \end{array}\right] = \left[\begin{array}{lll} \beta_1^{t} & \dots & \beta_n^{t} \\ \beta_1^{(t-1)} & \dots & \beta_n^{(t-1)} \\ \dots & \dots & \dots \\ \beta_1 & \dots & \beta_n \end{array}\right]$$

We recognize that H consists of some columns of the parity check matrix of the narrow sense BCH code of designed distance t on $\mathbf{k}$ (see Chapter 1, Section 5). So $\Gamma(L, g)$ is the subcode of this code containing all codewords whose support is contained in L.

♦

Now we consider Goppa codes of length n, where n divides $q^{m'} - 1$. The next theorem is based on a strong restriction: Goppa codes are viewed in the ambient space of cyclic codes of length n over $\mathbf{k}$ and "cyclic" means that the code is invariant under the shift on the support L. One can then prove that any Goppa code which is cyclic, in the sense above, is a BCH code.

Lemma 4.8 *Suppose that $L = \{\ 1,\ \beta,\ \dots,\ \beta^{n-1}\ \}$ where β is a primitive nth root of unity in $\mathbf{F}$. Then the code $\Gamma(L, g)$ consists of the codewords* c *whose MS polynomial satisfies:*

$$z^{n-1}\ M_{\rm c}(z) \quad (\text{mod } z^n - 1)\ \equiv\ 0 \quad (\text{mod } g(z))\ .$$

Moreover if c *satisfies $\sum_{i=1}^n c_i = 0$ then $zg(z)$ divides $M_{\rm c}(z)$.*

Proof: We simply generalize the proof of van Lint [139, p.113]. We denote by $Q(z)$ the polynomial $z^{n-1}\ M_{\rm c}(z)$. Let $\mathrm{c} = (c_1,\ \dots,\ c_n)$ be a codeword of length n on $\mathbf{k}$. Consider the polynomial of $\mathbf{F}[z]$:

$$P(z) = \frac{z^n - 1}{n} \sum_{\ell=0}^{n-1} \frac{M_{\rm c}(\beta^\ell)}{z - \beta^\ell} = \frac{1}{n} \sum_{\ell=0}^{n-1} M_{\rm c}(\beta^\ell) \prod_{i,\ i \neq \ell} (z - \beta^i)\ .$$

Note that $(n, p) = 1$, $gcd(z^n - 1, g(z)) = 1$ and $P(z)$ has degree less than or equal to $n - 1$. By differentiating $z^n - 1$, it is easy to check that

$$\prod_{i,\ i \neq \ell} (\beta^\ell - \beta^i) = n\beta^{-\ell}\ .$$

Thus we have for any j, $0 \leq j \leq n-1$:

$$P(\beta^j) = \frac{M_{\rm c}(\beta^j)}{n} \prod_{i,\ i\neq j} (\beta^j - \beta^i) = M_{\rm c}(\beta^j)\ \beta^{-j}\ .$$

Since $P(z)$ takes the same values as $Q(z)$ on the group of nth roots of unity, then $Q(z) = P(z)$. Furthermore we obtain

$$P(z) = \frac{z^n - 1}{n} \sum_{i=0}^{n-1} \frac{n\ c_i}{z - \beta^i} = (z^n - 1)\ R_{\rm c}(z)$$

because $M_{\rm c}(\beta^i) = nc_i$ by applying the inverse formula (4) (see Section 2.2). According to Definition 4.5, one deduces that c is in $\Gamma(L, g)$ if and only if $g(z)$ divides $Q(z)$, proving the first part of the theorem. Now, by definition of $M_{\rm c}(z)$, we have

$$Q(z) = z^{n-1} M_{\rm c}(z) = \sum_{s=0}^{n-1} \rho_{n-s}({\rm c})\ z^{s-1} \qquad (\text{mod } z^n - 1)\ ,$$

where $\rho_s({\rm c}) = \sum_{i=1}^{n} c_i \beta^{s(i-1)}$ (see (3) and (1)). This shows that $zQ(z)$ is divisible by z if and only if $\rho_n({\rm c}) = \sum_{i=1}^{n} c_i = 0$. When this property holds, we can conclude that $M_{\rm c}(z)/z$ is a multiple of $g(z)$, completing the proof. ♦

Theorem 4.9 *Assume that $L = \{\ 1,\ \beta,\ \ldots,\ \beta^{n-1}\ \}$, a cyclic subgroup of* $\mathbf{F}$ *where β is a primitive nth root of unity. If the code $\Gamma(L, g)$ is "cyclic", i.e. is invariant under the permutation $\beta^i \longmapsto \beta^{i+1}$ on L, then $g(z) = z^t$, for some t. So $\Gamma(L, g)$ is a BCH code of length n and designed distance t over* $\mathbf{k}$.

Proof: Suppose that $\Gamma(L, g)$ is cyclic. By definition of cyclic codes we can choose ${\rm c} \in \Gamma(L, g)$ such that $\rho_n({\rm c}) = 0$. Moreover, according to Lemma 4.8, $zg(z)$ divides $M_{\rm c}(z)$.

Suppose that $g(\gamma) = 0$ for some γ, $\gamma \neq 0$, belonging to some extension field of $\mathbf{k}$. Thus $M_{\rm c}(\gamma) = 0$. But the polynomials $M_{\rm c}(\beta^{-i} z)$, $0 \leq i \leq n-1$, are the MS polynomials of the shifts, say $sh_i({\rm c})$, of the codeword c (see Theorem 2.3). Since $sh_i({\rm c})$ is in $\Gamma(L, g)$ we have for all i:

$$M_{\rm c}(\beta^{-i}\gamma) = M_{sh_i({\rm c})}(\gamma) = 0$$

which contradicts the fact that $M_c(z)$ is a polynomial of degree strictly less than n. Hence $g(z)$ has no roots γ, unless $\gamma = 0$, meaning that $g(z) = z^t$ for some t. From Proposition 4.7, $\Gamma(L, g)$ is a BCH code, completing the proof. ♦

On the other hand, there is a large class of quasi-cyclic Goppa codes, i.e. Goppa codes $\Gamma(L, g)$ which are invariant under mutiplication by some element of $\mathbf{F}$. The class that we define below is not the more general one; we simply indicate the way of constructing such Goppa codes.

Proposition 4.10 *Recall that α denotes any primitive root of $\mathbf{F}$. Suppose that n divides $q^{m'} - 1$ and denote by β a primitive nth root of unity in $\mathbf{F}$. Let us define the Goppa code $\Gamma(L, g)$ such that $L = \{ \ \alpha^i \mid 0 \leq i \leq q^{m'} - 2 \ \}$ and $g(z)$ is a monic polynomial satisfying*

$$g(\beta z) = g(z) \ , \quad \textit{for any } z \ .$$

Then $\Gamma(L, g)$ is invariant under multiplication by β over L: $\Gamma(L, g)$ is quasi-cyclic.

Proof: Set $N = q^{m'} - 1$. From Lemma 4.8, $\Gamma(L, g)$ consists of those codewords c of $\mathbf{k}^N$ whose MS polynomial satisfies

$$z^{N-1} \ M_c(z) \quad (\text{mod } z^N - 1) \ \equiv \ 0 \quad (\text{mod } g(z)) \ .$$

From Theorem 2.3, $M_c(z/\beta)$ is the MS polynomial of the ν-shift of c where $\nu = N/n$ and $\beta = \alpha^\nu$. On the other hand, $g(\beta z) = g(z)$ means that the set of roots of $g(z)$ is invariant under the multiplication by β. Hence $g(z)$ divides $(z/\beta)^{N-1} \ M_c(z/\beta)$, implying that $g(z)$ divides

$$z^{N-1} \ M_c(z/\beta) = z^{N-1} \ M_{sh_\nu(c)}(z) \ .$$

So we conclude that the ν-shift of c is in $\Gamma(L, g)$; in other words, $\Gamma(L, g)$ is quasi-cyclic.
♦

Example 4.11 Our notation is as in Proposition 4.10. Let $\mathbf{F}'$ be an extension field of $\mathbf{F}$. Take

$$g(z) = z^n - \gamma \ , \quad \gamma \in \mathbf{F}' \setminus \mathbf{F} \ .$$

Obviously $g(\beta z) = \beta^n z^n - \gamma = g(z)$. So $\Gamma(L, g)$ is a quasi-cyclic code of length $N = q^{m'} - 1$ and dimension k, $k \geq N - m'n$.

From now on we will consider binary Goppa codes, i.e $\mathbf{k} = GF(2)$ and $\mathbf{F} = GF(2^m)$. Let $\Gamma(L, g)$ be a binary Goppa code of length n over $\mathbf{k}$. Any codeword c can be identified to its locator set $\{ \alpha_i \in L \mid c_i \neq 0 \}$. Assume that c has weight w, with $c_{i_1} = \cdots = c_{i_w} = 1$ and define

$$f_{\mathrm{c}}(z) = \prod_{j=1}^{w} (z - \alpha_{i_j}) \ . \tag{51}$$

By differentiating, we obtain

$$f'_{\mathrm{c}}(z) = \sum_{\ell=1}^{w} \prod_{\substack{j=1 \\ j \neq \ell}}^{w} (z - \alpha_{i_j}) \ .$$

This leads obviously to the following equality:

$$R_{\mathrm{c}}(z) = \sum_{i=1}^{n} \frac{c_i}{z - \alpha_i} \ = \frac{f'_{\mathrm{c}}(z)}{f_{\mathrm{c}}(z)} \ . \tag{52}$$

We conclude with the notation above:

Proposition 4.12 *Denote by $\widehat{g}(z)$ the lowest degree perfect square polynomial which is divisible by $g(z)$; let t be the degree of $g(z)$ and t' be the degree of $\widehat{g}(z)$.*

Then the codeword c *is in $\Gamma(L, g)$ if and only if $\widehat{g}(z)$ divides $f'_{\mathrm{c}}(z)$ and the minimum distance d of $\Gamma(L, g)$ is at least $t' + 1$. Moreover if the roots of $g(z)$ have multiplicity one then $g(z)^2$ divides $f'_{\mathrm{c}}(z)$ and $d \geq 2t + 1$.*

Proof: According to Definition 4.5, c is in $\Gamma(L, g)$ if and only if $R_{\mathrm{c}}(z) \equiv 0$ modulo $g(z)$. Since the roots of $f_{\mathrm{c}}(z)$ are of multiplicity one, $f_{\mathrm{c}}(z)$ and $f'_{\mathrm{c}}(z)$ have no common factors. Moreover, by definition, $g(z)$ and $f_{\mathrm{c}}(z)$ are relatively prime. So (52) means that $g(z)$ divides $R_{\mathrm{c}}(z)$ if and only if it divides $f'_{\mathrm{c}}(z)$.

