On duals of binary primitive BCH codes

Françoise Levy-Dit-Vehel

INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

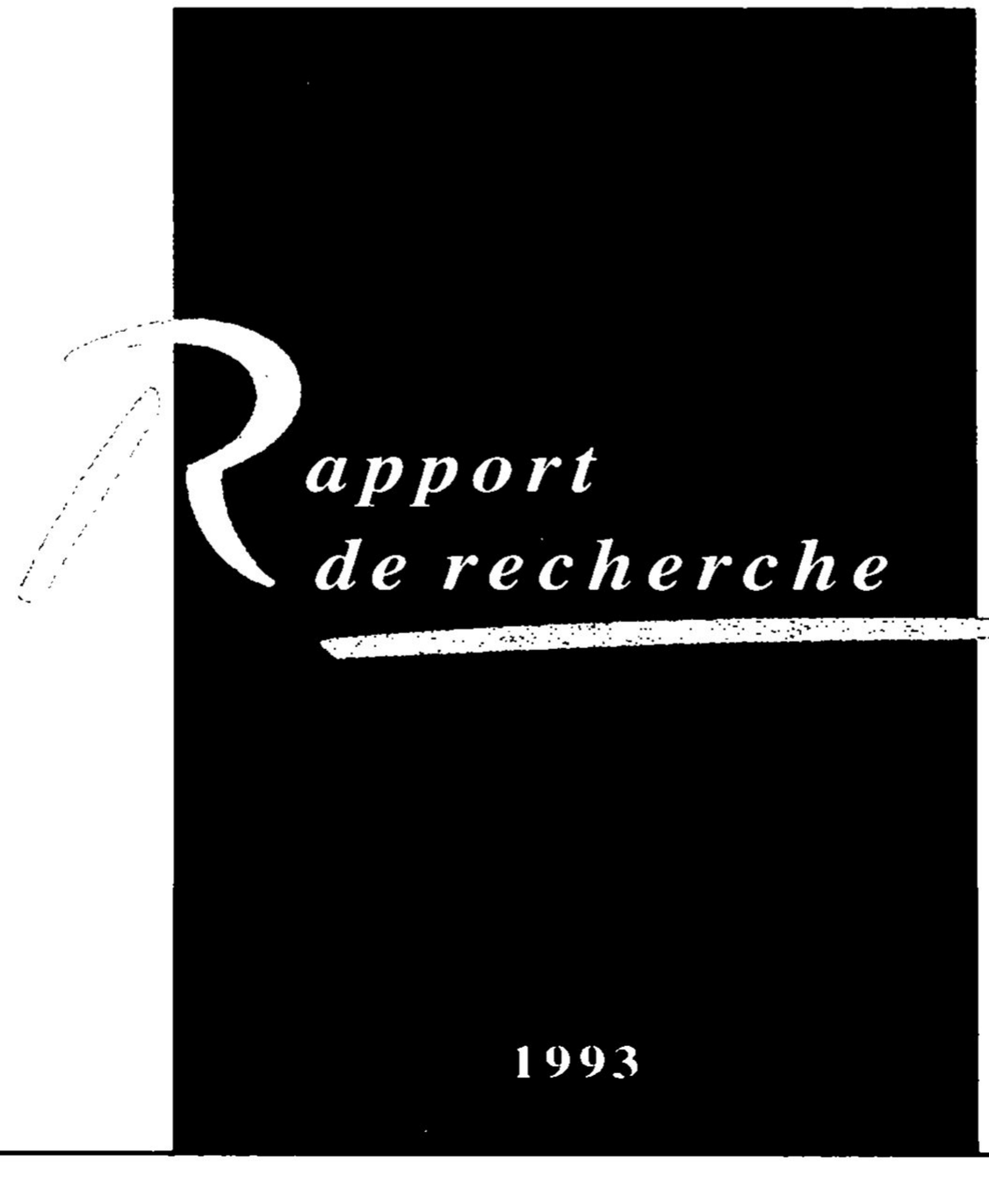
On duals of binary primitive BCH codes

Françoise LEVY-dit-VEHEL

N° 1835
Janvier 1993

PROGRAMME 2

Calcul Symbolique,
Programmation
et Génie lociciel



Sur des duaux de codes BCH primitifs binaires
On duals of binary primitive BCH codes