As the characteristic is 2, $f'_{\mathrm{c}}(z)$ is a perfect square. Hence $g(z)$ divides $f'_{\mathrm{c}}(z)$ if and only if $\widehat{g}(z)$ divides $f'_{\mathrm{c}}(z)$. This provides a lower bound on the minimum distance of $\Gamma(L, g)$: since the degree of $f_{\mathrm{c}}(z)$ is at least $t' + 1$ then $d \geq t' + 1$. When all roots of $g(z)$ have multiplicity one, $g(z)^2$ divides $f'_{\mathrm{c}}(z)$, proving that the weight of c is at least $2t+1$.

♦

Denote by $B(\delta)$ the binary BCH code of length n and designed distance δ. We know the form of the locator polynomials of the codewords of $B(\delta)$ (see Corollary 3.13). So the preceding proposition leads us to this natural question: what is the intersection between $B(\delta)$ and $\Gamma(L,g)$, when δ is exactly the lower bound $t'+1$? The general problem is difficult; however, it is often easy to characterize codewords belonging to this intersection. We conclude this section by giving some results on such codewords of weight δ.

Proposition 4.13 *Recall that* $\mathbf{F} = GF(2^m)$*. Let* $g(z)$ *be any polynomial of degree* t *on* $\mathbf{F}[z]$ *whose roots have multiplicity one. Set*

$$g(z) = \sum_{i=0}^{t} \lambda_i z^i \ , \quad \lambda_t = 1 \ .$$

Consider the binary Goppa codes $\Gamma(L,g)$ *such that*

$$L = \mathbf{F} \setminus \{ \ \gamma \in \mathbf{F} \mid g(\gamma) = 0 \ \} \ .$$

The code $B(\delta)$*,* $\delta = 2t+1$*, is the narrow-sense binary BCH code of length* $2^m - 1$ *and designed distance* δ*.*

Suppose that there is a codeword x *of weight* δ *in* $B(\delta) \cap \Gamma(L,g)$*. Then the locator polynomial of* x*, say* $\sigma_{\mathrm{x}}(z)$*, is of the form:*

$$\sigma_{\mathrm{x}}(z) = z^{\delta} f_{\mathrm{x}}(z^{-1}) \qquad \textit{with} \qquad f_{\mathrm{x}}(z) = \xi + \sum_{i=0}^{t-1} \lambda_i z^{2i+1} + z^{\delta} \ , \qquad (53)$$

where ξ *is some element of* $\mathbf{F}$*.*

Conversely, if there exists a polynomial of the form (53) which splits in $\mathbf{F}$ *and whose roots have multiplicity one, then it defines a codeword of weight* δ *contained in* $B(\delta) \cap \Gamma(L,g)$ *– proving that the minimum distance of both codes is exactly* δ*.*

Proof: Suppose that there is a codeword x of weight δ in $B(\delta) \cap \Gamma(L,g)$. Since $\mathrm{x} \in B(\delta)$, the form of $\sigma_{\mathrm{x}}(z)$ is known from Corollary 3.13:

$$\sigma_{\mathrm{x}}(z) = 1 + \sum_{r=1}^{t} \sigma_{2r} z^{2r} + \sigma_{\delta} z^{\delta} \ . \qquad (54)$$

Let $\{ \alpha_j \mid 1 \leq j \leq \delta \}$ be the set of locators of x. We have, by definition,

$$\sigma_{\mathrm{x}}(z) = \prod_{j=1}^{\delta}(1 - \alpha_j z) = z^{\delta} \prod_{j=1}^{\delta}(z^{-1} - \alpha_j) = z^{\delta} f_{\mathrm{x}}(z^{-1})$$

(see (51)). Therefore

$$f_{\mathrm{x}}(z) = z^{\delta}\sigma_{\mathrm{x}}(z^{-1}) = z^{\delta} + \sum_{r=1}^{t} \sigma_{2r} z^{\delta-2r} + \sigma_{\delta} = z^{\delta} + \sum_{i=0}^{t-1} \sigma_{2(t-i)} z^{2i+1} + \sigma_{\delta} \ ,$$

where $i = t - r$, with $\delta = 2t + 1$. As $\mathrm{x} \in \Gamma(L, g)$, $g(z)^2$ divides $f'_{\mathrm{x}}(z)$ from Proposition 4.12. But these polynomials have the same degree. So we have

$$f'_{\mathrm{x}}(z) = z^{2t} + \sum_{i=0}^{t-1} \sigma_{2(t-i)} z^{2i} = g(z)^2 \ ,$$

implying $\sigma_{2(i-t)} = \lambda_i$, completing the proof of (53).

Conversely if $f_{\mathrm{x}}(z)$ is given by (53), for some x, then $g(z)$ divides $f'_{\mathrm{x}}(z)$ by definition. Moreover $f'_{\mathrm{x}}(z)$ and $f_{\mathrm{x}}(z)$ cannot have common factors implying that the locators of x are in L. Hence x is in $\Gamma(L, g)$ and its locator polynomial, $\sigma_{\mathrm{x}}(z)$, has the form (54), completing the proof.

♦

A consequence of these last propositions is that we can easily characterize the binary Goppa codes containing a given codeword. Therefore, if we know precisely a minimum weight codeword of some BCH code, say $B(\delta)$, then we can construct the unique Goppa code of minimum distance δ containing this codeword. We illustrate these properties by the next example.

Example 4.14 For clarity we treat codewords which are idempotents. We consider binary codes of length 2^8, i.e. $m = 8$ and $\mathbf{F} = GF(256)$; $\Gamma(L, g)$ is a binary Goppa code with $L = \mathbf{F}$.

Consider a product of two minimal polynomials of degree 8:

$$\begin{aligned} h(z) &= \left(z^8 + z^5 + z^4 + z^3 + z^2 + z + 1\right)\left(z^8 + z^7 + z^5 + z^4 + 1\right) \\ &= 1 + z + z^2 + z^3 + z^5 + z^7 + z^8 + z^{10} + z^{12} + z^{15} + z^{16} \ . \end{aligned}$$

Denote by x the codeword, of weight 16, whose locators are the roots of $h(z)$; so $f_{\mathrm{x}}(z) = h(z)$, where f_{x} is defined by (51). Now we compute the binary factors of $f'_{\mathrm{x}}(z)$:

$$f'_{\mathrm{x}}(z) = 1 + z^2 + z^4 + z^6 + z^{14} = \left(z^7 + z^3 + z^2 + z + 1\right)^2 \ .$$

Let $g(z) = z^7+z^3+z^2+z+1$. Since $g(z)$ is the only proper factor of $f'_{\mathrm{x}}(z)$, we can conclude that the code $\Gamma(L,g)$ is the only binary Goppa code of length 256 containing x. Note that the minimum distance of this code is at least 15.

On the other hand, take

$$f_{\mathrm{x}}(z) = \left(z^8+z^7+z^6+z^5+z^4+z^3+1\right)(z+1) = z^9+z^3+z+1$$

giving

$$f'_{\mathrm{x}}(z) = z^8+z^2+1 = \left(z^4+z+1\right)^2 \ .$$

According to (53) and (54), x is a codeword of weight 9 in the BCH code of length 255 and designed distance 9. The polynomial z^4+z+1 is the minimal polynomial of an element γ of $GF(2^8)$, but it cannot have a common root with $f_{\mathrm{x}}(z)$. So x is a codeword of $\Gamma(L,g)$, where

$$g(z) = z^4+z+1 \quad \text{and} \quad L = \mathbf{F} \setminus \{\gamma, \gamma^2, \gamma^4, \gamma^8\} \ .$$

Implicitly, we have proved that the minimum distance of $B(9)$ (and of $\Gamma(L,g)$) is exactly 9.

Comments on Section 4.2 An extensive study of the cyclicity of extended Goppa codes was made by Stichtenoth in [134]; at the end of the paper the author noted that the problem of the characterization of classical Goppa codes (extended or not) which are cyclic remains open. Recently Berger obtained new results by classifying among alternant codes those for which the cyclicity is inherited from automorphism groups of generalized RS codes [19].

Several papers appeared recently characterizing or studying special classes of Goppa codes: quasi-cyclic Goppa codes [30], 2-divisible Goppa codes [145] or Goppa codes defined by particular polynomials [28]. They can be seen in a general context; their aim is to obtain precise results about the structure of Goppa codes.

4.3 On the weight enumerator of Preparata codes

In this section we present a new form for the weight enumerator of Preparata codes and a new proof of the formal duality between Kerdock and Preparata codes (see Theorem 4.20 later). Recall that the weight distribution of Preparata codes was first obtained by Semakov and Zinoviev [129]; the "formal duality" is due to Zaitsev et al. [151, 1972].

However our aim is to give an example of the construction of good non linear codes based on properties of some cyclic codes. We want to explain Preparata codes by means of tools developed for primitive cyclic codes. The cyclic codes in question have an affine-invariant extension and the material from Section 2 can be used to provide more properties of the most *famous* non linear codes.

By construction the Preparata codes are connected to the cosets of some binary cyclic codes. They are the codes of length 2^m-1, m odd, with defining set

$$cl(1) \cup cl(2^i+1) \ , \quad gcd(i,m) = 1 \ ,$$

where $cl(s)$ is the 2-cyclotomic coset modulo 2^m-1 containing s. These codes were previously denoted by $C_{1,2^i+1}$. For simplicity, we denote $C_{1,2^i+1}$ by B_i. The codes B_i have minimum distance 5 and the same weight enumerator as that of the double-error-correcting BCH code (the code B_1) as explained in Section 3.4.2; this was first proved by Kasami [87][88].

We consider here the extended codes, denoted by $\widehat{B}_i$. These codes are affine-invariant with parameters $[2^m, 2^m-2m-1, 6]$. Indeed such a code has defining set

$$T_i = \{0\} \cup cl(1) \cup cl(2^i+1) \ , \quad gcd(i,m) = 1 \ ,$$

which obviously is the defining set of an affine-invariant code (see Theorem 2.14). As B_i has minimum distance 5, its extension has minimum distance 6. The weight enumerator of any code $\widehat{B}_i^\perp$ is easily deduced from those of $B_i^\perp$ – which is the one of $B_1^\perp$ and was given in Theorem 3.30 – (see a precise explanation in [55]). That is:

Weights of $B_i^\perp$	Number of words
0	1
$2^{m-1}-2^{(m-1)/2}$	$(2^m-1)2^{m-1}$
2^{m-1}	$2^{2m}+2^m-2$
$2^{m-1}+2^{(m-1)/2}$	$(2^m-1)2^{m-1}$
2^m	1

(55)

The codes $\widehat{B}_i$ have the same weight distribution of cosets independent of i. Actually the codes B_i are known to be *uniformly packed* and *completely* *regular*, with the same distance matrix. This comes mainly from the fact that for such a code the external distance is equal to the covering radius. These results are to be found in [13] and [130], where uniformly packed codes were introduced; see also [72] for an extensive study. The next theorem is easily deduced; for clarity we outline the proof.

Theorem 4.15 *The binary extended cyclic codes* $\widehat{B}_i$ *of length* 2^m*, m odd, with defining set*

$$T_i = \{0\} \cup cl(1) \cup cl(2^i+1) \ , \quad gcd(i,m) = 1 \ ,$$

where $0 < i \leq (m-1)/2$*, are affine-invariant* $[2^m, 2^m-2m-1, 6]$ *codes. They are completely regular. They have the same cosets weight distribution. The covering radius and the external distance are equal to four. The distance matrix is*

weights	0	1	2	3	4
coset 0	1	0	0	0	0
coset 1	0	1	0	0	0
coset 2	0	0	1	0	ν_1
coset 3	0	0	0	μ	0
coset 4	0	0	0	0	ν_2

where $\mu = (2^{m-1}-1)/3$, $\nu_1 = (2^{m-2}-2)\mu$ *and* $\nu_2 = 2^{m-2}\mu$*; "coset i" means "coset of minimum weight i". The weight enumerators of the cosets are given in Table 10. Furthermore the codes* $\widehat{B}_i$ *are not equivalent.*

Proof: Recall that the external distance r of a linear code is the number of the non zero weights of its dual. The distance matrix has $r+1$ columns and t rows, where t is the number of distinct weight distributions of the cosets of the code. The $(j+1)$-st column contains the number of codewords of weight j for any weight distribution. Knowledge of this matrix is sufficient for the determination of the complete weight distribution of cosets (see Theorem 10.10 of Chapter 1).

A new formulation of the cosets weight distribution of $\widehat{B}_1$ was given in [55]. The distance matrix and the weight enumerators of cosets were obtained by using some properties which hold for any i. We point out that these results can be generalized: *the coset weight distribution of any* $\widehat{B}_i$ *is the same as the one of* $\widehat{B}_1$ *given in* [55]. We give a sketch of its proof.

- According to (55), the external distance of any code $\widehat{B}_i$ is four. Then the covering radius ρ of the codes B_i satisfies $\rho \leq 4$. Actually it is exactly four since $\widehat{B}_i$ is contained in the Reed-Muller (RM) code of order $m-2$ whose minimum distance is four.

- There are at most four distinct weight distributions. Indeed all cosets of weight one, and all cosets of weight two, have the same weight distribution since the codes $\widehat{B}_i$ are affine-invariant – i.e. invariant under a doubly-transitive group. On the other hand, the weight distributions of cosets of weight 3 and 4 are unique; this is a general result proved in [1], Corollary 1 and 2. Then *the codes $\widehat{B}_i$ are completely regular* since the weight distribution of each coset only depends on the minimum weight of the coset.

- One computes the weight distributions of cosets, and the coefficients of the distance matrix, by considering the linear codes of the form

$$C = \left(\mathrm{x} + \widehat{B}_i\right) \cup \widehat{B}_i \ , \quad \mathrm{x} \notin \widehat{B}_i \ ,$$

  where the weight of x satisfies $1 \leq wt(\mathrm{x}) \leq 4$ and is equal to the weight of C. As $C^\perp$ is contained in $\widehat{B}_i^\perp$, $C^\perp$ has at most four nonzero weights; the code $C^\perp$ has at most three weights when x is an odd weight codeword because in this case it cannot contain the all one vector. So, in any case, we can apply Theorem 3.29 to the weight distribution of C: we know the number of codewords of weight w, $0 \leq w \leq s-1$ and only s coefficients of the weight enumerator of $C^\perp$ are unknown ($s = 3$ or 4).

- Finally the weight enumerator of any code of type C is uniquely obtained from the weight enumerator of $\widehat{B}_i$ which does not depend on i. The distance matrix of all these codes is unique.

Berger has recently proved that two binary affine-invariant codes cannot be equivalent [17]. So the codes $\widehat{B}_i$ are not equivalent.
♦

The automorphism group of the generalized Preparata codes was found by Kantor [83]. In his paper, Kantor proved also the inequivalence of these codes by using a relatively simple description, due to Baker and Wilson.

We recall the definition of the classical extended Preparata codes, due to Baker and Wilson (see also [12]). Note that it was proved by Gœthals et al. that all these codes have the same weight enumerator [71].

For the remainder of the section, let $\mathbf{F}$ be the field of order 2^m with m odd, $\mathbf{k}$ the field of order 2, and $\mathcal{A} = \mathbf{k}[\mathbf{F}]$.

Definition 4.16 *Let i be is an integer such that $gcd(i, m) = 1$. The extended Preparata code $P(i)$ is a non linear binary code of length 2^{m+1}. By identifying any binary codeword with its support, $P(i)$ consists of the codewords described by all pairs*

$$(X,\ Y) \quad , \quad X \subset \mathbf{F} \quad \textit{and} \quad Y \subset \mathbf{F}\ ,$$

satisfying

(i) $\mid X \mid$ *and* $\mid Y \mid$ *are even ,*

(ii) $\displaystyle\sum_{x\in X} x = \sum_{y \in Y} y$ *, and*

(iii) $\displaystyle\sum_{x\in X} x^{2^i+1} + \sum_{y\in Y} y^{2^i+1} = (\sum_{x\in X} x)^{2^i+1}$.

A codeword (x, y) of $\mathcal{A} \times \mathcal{A}$ is a pair

$$\left(\mathrm{x} = \sum_{g\in X} X^g,\ \mathrm{y} = \sum_{g\in Y} X^g \right)$$

where (X, Y) is a pair of subsets of $\mathbf{F}$, the supports of x and y. We are going to present the previous definition in the ambient space $\mathcal{A} \times \mathcal{A}$. For clarity we first recall some definitions given in Section 2.2 about codes of $\mathcal{A}$.

We consider binary primitive codes. The coefficients of the MS polynomial of $\mathrm{x} \in \mathcal{A}$ are the values of the $\mathbf{k}$-linear maps defined for any $s \in [1, 2^m-1]$ as

$$\phi_s \ :\ \mathrm{x} \in \mathcal{A} \ \longmapsto \ \sum_{g\in\mathbf{F}} x_g g^s \in \mathbf{F}\ .$$

By convention, we have in addition: $\phi_0(\mathrm{x}) = \sum_{g\in\mathbf{F}} x_g$ (see (8)). The 2-weight of s is denoted by $wt_2(s)$; it is the sum $\sum_{i=0}^{m-1} s_i$, where $s = \sum_{i=0}^{m-1} s_i 2^i$, $s_i \in \{0, 1\}$. The Reed-Muller code of order $m - j$ is the following subspace of $\mathcal{A}$:

$$\mathcal{R}_2(m-j, m) = \{\ \mathrm{x} \in \mathcal{A} \mid wt_2(s) < j \ \Rightarrow \ \phi_s(\mathrm{x}) = 0\ \}\ . \qquad (56)$$

The extension of the 2-error-correcting BCH code is the following subspace of $\mathcal{A}$:

$$\widehat{B}_1 = \{ \ \mathrm{x} \in \mathcal{A} \mid \phi_0(\mathrm{x}) = \phi_1(\mathrm{x}) = \phi_3(\mathrm{x}) = 0 \ \} \ . \tag{57}$$

Recall that the RM codes and the extended BCH codes are ideals of $\mathcal{A}$. The code $\mathcal{R}_2(m-1, m)$, which is the radical $\mathcal{P}$ of $\mathcal{A}$, is the set of codewords of even weight. The code $\mathcal{R}_2(m-j, m)$ is the j-th power $\mathcal{P}^j$ of the radical of $\mathcal{A}$ (see Section 2.4).

Notation: In the sequel, and for simplicity, the code $\widehat{B}_1$ will be denoted by $\widehat{B}$ and the Preparata code $P(1)$ by $\overline{P}$. The code $\mathcal{R}_2(m-j, m)$ will be denoted by $\mathcal{P}^j$.

Lemma 4.17 *The Preparata code $\overline{P}$ consists of all pairs of codewords*

$$(\ \mathrm{x}, \ \mathrm{y}) \ , \quad \mathrm{x} \in \mathcal{A} \ , \ \mathrm{y} \in \mathcal{A} \quad ,$$

satisfying

(a) $\phi_0(\mathrm{x}) = \phi_0(\mathrm{y}) = 0 \quad ,$

(b) $\phi_1(\mathrm{x}) = \phi_1(\mathrm{y}) \quad$ *, and*

(c) $\phi_3(\mathrm{x}) + \phi_3(\mathrm{y}) = (\phi_1(\mathrm{x}))^3 \ .$

Moreover **(a)** *means that* x *and* y *are in* $\mathcal{P}$.

Suppose that **(a)** *is satisfied. Then* **(b)** *means that* $\mathrm{x}+\mathrm{y}$ *is in* $\mathcal{P}^2$*;* **(b)** *and* **(c)** *means that* $\mathrm{x}+\mathrm{y}$ *is in the coset* $\mathrm{z}+\widehat{B}$ *whose syndrome is*

$$(\phi_0(\mathrm{z}) = 0 \ , \ \phi_1(\mathrm{z}) = 0 \ , \ \phi_3(\mathrm{z}) = (\phi_1(\mathrm{x}))^3 \ ) \ . \tag{58}$$

Proof: We simply rewrite the conditions of Definition 4.16 by means of the functions ϕ_s and with $i = 1$. By definition

$$\sum_{x \in X} x^j = \phi_j(\mathrm{x}).$$

Condition **(i)** in Definition 4.16 means that x and y are even weight codewords, i.e. both are codewords of $\mathcal{P}$. Condition **(ii)** means that $\phi_1(\mathrm{x})$ equals $\phi_1(\mathrm{y})$. Since ϕ_1 is linear, this is equivalent to $\phi_1(\mathrm{x}+\mathrm{y}) = 0$. Therefore, if **(a)** is satisfied, **(b)** means that $\mathrm{x}+\mathrm{y} \in \mathcal{P}^2$; in other words x and y are in the same coset of $\mathcal{P}^2$.

In the same manner condition **(c)** is condition **(iii)** rewritten with ϕ_1 and ϕ_3. Assume that x and y satisfy **(a)**, **(b)** and **(c)**. Set $\mathrm{z} = \mathrm{x} + \mathrm{y}$ and note that $\phi_3(\mathrm{x}) + \phi_3(\mathrm{y}) = \phi_3(\mathrm{z})$. Then it is clear that the syndrome of z, with respect to $\widehat{B}$, is given by (58); any codeword of the coset $\mathrm{z} + \widehat{B}$ has such a syndrome.