Françoise Levy-dit-Vehel *

Résumé

Nous nous plaçons dans le cadre des codes cycliques étendus de longueur 2^m sur $\mathbf{F}_2$. Nous définissons une classe, notée $\{C^{(t)}\}_{2\leq t\leq m-1}$, de tels codes, dont l'ensemble de définition est caractérisé par une seule classe cyclotomique. Nous montrons que ce sont des duaux de codes BCH étendus. Nous étudions leur divisibilité, et prouvons qu'elle détermine la divisibilité de tous les duaux de codes BCH étendus. Ensuite, nous obtenons une borne inférieure sur leur distance minimale, qui s'applique à d'autres codes affine-invariants. En particulier, on obtient une borne pour tous les duaux des BCH étendus, qui est intéressante surtout quand la borne de Carlitz-Uchiyama est négative.

Abstract

We treat binary extended cyclic codes of length 2^m over $\mathbf{F}_2$. We introduce a class, denoted by $\{C^{(t)}\}_{2\leq t\leq m-1}$, of such codes, whose defining set is characterized by only one cyclotomic coset. We prove that they are duals of extended BCH codes. We study the divisibility of the $C^{(t)}$'s, and show that it determines the divisibility of all duals of extended BCH codes. Next we obtain a lower bound on their minimum distance, that yields results for several affine-invariant codes. In particular, it gives a bound for all duals of extended BCH codes, which is interesting especially when the Carlitz-Uchiyama bound is negative.

*Institut National de Recherche en Informatique et Automatique (INRIA) Domaine de Voluceau, Rocquencourt, BP 105, 78153 Le Chesnay Cedex FRANCE

1 Preliminaries

A binary cyclic code C of length $n = 2^m - 1$ is an ideal in the ring $\mathsf{F}_2[Z]/(Z^n - 1)$. Let α be a primitive root in F_{2^m}. Then, if $g(Z)$ is the generator polynomial of C, α^i is a zero of the code C if, and only if, $g(\alpha^i) = 0$. The set $T = \{i \in [0, n],\ \alpha^i \text{ is a zero of } C\}$, is the defining set of C. If $0 \notin T$, we can extend C and obtain a linear code C_e of length 2^m, so-called the extension of C, by adding a parity check symbol to each word of C:

$$c \in C,\ c = (c_0, \ldots, c_{n-1}) \Longleftrightarrow c' \in C_e,\ c' = (c_\infty, c_0, \ldots, c_{n-1}) \text{ where } c_\infty = \sum_{i=0}^{n-1} c_i.$$

The code C_e can be considered as a code of the group algebra $\mathcal{A} = \mathsf{F}_2[\{\mathsf{F}_{2^m}, +\}]$, which is the set of formal polynomials $x = \sum_{g \in \mathsf{F}_{2^m}} x_g X^g,\ x_g \in \mathsf{F}_2$.
And this because a word $c' = (c_\infty, c_0, \ldots, c_{n-1})$ in C_e can be represented by the polynomial

$$c'(X) = c_\infty X^0 + \sum_{i=0}^{n-1} c_i X^{\alpha^i}.$$

We say that $T_e = T \cup \{0\}$ is the defining set of C_e.
Recall that the BCH code of length n and designed distance d over F_2 is the cyclic code with defining set : $T(d) = \cup_{1 \leq s < d} cl(s)$, where $cl(s)$ is the cyclotomic coset of 2 modulo n containing s. We denote by $B(d)$, $EB(d)$, and $DEB(d)$ respectively the BCH code of designed distance d, its extension, and the dual of this extension.
We let w denote the Hamming weight of a vector of length n or $n + 1$, that is, the number of its non-zero components.