Conversely assume that x and y satisfy **(a)** and that $\mathrm{x} + \mathrm{y}$ is in the coset $\mathrm{z} + \widehat{B}$ whose syndrome is given by (58). As ϕ_1 and ϕ_3 are linear, **(b)** and **(c)** are satisfied.

♦

Our purpose is to prove Theorem 4.20. We begin by recalling the weight distribution of the cosets of the extended 2-error-correcting BCH codes. Theorem 4.18 and results presented in Table 10 were given in [55].

Theorem 4.18 *The extended* 2*-error-correcting BCH code of length* $2^m - 1$, *m odd, is denoted by* $\widehat{B}$. *Denote by* $W_{(i)}(X,Y)$ *the weight enumerator of the coset of* $\widehat{B}$ *of weight i.*

There are five distinct weight enumerators for the cosets of $\widehat{B}$: $W_{(i)}(X,Y)$ *for* $0 \le i \le 4$, *where* $W_{(0)}(X,Y)$ *is the weight enumerator of the code* $\widehat{B}$ *itself. The total number of cosets is* 2^{2m+1}. *The number of cosets of each weight is as follows:*

weight	*number*
1	2^m
2	$2^{m-1}(2^m - 1)$
3	$2^m(2^m - 1)$
4	$(2^{m-1} + 1)(2^m - 1)$

Among the cosets of minimum weight four, $2^m - 1$ *are in* $\mathcal{P}^2$ *and* $2^{m-1}(2^m - 1)$ *are in* $\mathcal{P} \setminus \mathcal{P}^2$. *The polynomials* $W_{(i)}(X,Y)$, $1 \le i \le 4$, *are given in Table 10. In this table the three weights of the dual of* $\widehat{B}$ *different from* 2^m *are denoted by* γ_i *and we write* Z^t *instead of* $(X+Y)^{2^m - t}(X-Y)^t$.

The following property on the cosets of $\widehat{B}$ of weight four and contained in $\mathcal{P} \setminus \mathcal{P}^2$ is surprising. As we will see in the proof of Lemma 4.22, it implies that the minimum distance of the code $\overline{P}$ is six. It can be obviously generalized to any code $\widehat{B}_i$.

Proposition 4.19 *Let D be a coset of* $\widehat{B}$ *contained in* $\mathcal{P} \setminus \mathcal{P}^2$. *Let* $\mathrm{x} \in D$. *Then the weight of D is four if and only if there is an* $h \in \mathbf{F}$ *such that* $\phi_3(X^h \mathrm{x}) = 0$.

$$W_{(1)}(X,Y) = \tfrac{1}{2^{2m+1}}\left(Z^0 + 2^{(m-1)/2}(2^m-1)Z^{\gamma_1} - 2^{(m-1)/2}(2^m-1)Z^{\gamma_3} - Z^{2^m}\right)$$

$$W_{(2)}(X,Y) = \tfrac{1}{2^{2m+1}}\left(Z^0 + 2^{m-1}Z^{\gamma_1} - (2^m+2)Z^{\gamma_2} + 2^{m-1}Z^{\gamma_3} + Z^{2^m}\right)$$

$$W_{(3)}(X,Y) = \tfrac{1}{2^{2m+1}}\left(Z^0 - 2^{(m-1)/2}Z^{\gamma_1} + 2^{(m-1)/2}Z^{\gamma_3} - Z^{2^m}\right)$$

$$W_{(4)}(X,Y) = \tfrac{1}{2^{2m+1}}\left(Z^0 - 2^{m-1}Z^{\gamma_1} + (2^m-2)Z^{\gamma_2} - 2^{m-1}Z^{\gamma_3} + Z^{2^m}\right)$$

with notation:

$$Z^t = (X+Y)^{2^m-t}(X-Y)^t$$

$$\gamma_1 = 2^{m-1} - 2^{(m-1)/2}\ , \quad \gamma_2 = 2^{m-1}\ , \quad \gamma_3 = 2^{m-1} + 2^{(m-1)/2}$$

Table 10: Weight distribution of cosets of the code $\widehat{B}$; see Theorem 4.8.

Proof: Recall that

$$X^h\mathrm{x} = X^h\left(\sum_{g\in\mathbf{F}} x_g X^g\right) = \sum_{g\in\mathbf{F}} x_g X^{g+h} \ .$$

Since $\widehat{B}$, $\mathcal{P}$ and $\mathcal{P}^2$ are invariant under the affine group, each coset X^hD satisfies

$$X^hD = X^h\mathrm{x} + \widehat{B} \ , \quad h \in \mathbf{F}$$

and is contained in $\mathcal{P} \setminus \mathcal{P}^2$. Clearly D and X^hD have the same weight enumerator. The syndrome of a coset $D = \mathrm{x} + \widehat{B}$ with $\mathrm{x} \in \mathcal{P} \setminus \mathcal{P}^2$ is $(0,\ \phi_1(\mathrm{x}),\ \phi_3(\mathrm{x}))$ where $\phi_1(\mathrm{x}) \neq 0$. Note that the weight of D is either 2 or 4 since D is contained in $\mathcal{P}$.

Assume that $\phi_3(\mathrm{x}) = 0$. If there is a codeword of weight 2, say $X^u + X^v$, in D, then we have

$$\phi_3(X^u + X^v) = u^3 + v^3 = 0 \ .$$

This leads to $u = v$ (as m is odd, $gcd(3, 2^m - 1) = 1$), a contradiction. So we have proved that D is a coset of weight 4 when $\phi_3(\mathrm{x}) = 0$.

Now we will prove that there are exactly $2^m(2^m - 1)$ cosets D of weight 4 such that $\phi_3(X^h\mathrm{x}) = 0$, for some h. First there are $2^m - 1$ cosets with syndrome

$$(0 \ , \ \phi_1(\mathrm{x}) = \beta \ , \ \phi_3(\mathrm{x}) = 0) \ , \quad \beta \in \mathbf{F}^* \ .$$

Let $\mathrm{x} = \sum_{g\in\mathbf{F}} x_g X^g$ and compute the syndrome of $X^h\mathrm{x}$:

$$\phi_1(X^h\mathrm{x}) = \sum_g x_g(h+g) = \sum_g x_g g + h\sum_g x_g = \phi_1(\mathrm{x}) = \beta$$

since the weight of x is even and by fixing β,

$$\begin{aligned} \phi_3(X^h\mathrm{x}) &= \sum_g x_g(h+g)^3 = \sum_g x_g(h^3 + g^3 + hg^2 + gh^2) \\ &= h^3\sum_g x_g + \sum_g x_g g^3 + h\sum_g x_g g^2 + h^2\sum_g x_g g \\ &= \phi_3(\mathrm{x}) + h\beta^2 + h^2\beta \ . \end{aligned}$$

So $\phi_3(X^h\mathrm{x}) = \phi_3(\mathrm{x})$ if and only if either $h = 0$ or $h = \beta$. Hence the set $\{\phi_3(X^h\mathrm{x}) \mid h \in \mathbf{F}\}$ has cardinality 2^{m-1}, corresponding to 2^{m-1} equivalent, and distinct, cosets with syndromes

$$(0 \ , \ \beta \ , \ \phi_3(X^h\mathrm{x}) = \phi_3(\mathrm{x}) + h^2\beta + h\beta^2 \ ) \ , \quad h \in \mathbf{F} \ .$$

We then obtain exactly the $2^{m-1}(2^m-1)$ cosets that we expected. But this is exactly the number of cosets of weight four contained in $\mathcal{P}\setminus\mathcal{P}^2$ (see Theorem 4.18), completing the proof
♦

Now we come back to the Preparata codes. Recall that for any codeword $(\mathrm{x},\ \mathrm{y}) \in \overline{P}$, x and y are in $\mathcal{P}$. This shows that the Preparata codes are constructed from even weight cosets of $\widehat{B}$ only. Our notation is that of Theorem 4.18. The polynomials $W_{(i)}(X,Y)$ are given in Table 10.

Theorem 4.20 *Denote by $W(X,Y)$ the weight enumerator of the Preparata code of length 2^{m+1}, m odd. Then :*

$$\begin{aligned} W(X,Y) &= 2^m(2^m-1)\ W_{(2)}(X,Y)\ W_{(4)}(X,Y) \\ &\quad +(2^m-1)\ \left(W_{(4)}(X,Y)\right)^2 \\ &\quad +\ \left(W_{(0)}(X,Y)\right)^2 \end{aligned} \tag{59}$$

If we apply the MacWilliams identity to $W(X,Y)$, by using the formulas of Table 10, we obtain the weight polynomial of the Kerdock code of length 2^{m+1}:

$$\begin{aligned} K(X,Y) &= T^0 + 2^{m+1}(2^m-1)T^{2^m-2^{(m-1)/2}} + (2^{m+2}-2)T^{2^m} \\ &\quad +2^{m+1}(2^m-1)T^{2^m+2^{(m-1)/2}} + T^{2^{m+1}} \end{aligned} \tag{60}$$

where $T^i = X^{2^{m+1}-i}\ Y^i$.

We begin by proving two Lemmas.

Lemma 4.21 *Consider the subcode L of the Preparata code $\overline{P}$ where*

$$L = \overline{P} \cap \{\ (\mathrm{x},\ \mathrm{y}) \mid \mathrm{x} \in\ \mathcal{P}^2\ \}\ .$$

Then

$$L = \bigcup_{\mathrm{x}\in\mathcal{P}^2} (\mathrm{x}+\widehat{B}) \times (\mathrm{x}+\widehat{B}),$$

and the weight enumerator of L is equal to

$$(2^m-1)\ \left(W_{(4)}(X,Y)\right)^2 +\ \left(W_{(0)}(X,Y)\right)^2\ . \tag{61}$$

Proof: By definition $\mathrm{x} \in \mathcal{P}^2$ if and only if $\phi_0(\mathrm{x}) = \phi_1(\mathrm{x}) = 0$. Assuming this we write conditions **(a)**, **(b)** and **(c)** of Lemma 4.17. We get that a pair $(\mathrm{x},\ \mathrm{y})$ is in L if and only if

$$\begin{array}{rcl} \phi_0(\mathrm{x}) & = & \phi_1(\mathrm{x}) \ = \ 0 \\ \phi_s(\mathrm{x}) & = & \phi_s(\mathrm{y}) \ \ , \quad s = 0,1,3 \ . \end{array} \tag{62}$$

Clearly (62) is equivalent to

$$\mathrm{x} \in \mathcal{P}^2 \ \text{ and } \ \mathrm{y} \in \mathrm{x} + \widehat{B} \ . \tag{63}$$

So any pair $(\mathrm{x},\ \mathrm{y})$ of L belongs to $(\mathrm{x} + \widehat{B}) \times (\mathrm{x} + \widehat{B})$. Conversely $\mathrm{x} + \widehat{B}$ is contained in $\mathcal{P}^2$ for any $\mathrm{x} \in \mathcal{P}^2$. According to (63) we have: for any x' in $\mathrm{x} + \widehat{B}$ then $(\mathrm{x}',\ \mathrm{y})$ is in L for all $\mathrm{y} \in \mathrm{x} + \widehat{B}$, implying $(\mathrm{x} + \widehat{B}) \times (\mathrm{x} + \widehat{B}) \subseteq L$. When $\phi_3(\mathrm{x}) = 0$, then $\mathrm{x} \in \widehat{B}$ and we obtain $\widehat{B} \times \widehat{B} \subseteq L$. We have proved that

$$L = \widehat{B} \times \widehat{B} \ \bigcup_{\mathrm{x} \in \mathcal{P}^2 \setminus \widehat{B}} (\mathrm{x} + \widehat{B}) \times (\mathrm{x} + \widehat{B}).$$

The cosets $(\mathrm{x} + \widehat{B})$ are the cosets of $\widehat{B}$ of weight four which are contained in $\mathcal{P}^2$. There are $2^m - 1$ such cosets. They have the same weight enumerator (see Theorem 4.18).

On the other hand, the weight enumerator of any product of codes, say $A \times A'$, is the product of the weight enumerator of A and the weight enumerator of A'. The weight enumerator of L is immediate; one obtains (61) with the notation of Table 10.

♦

Lemma 4.22 *Set* $\mathcal{I} = \mathcal{P} \setminus \mathcal{P}^2$. *Denote by* $\delta(\mathrm{x})$ *the weight of the coset* $(\mathrm{x} + \widehat{B})$. *Consider the subcode* N *of* $\overline{P}$ *where*

$$N = \overline{P} \cap \{\ (\mathrm{x},\ \mathrm{y}) \mid \mathrm{x} \in \mathcal{I}\ \}\ .$$

Then

$$N = \bigcup_{\substack{\mathrm{x} \in \mathcal{I},\ \mathrm{z} \in \mathcal{P}^2 \\ \phi_3(\mathrm{z}) = \phi_1(\mathrm{x})^3}} (\mathrm{x} + \widehat{B}) \times (\mathrm{x} + \mathrm{z} + \widehat{B})\ ,$$

Moreover, for any product of cosets above, if $\delta(\mathrm{x}) = 2$ *then* $\delta(\mathrm{x} + \mathrm{z}) = 4$ *and if* $\delta(\mathrm{x}) = 4$ *then* $\delta(\mathrm{x} + \mathrm{z}) = 2$.

The weight enumerator of N is equal to

$$2^m(2^m-1)\ W_{(2)}(X,Y)\ W_{(4)}(X,Y)\ .$$

Proof : By definition of $\overline{P}$, the pair (x, y) is in $\overline{P}$ if and only if the product of the cosets $(\mathrm{x}+\widehat{B})\times(\mathrm{y}+\widehat{B})$ is in $\overline{P}$. This is because $\phi_s(\mathrm{x}+\widehat{B})=\phi_s(\mathrm{x})$, for $s\in\{0,1,3\}$, implying that the conditions of Lemma 4.17 hold for the cosets of $\widehat{B}$ generated by x and y. On the other hand, a coset $\mathrm{x}+\widehat{B}$ is in $\mathcal{I}$ if and only if it is an even weight coset such that $\phi_1(\mathrm{x})\neq 0$. The weight of any coset contained in $\mathcal{I}$ is either 2 or 4.

Let x and y be any elements of $\mathcal{A}$ and set $\mathrm{z}=\mathrm{x}+\mathrm{y}$. The pair (x, y) is in N if and only if $\mathrm{x}\in\mathcal{I}$ and $(\mathrm{x},\ \mathrm{y})\in\overline{P}$. This is clearly equivalent to

$$\mathrm{x}\in\mathcal{I},\ \mathrm{z}\in\mathcal{P}^2\ \text{ and }\ \phi_3(\mathrm{z})=\phi_1(\mathrm{x})^3\ .$$

Indeed $\mathrm{z}\in\mathcal{P}^2$, with $\mathrm{x}\in\mathcal{I}$, is equivalent to conditions **(a)** and **(b)** of Lemma 4.17. The last equality corresponds to condition **(c)**.

Set $\beta=\phi_1(\mathrm{x})$ and denote respectively by D and D' the cosets $(\mathrm{x}+\widehat{B})$ and $(\mathrm{y}+\widehat{B})$. If $\delta(\mathrm{x})=4$, we can suppose $\phi_3(\mathrm{x})=0$ (from Proposition 4.19 and because $\widehat{B}$ is affine-invariant). Then conditions **(b)** and **(c)** give

$$\phi_1(\mathrm{y})=\beta\quad\text{and}\quad\phi_3(\mathrm{y})=\beta^3\ .$$

Hence the coset D' contains the codeword X^0+X^β whose syndrome is obviously $(0,\ \beta,\ \beta^3)$. Conversely suppose that $\delta(\mathrm{x})=2$. Up to equivalence we can assume that D contains the codeword $\mathrm{x}=X^0+X^\beta$. Condition **(c)** gives

$$\phi_3(\mathrm{x})+\phi_3(\mathrm{y})=\beta^3=\beta^3+\phi_3(\mathrm{y})$$

since $\phi_3(\mathrm{x})=\beta^3$. So $\phi_3(\mathrm{y})=0$ implying that D' has weight four.

It is important to notice that for any given coset D, the coset D' is uniquely determined. Since there are $2^{m-1}(2^m-1)$ cosets of weight four and $2^{m-1}(2^m-1)$ cosets of weight two contained in $\mathcal{I}$, we have $2^m(2^m-1)$ cosets in N. We obviously deduce the weight polynomial of N.
♦

Proof of Theorem 4.20: The proof is easily deduced from the two previous lemmas. The codewords (x, y) of $\overline{P}$ are such that x and y both have even weight. So x (resp. y) is either in $\mathcal{P}\setminus\ \mathcal{P}^2$ or in $\mathcal{P}^2$. Obviously the code $\overline{P}$ is equal to the union of L and N, two sets which do not intersect. Therefore the weight enumerator of $\overline{P}$ is equal to the weight enumerator of L plus the weight enumerator of N – these weight enumerators are given by Lemmas 4.21 and 4.22.

It is well-known that the weight enumerator of the Preparata code is the MacWilliams transform of the weight enumerator of the Kerdock code; this was proved by Semakov, Zaitsev and Zinoviev [151] (see also [111, ch.5, §5]). We give another proof of this property.

The weight enumerator $W_{(0)}(X,Y)$ is given by (55); the $W_{(i)}(X,Y)$ are given in Table 10. By using these formulas and (59), one computes the weight enumerator of the code $\overline{P}$ and obtains

$$\begin{aligned} W(X,Y) &= \frac{1}{2^{4m+2}}\Big(2^{2m}U^0 + 2^{2m}U^{2^{m+1}} + (2^{4m+1}-2^{3m+1})U^{2^m-2^{(m-1)/2}} \\ &+ (2^{4m+1}-2^{3m+1})U^{2^m+2^{(m-1)/2}} + (2^{3m+2}-2^{2m+1})U^{2^m}\Big) \end{aligned}$$

where $U^i = (X+Y)^{2^{m+1}-i}(X-Y)^i$. The MacWilliams transform of the weight enumerator of the code $\overline{P}$ is

$$K(X,Y) = \frac{1}{2^{2^{m+1}-2(m+1)}}W(X+Y, X-Y).$$

So, in the expression of $W(X,Y)$, U^i is replaced by

$$((X+Y)+(X-Y))^{2^{m+1}-i}\,((X+Y)-(X-Y))^i = 2^{2^{m+1}}X^{2^{m+1}-i}Y^i.$$

We obtain

$$\begin{aligned} K(X,Y) &= X^{2^{m+1}} + Y^{2^{m+1}} + 2^{m+1}(2^m-1)X^{2^m+2^{(m-1)/2}}Y^{2^m-2^{(m-1)/2}} \\ &+ 2^{m+1}(2^m-1)X^{2^m-2^{(m-1)/2}}Y^{2^m-2^{(m-1)/2}} + (2^{m+2}-2)X^{2^m}Y^{2^m}\ , \end{aligned}$$

which is the weight enumerator of the Kerdock code, given in (60), completing the proof.

♦

Comments on Section 4.3 Note that the description of the automorphism group of Kerdock codes is to be found in [40].

The class of codes $\widehat{B}_i$ is an example of nonequivalent codes which have the same weight distribution of cosets, as stated in Theorem 4.15. Note that, according to Theorem 4.15, we could consider $P(i)$ and the cosets of $\widehat{B}_i$ throughout the section. We claim that the result given by Theorem 4.20 holds for any i.

The number of distinct weight enumerators of cosets of the primitive 2-error-correcting BCH codes, extended or not, is the same for any length $2^m - 1$. This number is four when m is odd; it is eight for m even. It is respectively five and eight for the extended codes [55]. This property does not hold for the 3-error-correcting BCH codes, providing several conjectures (see [57]). Note that, however, the external distance of the 3-error-correcting BCH codes is five (six for the extension) for any length. For these codes, the external distance is a constant while the number of weight enumerators of cosets increases with the length. The Gœthals codes are built from cosets of the 3-error-correcting BCH codes and there is a direct definition analogous to Definition 4.16 of these codes [12]; so it is possible to state a lemma analogous to Lemma 4.17.

About the Preparata codes, our aim is to explain the following point of view. Each code is a union of product sets $C_1 \times C_2$ where C_1 and C_2 are cosets of the extended 2-error-correcting BCH code. By fixing C_1 we determine C_2, and vice-versa. So *the definition of the codewords of $\overline{P}$ is based on relations on these cosets and not on relations on the words of these cosets.* Furthermore we are not surprised that the weight enumerator of $\overline{P}$ is in a certain sense not dependent on the construction of the code. This is especially true for the cosets of weight four: there are two distinct kinds of cosets of weight four and both have the same weight enumerator.

There are many other possible relations between the cosets which do not change the weight enumerator. They could provide other constructions and then other codes with the same weight enumerator. It could provide, for instance, a construction of the *Preparata-like* code obtained in [75].

5 Conclusion

This chapter does not give an exhaustive overview of problems involving unknown properties of cyclic codes. Our aim was to emphasize that research on cyclic codes remains a topic of great interest for a large community.

We have focused on some problems which have been recognized as hard for a long time. Therefore some recent new topics are not developed here. The most famous example is the fast-expanding study of cyclic codes over

Z_k, k not a prime, originated by the work of HAMMONS et al. [75] (in the case $k = 4$)– see also the earlier paper due to NECHAEV [119]. The authors showed that some codes, not cyclic in the usual sense, can be viewed as Z_4-cyclic codes. In [75], they conclude that *this new point of view should completely transform the study of cyclic codes*. Our purpose is not in conflict because we wish to develop the idea that important problems in cyclic codes remain unsolved and necessitate new tools or new methods for going further.