Definition 1 *Let $S = [0, n]$. The 2-ary expansion of an element $s \in S$ is : $s = \sum_{i=0}^{m-1} s_i 2^i$, $s_i \in \{0, 1\}$. We denote by $\ll$, the partial order on S defined as follows:*

$$s, t \in S,\ s \ll t \Longleftrightarrow s_i \leq t_i,\ i \in [0, m-1]$$

When $s \ll t$, s is said to be a descendant of t. We say that s and t are not related when $s \not\ll t$ and $t \not\ll s$. An antichain of $(S, \ll)$ is a subset of S of not related elements.
Let Δ be the map :

$$\Delta :\ I \subset [0, n] \mapsto \Delta(I) = \cup_{t \in I} \{s \in S,\ s \ll t\} = \cup_{t \in I} \Delta(\{t\})$$

$\Delta(\{t\})$ will often simply be denoted by $\Delta(t)$.
A code of the algebra $\mathcal{A}$ (ie. a F_2-subspace of $\mathcal{A}$), is called affine-invariant if its automorphism group contains the group $\mathrm{GA}(m)$ of affine permutations of F_{2^m} :

$$p_{u,v} : \sum_{g \in \mathsf{F}_{2^m}} x_g X^g \to \sum_{g \in \mathsf{F}_{2^m}} x_g X^{ug+v},\ u, v \in \mathsf{F}_{2^m},\ u \neq 0$$

Theorem 1 *([Ka,Li,Pe 2],[Ch.1]) Let C_e be an extended cyclic code of $\mathcal{A}$, with defining set T_e. Then, C_e is affine-invariant if, and only if :*
$\Delta(T_e) = T_e$, or C_e is an ideal of $\mathcal{A}$.

An element s is maximal (resp. minimal) in I if its strict majorants (resp. minorants) are not in I.

Definition 2 *([Ch.1],[Ch.2]) If C_e is an extended cyclic code with defining set T_e, the border of C_e is the set of minimal elements of $[0,n] \setminus T_e$.*

Note : Let C_e be an affine-invariant code with border F. Then the set $\{n-f,\ f \in F\}$ is the set of maximal elements of the defining-set of the dual of C_e [Ch.1].
Let C be a binary cyclic code and C_e its extension. Denote by d_{min}, d_{odd}, and d_{even}, respectively the minimum weight, the minimum odd weight, and the minimum even weight of C. If C_e is affine-invariant, then $d_{min} = d_{odd} = d_{even} - 1$.

A binary linear code C is said to be k-divisible, $k > 1$, if the weights of all its words are divisible by k, and if there exists a word of C whose weight is not divisible by $l > k$. If $2 \not| k$, then the code is equivalent to a degenerate code (in which every symbol is repeated k times) [Wa]. We thus consider the case $k = 2^a,\ a \in \mathbf{N}^*$.
The divisibility of RM-codes is known [Mc El]. For every extended cyclic code can be located among the RM-codes, it has at least the divisibility of the smallest RM-code it is included in. We shall call this divisibility the minimum divisibility of the code.
We recall the theorem of Mac Eliece, adapted here to the context of binary extended cyclic codes :

Theorem 2 *: Let C_e be an extended cyclic code of length 2^m over $\mathbf{F}_2$, with defining set T. Then, C_e is 2^λ-divisible, where $\lambda = \omega - 1$, and*

$$\omega = min\{r,\ \prod_{i=1} \alpha^{u_i} = 1,\ u_i \in [0,n[\setminus T\}$$

α being a primitive root in $\mathbf{F}_{2^m}$.

2 A class of duals of primitive extended BCH codes

We are studying a class of primitive extended cyclic codes over $\mathbf{F}_2$, defined as follows :

Definition 3 *Let $n = 2^m - 1$ and $t \in [2, m-1]$.*
The $C^{(t)}$ code is the affine-invariant code of length 2^m, whose border is $F_t = cl(2^t - 1)$.

Proposition 1 *The defining set of $C^{(t)}$ is $D_t = \{u \in [0,n],\ u$ has no run of t consecutive ones$\}$*

Note : An element $x \in [0,n]$ has a run of t consecutive ones if, and only if, a cyclic shift of x has a run of t consecutive ones. For instance, $(110\ldots0\underbrace{1\ldots1}_{t-2}) \in cl(2^t-1)$ is such an element.

Proof . If F denotes the border of an affine-invariant code, its defining set is given by

$$I = \bigcap_{f \in F} N(f)$$

where $N(f) = \{s \in S,\ s \neq f,\ s \ll f$ or s and f are not related$\}$, is the set of non-majorants of f in S.
So the defining set of $C^{(t)}$ is :

$$D_t = \cap_{f \in cl(2^t-1)} N(f) = \cap_{f \in cl(2^t-1)} \{u \in [0,n] \setminus \{f\},\ u \ll f \text{ or } f \text{ and } u \text{ are not related}\}$$

Let $s_t = 2^t - 1$. $s_t = (0 \ldots 0 \underbrace{1 \ldots 1}_{t})$ and $w(s_t) = t$.

Let $u \in \cap_{f \in cl(s_t)} N(f)$. Then, if $u \ll f,\ u \neq f\ for all f in F_t$, we have $w(u) < t$.
If u and f are not related, for all f in F_t, then u has not t consecutive ones. Indeed, if

$$u = (\epsilon \ldots \epsilon \underbrace{1 \ldots 1}_{t} \underbrace{\epsilon \ldots \epsilon}_{z})$$

where $\epsilon \in \{0,1\}$, then $2^z s_t$ is a descendant of u.
Moreover, $w(u) < t \Rightarrow u$ has not t consecutive ones.
So $D_t \subset \{u \in [0,n],\ u$ has not t consecutive ones$\}$.
Conversely, if $u \in [0,n]$ has not t consecutive ones, then either $w(u) < t$, or u is unrelated with every element of F_t, so u belongs to D_t. Thus,

$$D_t = \{u \in [0,n],\ u \text{ has not } t \text{ consecutive ones}\}$$

□

We denote by $\lceil x \rceil$, (resp. $\lfloor x \rfloor$), the least (largest) integer greater (smaller) than or equal to x.

Theorem 3 *The code $C^{(t)}$ is the dual of an extended BCH code. More precisely, $C^{(t)} = DEB(d_t)$, where d_t is the smallest element of $[0,n]$ having no run of t consecutive zeroes.*
If $t < \lceil \frac{m}{2} \rceil$, then $d_t = \sum_{i=1}^{a} 2^{m-it} + (1 - \delta_{r,0})$, where $m = at + r,\ r < t$.
If $t \geq \lceil \frac{m}{2} \rceil$, $d_t = 2^{m-t} + 1$

Proof . We identify an element s in $[0,n]$ with its binary representation $(s_{m-1}, \ldots, s_0)$, where $s = \sum_{i=0}^{m-1} s_i 2^i$. First, if $t \geq \lceil \frac{m}{2} \rceil$, then $m - t \leq \lfloor \frac{m}{2} \rfloor \leq t$, and so

$$2^{m-t} + 1 = (\underbrace{0 \ldots 0}_{t-1} 1\ \underbrace{0 \ldots 0}_{m-t-1<t}\ 1)$$

is the smallest element of $[0,n]$ having no run of t consecutive zeroes.
If $t < \lceil \frac{m}{2} \rceil$, let $m = at + r,\ r < t$; (Note that in this case, $a \geq 2$). Then, the element

$$(\overbrace{0 \ldots 0}^{t-1} 1 \ldots \overbrace{0 \ldots 0}^{t-1} 1 \underbrace{0 \ldots 01}_{r<t})$$
$$\underbrace{\qquad\qquad\qquad\qquad}_{a \text{ blocks}}$$

is the smallest element of $[0, n]$ having no run of t consecutive zeroes.
Besides, we clearly have :

$$2^{m-t} - 1 < d_t$$

$d_t - (2^{m-t} - 1) = \sum_{i=1}^{a} 2^{m-it} + (1 - \delta_{r,0}) - (2^{m-t} - 1) \geq \sum_{i=2}^{a} 2^{m-it} + 1 > 0.$