This chapter is based on valuable discussions with a number of researchers of the community. Particularly we want to express our gratitude to E.F. ASSMUS, JR, D. AUGOT, C. CARLET, T.P. BERGER, J. WOLFMANN and V. ZINOVIEV for their contributions.

We would further mention N. SENDRIER, A. CANTEAUT, and F. LEVY-DIT-VEHEL who have provided respectively Tables 2, 3 and 4 and gave information about all their numerical results.

References

[1] E.F. ASSMUS, JR & V. PLESS *On the covering radius of extremal self-dual codes*, IEEE Transactions on Information Theory, vol. IT-29, n. 3, May 1983.

[2] E.F. ASSMUS JR & J.D. KEY, *Designs and their codes*, Cambridge Tracts in Mathematics, Volume 103, Cambridge University Press, 1992.

[3] E.F. ASSMUS, *On the Reed-Muller codes*, Discrete Mathematics 106/107 (1992) 25-33.

[4] D. AUDIBERT & N. SENDRIER, *Distribution des poids des codes cycliques binaires de longueur* 63. INRIA-report Number 2299, July 1994.

[5] D. AUGOT, *Etude algèbrique des mots de poids minimum des codes cycliques. Méthodes d'algèbre linéaire sur les corps finis*, Thèse de l'Université Paris 6, Décembre 1993.

[6] D. AUGOT, *Description of minimum weight codewords of cyclic codes by algebraic system*, Finite Fields and their Applications,2, 138-152 (1996) pp. 138-152.

[7] D. Augot, P. Charpin & N. Sendrier, *The minimum distance of some binary codes via the Newton's Identities*, EUROCODE'90, LNCS 514, pp. 65-73, Springer-Verlag.

[8] D. Augot, P. Charpin & N. Sendrier, *Sur une classe de polynômes scindés de l'algèbre* $\mathbf{F}_{2^m}[Z]$, C. R. Acad. Sci. Paris, t.312, Série I, pp. 649-651, 1991.

[9] D. Augot, P. Charpin & N. Sendrier, *Studying the locator polynomials of minimum weight codewords of BCH codes*, IEEE Transactions Information Theory, vol. 38, n.3, pp. 960-973, May 92.

[10] D. Augot & N. Sendrier, *Idempotents and the BCH bound*, IEEE Transactions on Information Theory, Vol. 40, N. 1, January 94, pp. 204-207.

[11] D. Augot & F. Levy-dit-Vehel, *Bounds on the minimum distance of the duals of BCH codes* , IEEE Transactions on Information Theory, vol. 42, N0 4, July 1996, pp. 1257-1260.

[12] R.D. Baker, J.H. Van Lint & R.M. Wilson, *On the Preparata and Gœthals codes*, IEEE Transactions on Information Theory, Vol. IT29, N.3, May 83, pp. 341-5.

[13] L.A. Bassalygo & V.A. Zinoviev, *Remark on uniformly packed codes*, translated from Problemy Peredachi Informatsii, vol. 13, N. 3, pp. 22-25, July-September 1977.

[14] L.D. Baumert & R. J. McEliece, *Weights of irreducible cyclic codes*, Information and Control 20, 158-175 (1972).

[15] L.D. Baumert & J. Mikkeltveit, *Weight distributions of some irreducible cyclic codes*, JPL technical report, vol. 16, pp. 128-131, 1973.

[16] T. Becker & V. Weispfenning, *Gröbner bases, a computationnal approach to commutative algebra*, Springer-Verlag, 1993.

[17] T. P. Berger, *Automorphism groups and the permutation groups of affine-invariant codes*, Proceedings of Finite Fields and Applications (third conference), Glasgow, England, London Mathematical Society, Lecture Series 233, Cambridge University Press, pp. 31-45 (1996).

[18] T. P. Berger, *On the automorphism group of affine-invariant codes*, Designs Codes and Cryptography, 7, 215-221 (1996), pp. 215-221.

[19] T. P. Berger, *From Cyclic Alternant codes to Cyclic Goppa codes*, Proceedings of Finite Fields and Applications (4th conference), Waterloo, Canada, 1998, to appear.

[20] T.P. Berger & P. Charpin, *The automorphism group of Generalized Reed-Muller codes*, *Discrete Mathematics* 117 pp. 1-17, 1993.

[21] T.P. Berger & P. Charpin, *The permutation group of affine-invariant extended cyclic codes*, IEEE Transactions on Information Theory, vol. 42, No. 6, November 1996, pp. 2194-2209.

[22] E.R. Berlekamp, Algebraic Coding Theory, McGraw-Hill, New-york, 1968.

[23] E.R. Berlekamp, *The weight enumerators for certain subcodes of the second order Reed-Muller codes*, Info. and Control, 17(1970) 485-500.

[24] E.R. Berlekamp & J. Justesen, *Some long cyclic linear binary codes are not so bad*, IEEE Transactions on Information Theory, IT-20, May 1974, pp. 351-356.

[25] S.D. Berman, *On the theory of group codes*, Kibernetika, Vol. 3, N. 1, pp. 31-39, 1967.

[26] S.D. Berman, *Semisimple cyclic and abelian codes, II*, Kibernetika, Vol. 3, N. 3, pp. 21-30, 1967.

[27] E. Biham & A. Shamir, *Differential cryptanalysis of DES-like cruptosystems*, Journal of Cryptology, Vol. 4 No. 1 (1991), pp. 3-72.

[28] V. Bezzateev & N.A. Shekhunova, *A subclass of binary Goppa codes with improved estimation of the code dimension*, Designs, Codes and Cryptography, to appear.

[29] R.E. Blahut, *Transform techniques for error control codes*, IBM J. Res. Dev. 23 (1979), 299-315.

[30] F. Blanchet & G. Bommier, *Binary quasi-cyclic Goppa codes*, submitted – abstract in the Proceedings of "1997 IEEE International Symposium on Information Theory", p. 504, June 29 - July 4, 1997.

[31] M. de Boer & R. Pellikaan, *Grobner bases for error-correcting codes and their decoding* in "Some tapas of computer algebra" (A.M. Cohen, H. Cuypers and H. Sterk eds.) by Springer-Verlag, to appear.

[32] P. Bours, J.C.M. Janssen, M. van Asperdt & H.C.A. van Tilborg, *Algebraic decoding beyong e_{BCH} of some binary cyclic codes, when $e > e_{BCH}$*, IEEE Transactions on Information Theory, Vol. 36, No 1, January 1990, pp. 214-222.

[33] A.E. Brouwer & L.M.G.M. Tolhuizen, *A Sharpening of the Johnson Bound for Binary Linear Codes*, Designs, Codes and Cryptography, vol. 3, No. 1, pp. 95-98, 1993.

[34] A.R. Calderbank, G. McGuire, P.V. Kumar & T. Helleseth, *Cyclic codes over Z_4, locator polynomials and Newton's Identities*, IEEE Transactions on Information Theory, Vol. 42, N.1, January 96, pp. 217-27.

[35] A.R. Calderbank, G. McGuire, B. Poonen & M. Rubinstein, *On a conjecture of Helleseth regarding pairs of binary m-sequences*, IEEE Transactions on Information Theory, Vol. 42, N. 3, May 1996, pp. 988-990.

[36] P. Camion, C. Carlet, P. Charpin & N. Sendrier, *On correlation-immune functions*, Advances in Cryptology, CRYPTO'91, LNCS, Springer Verlag n° 576, 86-100.

[37] P. Camion & A. Canteaut, *Construction of t-resilient functions over a finite alphabet*, EUROCRYPT'96, Advances in Cryptology, Lecture Notes in Computer Science 1070, 283-293 (1996)

[38] A. Canteaut & F. Chabaud, *A new algorithm for finding minimum weight codewords in a linear code: application to primitive narrow-sense BCH codes of length* 511, IEEE Transactions on Information Theory, to appear.

[39] C. Carlet, *A transformation on Boolean functions, its consequences on some problems related to Reed-Muller codes*, EUROCODE' 90, LNCS n° 514, pp. 42-50, Springer-Verlag (1991).

[40] C. Carlet, *The automorphism groups of the Kerdock codes*, Journal of Information & Optimization Sciences, Vol. 12(1991), No 3, pp. 387-400.

[41] C. Carlet, *The divisors of $x^{2^m} + x$ of constant derivatives and degree* 2^{m-2}, SIAM Journal on Discrete Math., vol 7, no 2, 238-244 (1994).

[42] C. Carlet, *Two new classes of bent functions*, Proceedings of EUROCRYPT' 93, Advances in Cryptology, LNCS, n° 765, 77-102.

[43] C. Carlet, *Partially-bent functions*, Designs Codes and Cryptography, 3, 135-145 (1993).

[44] C. Carlet, P. Charpin & V. Zinoviev, *Codes, Bent Functions and Permutations Suitable For DES-like Cryptosystems*, submitted.

[45] C. Carlet, P. Guillot, *An alternate characterization of the bentness of binary functions, with uniqueness*, Designs Codes and Cryptography, to appear.

[46] G. Castagnoli, J.L. Massey, P.A. Schoeller & N. von Seeman, *On repeated-root cyclic codes*, IEEE Transactions Inform. Theory IT-37 (1991), pp. 337-342.

[47] A.G. Cerveira, On a class of wide-sense binary BCH codes whose minimum distance exceed the BCH bound, IEEE Transactions on Information Theory, 14(1968) 784-785.

[48] F. Chabaud & S. Vaudenay, *Links between differential and linear cryptanalysis*, Proceedings of EUROCRYPT"94, Advances in Cryptology, LNCS, n° 950, 356-366.

[49] P. Charpin, *The extended Reed-Solomon codes considered as ideals of a modular algebra*, Annals of Discrete Mathematics 17(1983), 171-176.

[50] P. Charpin, *A description of some extended cyclic codes with application to Reed-Solomon codes*, Discrete Mathematics 56 (1985) 117-124.

[51] P. Charpin, *Codes cycliques étendus invariants sous le groupe affine*, Thèse de Doctorat d'Etat, Univ. PARIS VII, 1987.

[52] P. Charpin, *Codes cycliques étendus affines-invariants et antichaines d'un ensemble partiellement ordonné*, Discrete Mathematics 80 (1990), 229-247.

[53] P. Charpin, *On a class of primitive BCH codes*, IEEE Transactions on Information Theory, vol. 36, pp. 222-228, Number 1, 1990.

[54] P. Charpin & F. Levy-dit-Vehel, *On self-dual affine-invariant codes*, Journal of Combinatorial Theory, Series A, Vol. 67, N. 2, August 1994, p. 223-244.