To prove the theorem, it suffices to show that the defining set, say $D_t^{\perp}$, of the dual of $C^{(t)}$, is the defining set of the extended BCH code of designed distance d_t, that is :

$$D_t^{\perp} = \cup_{s<d_t} cl(s)$$

$D_t^{\perp} = \{n - s,\ s \notin D_t\} = \{n - s, s$ has at least t consecutive ones$\}$, or :
$D_t^{\perp} = \{u \in [0, n],\ u$ has at least t consecutive zeroes$\}$.
Recall that $\{n - f,\ f \in F_t\} = cl(2^{m-t} - 1)$, is the set of maximal elements of $D_t^{\perp}$. It means that the maximal elements of $D_t^{\perp}$ are those having exactly t consecutive zeroes. Thus we immediately have :

$$D_t^{\perp} \supset \cup_{0 \leq s \leq 2^{m-t}-1} cl(s).$$

Moreover, $D_t^{\perp}$ cannot contain a class with smallest element strictly larger than $2^{m-t} - 1$, because it would also be a maximal element of $D_t^{\perp}$. Thus, $D_t^{\perp}$ is the defining-set of an extended BCH code. Its designed distance is the smallest element which is both the smallest element of its cyclotomic coset, and strictly greater than $2^{m-t} - 1$, that is, the smallest element not having t consecutive zeroes. Thus, $D_t^{\perp} = \cup_{0 \leq s < d_t} cl(s)$. □

Proposition 2 *For* $t \geq \lceil \frac{m}{2} \rceil$, $dim\, C^{(t)} = m\, 2^{m-t-1} + 1$.
For $t < \lceil \frac{m}{2} \rceil$, *we deduce from [Ma] that :*

$$dim\, C^{(t)} = m \sum_{k=1}^{\lfloor \frac{m}{t+1} \rfloor} \frac{(-1)^{k-1}}{k} \begin{pmatrix} m - kt - 1 \\ k - 1 \end{pmatrix} 2^{m-k(t+1)} + 1$$

Proof . • $t \geq \lceil \frac{m}{2} \rceil$.
According to theorem 1, $C^{(t)} = DEB(2^{m-t} + 1)$, with $m - t \leq \lfloor \frac{m}{2} \rfloor$.
$dim C^{(t)} = |\cup_{1<s<2^{m-t}+1} cl(s)| = |D_t^{\perp}|$.
But for $s < 2^{\lceil \frac{m}{2} \rceil} + 1$, s odd, the cyclotomic cosets of 2 modulo n containing s are all distinct and of cardinal m. (see [Sl], p. 262). Moreover, there are 2^{m-t-1} cyclotomic cosets whose smallest element is strictly less than $2^{m-t} + 1$. Besides, 0 belongs to $D_t^{\perp}$.
Thus,

$$dim\, C_t = m\, 2^{m-t-1} + 1$$

• $t < \lceil \frac{m}{2} \rceil$.
$dim\, C_t = |D_t^{\perp}|$. In the proof of theorem 1, we saw that $cl(2^{m-t} - 1)$ is the set of maximal elements of $D_t^{\perp}$. So we have

$$|D_t^{\perp}| = |\cup_{i=0}^{m-1} \Delta^*(2^i(2^{m-t} - 1)\, mod\, n) \cup \{0\}|$$

where $\Delta^*(s)$ is the set of descendants of s except 0. As $2^i(2^{m-t} - 1)\, mod\, n$ has in its binary representation t consecutive zeroes, a nonzero descendant, say s, of $2^i(2^{m-t} - 1)\, mod\, n$ must

have in its binary representation a '1' followed circularly by t '0'; that means, if we write the digits of s in a circle, there must have a one followed by t '0''s. We call *pattern*, a '1' followed circularly by t zeroes. Conversely, if s has a pattern in its binary representation, it is a descendant of an element of the form $2^i(2^{m-t}-1) \, mod \, n$.
We have thus proved :

$$|\cup_{i=0}^{m-1} \Delta^*(2^i(2^{m-t}-1) \, mod \, n)| = |\{\text{strings of length } m \text{ having at least one pattern }\}|$$

In a string of length m, there is $\lfloor \frac{m}{t+1} \rfloor$ blocks of length $t+1$.
Let $A_k = \{$ strings containing k patterns $\}$, for $1 \leq k \leq \lfloor \frac{m}{t+1} \rfloor$. According to the inclusion-exclusion principle, we have :

$$|\cup_{i=1}^{\lfloor \frac{m}{t+1} \rfloor} A_i| = |A_1| - |A_2| + \ldots + (-1)^{\lfloor \frac{m}{t+1} \rfloor} |A_{\lfloor \frac{m}{t+1} \rfloor}|$$

And $|\cup_{k=1}^{\lfloor \frac{m}{t+1} \rfloor} A_k|$ is the number of strings having at least one pattern.
Computation of the $|A_k|$'s :
$|A_1|$ is the number of strings having one pattern.
In a string containing one fixed pattern, there are two ways of choosing each of the remaining $m-t-1$ digits. So the number of strings containing one fixed pattern is 2^{m-t-1}. Besides, this pattern can be put in m positions. So the number of strings having any pattern is $m \, 2^{m-t-1} = |A_1|$.
Computation of the $|A_k|$'s, for $2 \leq k \leq \lfloor \frac{m}{t+1} \rfloor$.
We have to count the number of strings having k patterns. Let us fix the position of the first pattern (this position can be fixed in m ways).
Placing the other $(k-1)$ patterns amounts to placing the first element (a '1') of each pattern. And once we have placed the first digit of a pattern, the following t positions are reserved (by zeroes). So the number of ways of placing the other $(k-1)$ patterns is the number of choosing $(k-1)$ positions (the first of each pattern) out of $m-(t+1)-(k-1)t = m-kt-1$. Moreover, once these k patterns settled, it remains $m-k(t+1)$ positions that can be filled by zeroes or ones, that makes $2^{m-k(t+1)}$ possibilities. Noticing that each of the k patterns can play the role of the first one, we have to divide the number of strings obtained by k.
Thus :

$$|A_k| = \frac{m}{k} \begin{pmatrix} m-kt-1 \\ k-1 \end{pmatrix} 2^{m-k(t+1)}$$

and finally :

$$|\cup_{k=1}^{\lfloor \frac{m}{t+1} \rfloor} A_k| = m \sum_{k=1}^{\lfloor \frac{m}{t+1} \rfloor} \frac{(-1)^{k-1}}{k} \begin{pmatrix} m-kt-1 \\ k-1 \end{pmatrix} 2^{m-k(t+1)}$$

□

Example :
Let $m = 8, \; t = 3$.
$C^{(3)}$ is the affine-invariant code with border

$$F_3 = cl(7) = \{7, 14, 28, 56, 112, 224, 193, 131\}$$

It is the dual of the extended BCH code with designed distance

$$d_3 = \sum_{i=1}^{2} 2^{8-3i} + (1 - \delta_{2,0}) = 37.$$

The corresponding defining-set D_3 is the union of the following cyclotomic cosets :

$$\{0\},\ cl(1),\ cl(3),\ cl(5),\ cl(9),\ cl(13),\ cl(17),\ cl(19),$$

$$cl(21)\ , cl(25),\ cl(27),\ cl(37),\ cl(43),\ cl(45),\ cl(51),$$

$$cl(53),\ cl(85),\ cl(91)$$

That corresponds to all elements of $[0, n]$ having not 3 consecutive ones in their binary representation. The dimension of the code is 125.

3 A bound on the minimum distance of $C^{(t)}$:

We denote by $RM(r, m)$ (or simply $RM(r)$ when there cannot be any ambiguity on m), the Reed-Muller code of length 2^m and order r, that is, the code with defining-set $\{s \in [0, n],\ \omega_2(s) < m - r\}$, where $\omega_2(s)$ is the 2-weight of the element s written in binary, ie. $\omega_2(s) = \sum_{i=0}^{m-1} s_i$, if $s = \sum_{i=0}^{m-1} s_i 2^i$. Since $C^{(t)} \subset RM(m - t)$, we immediately have $d_{min} C^{(t)} \geq 2^t$. But we shall see that, for almost all t's in the range $[2, m - 1]$, we can refine this bound.

lemma 1 *Let C be an affine-invariant code of length $n+1$, with defining set I, and suppose*

$$[0, d[\subset I, \quad and \quad d \notin I$$

Then

1. Any interval included in I is of length $\leq d$.
2. If there exists s and z such that $(z, n) = 1$, and

$$[0, d[,\ [z, z + d[, \ldots,\ [(s - 1)z, (s - 1)z + d[$$

are included in I, then $d_{min} C \geq d + s$.