[55] P. Charpin, *Weight Distributions of Cosets of 2-Error-Correcting Binary BCH Codes, Extended or not*, IEEE Transactions on Information Theory, vol. IT-40, pp. 1425-1442, Sept. 1994.

[56] P. Charpin, *Tools for cosets weight enumerators of some codes*, Proceedings of "Finite Fields: Theory, Applications and Algorithmes", AMS publication, Contemporary Mathematics, vol. 168, 1994, pp. 1-13.

[57] P. Charpin & V. Zinoviev, *On coset weight distributions of the* 3-*error-correcting BCH codes*, SIAM Journal of discrete Mathematics, Vol. 10, No. 1, pp. 128-145, February 1997.

[58] P. Charpin, A. Tietäväinen & V. Zinoviev, *On binary cyclic codes with* $d = 3$, Problems of Information Transmission, vol. 33, No 3 (1997).

[59] X. Chen, I.S. Reed, T. Helleseth & T.K. Truong, *Use of Gröbner bases to decode binary cyclic codes up to the minimum distance*, IEEE Transactions on Information Theory, vol. 40, N.5, September 94, pp. 1654-1661.

[60] X. Chen, I.S. Reed, T. Helleseth & T.K. Truong, *General principles for the algebraic decoding of cyclic codes*, IEEE Transactions on Information Theory, vol. 40, N.5, September 94, pp. 1661-63.

[61] S.D. Cohen, *The length of primitive BCH codes with minimal covering radius*, Designs, Codes and Cryptography, 10, 5-16 (1997).

[62] G.D. Cohen, S.N. Litsyn, A.C. Lobstein, H.F. Mattson,Jr, *Covering radius 1985-1994*, Applicable Algebra in Engineering, Communication and Computing, Vol. 8, No. 3, 1997.

[63] P. Delsarte & J.M. Gœthals, *Irreducible binary cyclic codes of even dimension*, in: Combinatorial Mathematics and its Applications, Proc. Second Chapel Hill Conference, May 70 (Univ. of North Carolina, Chapel Hill, N.C.,1970) pp. 100-113.

[64] P. Delsarte, J.M. Gœthals & F.J. MacWilliams *On generalized Reed-Muller codes and their relatives*, Info. and Control, 16 (1974) 403-442.

[65] Y. Desaki, T. Fujiwara & T. Kasami, *The weight distributions of extended binary BCH codes of length* 128, IEEE Transactions on Information Theory, to appear.

[66] H. Dobbertin, *Almost perfect nonlinear power functions on* $GF(2^n)$, submitted.

[67] G. Feng & K.K. Tzeng, *A new procedure for decoding cyclic and BCH codes up to actual minimum distance*, IEEE Transactions on Information Theory, vol. 40, N.5, September 94, pp. 1364-74.

[68] K.O. Geddes, S.R. Czapor & G. Labahn, *Algorithms for computer algebra*, Kluwer Academic Publishers, 1992.

[69] A. M. Gleason, *Weight polynomials of self-dual codes and the MacWilliams identities*, in: Actes Congrés International de Mathématiques, 3 1970 (Gauthier-Villars, Paris, 1971) 211-215.

[70] J.M. Gœthals, *Factorisation of cyclic codes*, IEEE Transactions on Information Theory, vol. IT-13, pp. 242-246, April 1967.

[71] J.M. Gœthals & S.L. Snover, *Nearly perfect codes*, Discrete Mathematics 3 (1972) 64-88.

[72] J.M. Gœthals & H.C.A. van Tilborg, *Uniformly packed codes*, Philips Res. Repts 30, 9-36, 1975.

[73] J.R. Griggs, *Maximum antichains in the product of chains*, Order 1(1984), 21-28.

[74] V.D. Goppa, *A new class of linear error-correcting codes*, Problemy Peredachi Informatsii 6(1970), 24-30.

[75] A.R. Hammons, Jr., P.V. Kumar, A.R. Calderbank, N.J.A. Sloane & P. Solé, *The Z_4-linearity of Kerdock, Preparata, Gœthals, and related codes*, IEEE Transactions on Information Theory, V. 40, N.2, (March 1994), pp. 301-319.

[76] H.J. Helgert & R.D. Stinaff. *Shortened BCH codes*, IEEE Transactions on Information Theory, November 1973, pp. 818–820.

[77] T. Helleseth, *On the covering radius of cyclic linear codes and arithmetic codes*, Discrete Applied Mathematics, 11(1985), pp. 157-173.

[78] T. Helleseth & P.V. Kumar, *On the weight hierarchy of the semiprimitive codes*, Discrete Mathematics 152 (1996) 185-190.

[79] T. Helleseth, T. Klove & J. Mikkeltveit, *The weight distribution of irreducible cyclic codes with block lengths $n_1((q^\ell-1)/N)$*. Discrete Mathematics 18(1977) 179-211.

[80] W.C. Huffman, *The automorphism groups of the generalized quadratic residue codes*, IEEE Transactions on Information Theory, vol. 41, N.2, March 1995, 378-386.

[81] H. Janwa & R.M. Wilson, *Hyperplane sections of Fermat varieties in P^3 in char. 2 and some applications to cyclic codes*, in Proceedings AAECC-10 (G. Cohen, T. Mora and O. Moreno Eds), LNCS 673, pp. 180-194, Springer-Verlag, New York/Berlin, 1993.

[82] H. Janwa, G. McGuire & R.M. Wilson, *Double-error-correcting codes and absolutely irreductible polynomials over GF(2)*, Journal of Algebra 178, 665-676 (1995).

[83] W.M. Kantor, *On the inequivalence of generalized Preparata codes*, IEEE Transactions on Information Theory, Vol. IT-29, N. 3, May 1983, pp. 345-348.

[84] T. Kasami, *Some lower bound on the minimum weight of cyclic codes of composite length*, IEEE Transactions on Information Theory, vol. 14, N.6, November 1968, pp. 814-818.

[85] T. Kasami, S. Lin & W.W. Peterson, *Polynomial codes*, IEEE Transactions on Information Theory, Vol. 14, N. 6, Novembre 1968, pp. 807-814.

[86] T. Kasami, *An upper bound on k/n for affine-invariant codes with fixed d/n*, IEEE Transactions on Information Theory, 15(1969) 174-176.

[87] T. Kasami, *Weight distributions of Bose-Chaudhuri-Hocquenghem Codes*, in: R.C. Bose and T.A. Dowlings, eds, Combinatorial Math. and Applications, (Univ. of North Carolina Press, Chapel Hill, NC, 1969) Ch. 20.

[88] T. Kasami, *The weight enumerators for several classes of subcodes of the 2nd order binary Reed-Muller codes*, Info. and Control, 18(1971) 369-394.

[89] T. Kasami & S. Lin. *Some results on the minimum weight of primitive BCH codes*, IEEE Transactions on Information Theory, November 1972, pp. 824–825.

[90] T. Kasami, S. Lin & W.W. Peterson *Some results on cyclic codes which are invariant under the affine group and their applications*, Info. and Control, vol. 11, pp. 475-496 (1967).

[91] T. Kasami, S. Lin & W.W. Peterson *New generalisations of the Reed-Muller codes. Part I: Primitive codes*, IEEE Transactions on Information Theory, vol. IT-14, pp. 189-199 (1968).

[92] T. Kasami, N. Tokura, *On the weight structure of Reed-Muller codes*, IEEE Transactions on Information Theory, Vol. IT-16, N.6, Novembre 1970, pp. 752-825.

[93] T. Kasami & N. Tokura, *Some remarks on BCH bounds and minimum weights of binary primitive BCH codes*, IEEE Transactions on Information Theory, vol. 15, N. 3, May 1969, pp. 408–413.

[94] G. Lachaud & J. Wolfmann, *The weights of the orthogonals of the extended quadratic binary Goppa codes*, IEEE Transactions on Information Theory, 36(1990) 686-692.

[95] P. Langevin, *A new class of two weight codes*, Proceedings of Finite Fields and Applications (third conference), Glasgow, Grande Bretagne, London Mathematical Society, Lecture Series 233, Cambridge University Press, pp. 181-187 (1996).

[96] P. Langevin & J.P. Zanotti, *Linear codes with balanced weight distribution*, Applied Algebra in Engineering Communication and Computing, vol.6, 299-307 (1995).

[97] F. Laubie, *Codes ideaux de certaines algèbres modulaires et ramification*, Communications in Algebra, 15(5), 1001-1016 (1987).

[98] D. Lazard, *Systems of algebraic equations (algorithms and complexity)*, Proceedings of Cortona Conference, University of Carolina Press, 1993.

[99] J.S. Leon, J.M.Masley & V. Pless, *Duadic codes*, IEEE Transactions on Information Theory, vol. IT-30, 1984, 709-714.

[100] F. Levy-dit-Vehel, *Divisibilité des codes cycliques: Applications et prolongements*, Thèse de l'Université Paris 6, 1994.

[101] F. Levy-dit-Vehel, *Bounds on the minimum distance of the duals of extended BCH codes over F_p* : Applied Algebra in Engineering Communication and Computing, vol.6 n^0 3, pp.175-190, 1995, Springer-Verlag.

[102] R. Lidl & H. Niederreiter, *Finite Fields*, Encyclopedia of mathematics and its applications 20, Cambridge University Press, Second edition, 1997.

[103] S. Lin & E.J. Weldon, *Further results on cyclic product codes*, IEEE Transactions on Information Theory, vol. IT-16, N. 4, pp. 452-459, July 1970.

[104] R.J. McEliece, *Quadratic forms over finite fields and second order Reed-Muller codes*, JPL Space Programs Summary, 37-58-III (1969) 28-33.

[105] R.J. McEliece, *Weight congruence for p-ary cyclic codes*, Discrete Mathematics 3(1972) 177-192.

[106] R.J. McEliece & H. Rumsey, *Euler products, cyclotomy and coding*, J. Number Theory, Vol. 4, N. 3, pp. 302-311, June 1972.

[107] R.J. McEliece, *A public-Key cryptosystem based on algebraic coding theory*, DSN Progress Report 42-44, Jet Propulsion Laboratory 1978, pp114-116.

[108] R.J. McEliece, *Irreducible cyclic codes and Gauss sums*, in: M. Hall, Jr and J.H. van Lint, eds, "Combinatorics", (Reidel, Dordrecht, 1975) pp. 185-202.

[109] R.J. McEliece & D.V. Sarwate, *On Sharing secrets and Reed-Solomon codes*, Commun. of the ACM, 24:583-584, 1981.

[110] F.J. MacWilliams & J. Seery, *The weight distributions of some minimal cyclic codes*, IEEE Transactions on Information Theory, Vol. IT-27, N.6, November 1981, pp. 796-806.

[111] F.J. MacWilliams & N.J.A. Sloane *The theory of Error Correcting Codes*, North-Holland 1986.

[112] J.P. Martin, *Codes et suites à racines multiples*, Thèse de l'Université de Toulon et du Var, January 1994.

[113] J.P. Martin, *Construction of the best binary cyclic codes of even length*, EUROCODE' 92, CISM Courses and Lectures n° 338, 65-76, Springer-Verlag, Wien - New-York.

[114] J.L. Massey, D.J. Costello, Jr., & J. Justesen, *Polynomial weights and code construction*, IEEE Transactions on Information Theory, Vol. IT-19, N.1, January 1973, pp. 101-110.

[115] J.L. Massey & T. Schaub, *Linear complexity in coding theory*, in Coding theory and Applications, LNCS vol.311, pp. 19-32, Springer-Verlag 1988.

[116] J.L. Massey, *Minimal codewords and secret sharing*, Proceedings of the 6th Joint Swedish-Russian International Workshop on Information Theory 1993, pp. 276-279.

[117] J.L. Massey, *Some applications of coding theory in cryptography*, in "Codes and Ciphers: Cryptography and Coding IV" (Ed. P.G. Farell), Essex, England: Formara Ltd., 1995, pp.33-47.

[118] M. Matsui, *Linear cryptanalysis method for DES cipher*, EUROCRYPT'93 Advances in Cryptography, Lecture Notes in Computer Science 765, p. 386-397 (1994).

[119] A.A. Nechaev, *Kerdock code in a cyclic form*, Discrete Math. Appl., Vol.1, N.4, pp. 365-384 (1991).

[120] G. Pasquier, *The binary Golay code obtained from an extended cyclic code over F_8*, European Journal of Combinatorics, vol 1,pp. 369-370, 1980.

[121] G. Pasquier, *A binary extremal doubly even self-dual code* $[64, 32, 12]$ *obtained from an extended Reed-Solomon code over F_{16}*, IEEE Transactions on Information Theory, Vol. IT-27, N. 6, November 1981, pp. 807-808.

[122] R.L. Pele, *Some remarks on the vector subspaces of a finite field*, AF Cambridge Research Labs., Bedford, Mass., Scientific Rept, AFCRL-66-477.

[123] W.W. Peterson & E.J. Weldon, Error-Correcting Codes,, MIT Press, 1961.

[124] V. Pless, *Power moment identities on weight distributions in error-correcting codes*, Info. and Control, 6(1963) 147-152.

[125] J.C.C.M. Remijn & H.J. Tiersma, *A duality theorem for the weight distribution of some cyclic codes*, IEEE Transactions on Information Theory, Vol. 34, n. 5, September 1988, pp. 1348-1351.

[126] F. Rodier, *On the spectra of the duals of binary BCH codes of designed distance $\delta = 9$*, IEEE Transactions on Information Theory, 38(1992) 478-479

[127] T. Schaub, *A linear complexity approach to cyclic codes*, Dissertation, Swiss Federal Institute of Technology, Zuerich 1988.

[128] J. Seberry, X. Zhang & Y. Zheng, *Nonlinearly balanced boolean functions and their propagation characteristics*, Proceedings of CRYPTO"93, Advances in Cryptology, LNCS, n° 773, 49-60.

[129] N. V. Semakov & V. A. Zinoviev, *Balanced codes and tactical configurations*, Problems of Info. Trans., 5(3)(1969) 22-28.

[130] N.V. Semakov, V.A. Zinoviev & G.V. Zaitsev, *Uniformly packed codes*, Problems of Information Transmission, vol. 7, No 1, pp. 38-50. 1971.

[131] K.K. Shen, C. Wang, K.K. Tzeng & B.Z. Shen, *Generation of matrices for determining minimum distance and decoding of cyclic codes*, IEEE Transactions on Information Theory, vol. 42, N. 2, March 1996, pp. 653-657.

[132] N.J.A. Sloane & J.G. Thompson, *Cyclic self-dual codes*, IEEE Transactions on Information Theory, Vol. IT-29, N. 3, May 1983, pp. 364-366.

[133] A.B. Sorensen, *Projective Reed-Muller codes*, IEEE Transactions on Information Theory, vol. 37, N. 6, November 1991, pp. 1567-1576.

[134] H. Stichtenoth, *Which extended Goppa codes are cyclic*, Journal of Combinatorial theory, Series A 51, 205-220 (1989).

[135] T. Sugita, T. Kasami & T. Fujiwara, *The weight distribution of the third order Reed-Muller code of length* 512, IEEE Transactions on Information Theory, Vol. 42, N. 5, September 1996, pp. 1622-25.

[136] A. Tietäväinen, *On the covering radius of long binary BCH codes*, Discrete Applied Mathematics 16(1987), pp. 75-77.

[137] J.A. Thiong-Ly, *Automorphisms of two families of extended non binary cyclic Goppa codes*, LNCS Vol.229, pp. 112-121, Springer-verlag, New-York/Berlin, 1985.

[138] M. van der Vlugt, *The true dimension of certain binary Goppa codes*, IEEE Transactions on Information Theory, Vol. 36, N. 2, March 1990, pp. 397-398.

[139] J.H. van Lint, *Introduction to Coding Theory*, Graduate Texts in Math. Vol.86,, Springer-Verlag, Berlin/Heidelberg/New-york, 1982.

[140] J.H. van Lint, *Repeated-root cyclic codes*, IEEE Transactions on Information Theory, Vol-37, N. 2, March 1991, pp. 343-345.

[141] J.H. van Lint & R.M. Wilson, *On the minimum distance of cyclic codes*, IEEE Transactions on Information Theory, 32(1):23, January 1986, pp. 23-40.

[142] J.H. van Lint & R.M. Wilson, *Binary cyclic codes generated by* m_1m_7, IEEE Transactions on Information Theory, 32(2):283, March 1986, p. 283.

[143] H.C.A. van Tilborg, *On weights in codes*, Report 71-WSK-03, Department of Mathematics, Technological University of Eindhoven, Netherlands, December 1971.

[144] M. van der Vlugt, *Non-BCH triple-error-correcting codes*, IEEE Transactions on Information Theory, Vol. 42, No. 5, September 1996, pp. 1612-1614.

[145] P. Véron, *Goppa Codes and Trace Operator*, IEEE Transactions on Information Theory, to appear, January 1998.

[146] J. Wolfmann, *New bounds on cyclic codes from algebraic curves*, in Lecture Notes in Computer Science, vol.388,p.47-62, Springer-Verlag 1989.

[147] J. Wolfmann, *The weights of the dual of the Melas code over* $GF(3)$, Discrete Mathematics, Vol. 74, 1989, pp. 327-329.

[148] J. Wolfmann, *The number of solutions of certain diagonal equations over finite fields*, J. of Number Theory, vol. 42, pp. 247-257, 1992.

[149] J. Wolfmann, *New results on diagonal equations over finite fields from cyclic codes*, AMS publication, Contemporary Mathematics, vol. 168, 1994, pp. 387-395.

[150] J. Wolfmann, *Weight distribution of some binary primitive cyclic codes*, IEEE Transactions on Information Theory, Vol. 40, N0 6, November 1994, pp. 2068-71.

[151] G.V. Zaitsev, V.A. Zinoviev & N.V. Semakov, *On duality of Preparata and Kerdok codes*, Proceedings of the Fifth All-Union Conference on Coding Theory, Part 2, Moscow-Gorkyi, 1972, pp. 55-58.

[152] J.P. Zanotti, *Codes à distribution de poids equilibrée*, Thèse de l'Université de Toulon et du Var, January 1995.

[153] J.P. Zanotti, *Automorphism Groups of BWD codes*, Journal of Combinatorial Theory, Series A, Vol. 78, No 2, May 1997, pp. 303-308.

[154] K.H. Zimmermann, *On generalizations of repeated-root cyclic codes*, IEEE Transactions on Information Theory, vol.42, N. 2, March 1996, pp. 641-649.

Index

p-ary.RM code, 18

affine-invariant code, 16, 68
affine.polynomial, 40
almost bent.function, 71
almost perfect nonlinear.function, 71
alternant code, 70, 80
antichain, 17
asymptotically good.cyclic code, 69
automorphism group of.cyclic code, 68

BCH bound, 19, 38, 45
BCH code, 2, 11, 50, 75, 76, 78
Boolean function, 71
border of.affine-invariant code, 17
border of.RS code, 18

Carlitz-Ushiyama.bound, 45, 48
codeword of.BCH code, 38
completely regular.code, 81
cryptographic primitive, 71
cryptography, 70
cyclic code, 2, 3
cyclic.Goppa code, 76

defining set of.cyclic code, 5
diagonal equation, 14
divisibility of.cyclic code, 49, 50, 66
double-error-correcting.BCH code, 81

elementary symmetric function, 27
equivalent.cyclic code, 69

Fourier transform, 3, 5

generalized.Newton identities, 27, 30
generalized.Reed-Muller code, 2, 11
generalized.RS code, 80
generator system.affine-invariant code, 21
Goppa code, 74
group algebra.code, 3

Hartmann–Tzeng bound, 56

idempotent, 36
irreducible cyclic code, 68
irreducible.cyclic code, 14, 64

Kerdock code, 80
Kloosterman sum, 66

linear.polynomial, 40
locator, 26
locator polynomial, 27, 41, 78

Mattson-Solomon.polynomial, 3, 5, 76, 83
McEliece cryptosystem, 70, 74
Melas code, 55, 66
minimal.polynomial, 37
minimum distance.BCH code, 40, 45
minimum weight codeword.GRM code, 41, 43

Newton identities, 26, 28
non linear.affine-invariant codes, 69
non linear.cyclic code, 68

Pless power moments, 56
polynomial.code, 3
poset of.affine-invariant code, 17
power sum function, 27
Preparata code, 80

primitive form of.cyclic code, 14
primitive.cyclic code, 3, 12
projective.GRM code, 54

quadratic residue code, 2, 11, 33, 68, 70
quasi-cyclic.Goppa code, 77

radical, 21
rank-bounding.algorithm, 49
Reed-Muller code, 51, 70, 83
Reed-Solomon code, 2, 11, 23
repeated-root.cyclic code, 3, 5, 69

self-dual.affine-invariant code, 23, 25
self-dual.cyclic code, 12
self-dual.Reed-Muller code, 24, 51
self-orthogonal.cyclic code, 20
sequences, 55
size.affine-invariant code, 21
splitting field, 36

two-weights.cyclic code, 66

uniformly packed.code, 81

weight enumerator.BCH code, 49
weight enumerator.cyclic code, 49
Weil bound, 48, 50, 55
with two zeros.cyclic code, 54, 71, 81