Proof . *1.* It suffices to show that, for all k in I, there exists an integer k' such that : $k' > k$, $k' \notin I$, and $k' - k \leq d$. Then, any interval with k as first element and incuded in I will be contained in $[k, k'[$ and thus will be of length smaller than or equal to d. Let k belong to I. If $0 \leq k < d$, then any interval included in I, with k as first element is of length less than d, because $d \notin I$. We can thus suppose $k > d$.
Write k and d in base 2 : $k = \sum_{i=0}^{m-1} k_i 2^i$, $d = \sum_{i=0}^{m-1} d_i 2^i$. As $k > d$, there exists a j such that $k_j > d_j$, $k_{j+1} \geq d_{j+1}, \ldots$. Indeed, if such a j did not exist, then k would be a descendant of d and that would imply $k \leq d$, a contradiction. Let j_0 be the minimum of those j's. Then,

$j_0 \neq 0$ otherwise k would be an ascendant of d, and, as C is affine-invariant, k would not belong to I. Let $k' = \sum_{i=0}^{j_0-1} d_i 2^i + \sum_{i=j_0}^{m-1} k_i 2^i$.
By construction, $d \ll k'$, so that $k' \notin I$. Moreover, we have $k' > k$. But

$$k' - k \leq \sum_{i=0}^{j_0-1} d_i 2^i \leq d$$

2. Let C^* be the cyclic code whose extension is C. Then, the defining-set of C^* is $I^* = I \backslash \{0\}$. Thus the following $(s-1)$ intervals belong to I^* :

$$[z, z+d[, \ldots, [(s-1)z, (s-1)z+d[$$

Recall that the Hartmann-Tzeng bound [Sl.] states that, if the elements $b + i_1 c_1 + i_2 c_2$ belong to the defining-set of a cyclic code of length n, where c_1 and c_2 are relatively prime to n, $0 \leq i_1 \leq \delta - 2$ and $0 \leq i_2 \leq r$, then the minimum distance of the code is at least $\delta + r$. We can apply this bound to I^*, with $c_1 = 1$, $c_2 = z$, $b = z$, $\delta = d+1$, $r = s-2$. We obtain : $d_{min}(C^*) \geq \delta + r = d + 1 + s - 2 = d + s - 1$. But, as C is affine-invariant, $d_{min}(C) = d_{min}(C^*) + 1$, so that $d_{min}(C) \geq d + s$. □

Applying this lemma to the $C^{(t)}$'s, we obtain :

Theorem 4 *For $2 \leq t < m-2$, the minimum weight δ of $C^{(t)}$ satisfies: $\delta \geq 2^{t+1} - 2^{t-1}$.*

Remark :
For $t = m-2$ or $t = m-1$, $C^{(t)}$ is the dual of the extended two or one error correcting BCH code, so that the minimum weight of $C^{(t)}$ is known: It is $2^{m-1} - 2^{\lfloor \frac{m}{2} \rfloor}$ and 2^{m-1} respectively.

Proof . Let $2 \leq t < m-2$. Then, the intervals $[0, 2^t - 1[$ and $[2^{t+1}, 2^{t+1} + 2^t - 1[$ belong to the defining-set D_t of $C^{(t)}$. With $z = 2^{t+1}$ prime to n, we can apply the lemma and we find : $d_{min} C^{(t)} \geq 2^t - 1 + 2 = 2^t + 1$. For $C^{(t)} \subset RM(m-t)$, the smallest possible weight for $C^{(t)}$ is $2^{t+1} - 2^{t-1}$, according to the theorem of Kasami and al. :

Theorem 5 *[Ka, To]*
Let $N_{m,\nu,w}$, the number of codewords of weight w in the ν-th order RM-code of length 2^m. Assume that $\nu \geq 2$ and $2^{m-\nu} < w < 2^{m-\nu+1}$. Let $\gamma = min(m-\nu, \nu)$, and $\beta = (1/2)(m-\nu+2)$. Then :

$$N_{m,\nu,w} = 0, \text{ unless } w = 2^{m-\nu+1} - 2^{m-\nu+1-\mu}, \text{ with } 1 \leq \mu \leq max(\gamma, \beta)$$

In our context, $\nu = m - t$, $\gamma = t$, $\beta = (t/2) + 1$, and $1 \leq \mu \leq t$. □

We give in the appendix another proof of th.4, which uses the Newton's identities.

4 Divisibility properties

Theorem 6 *The code* $C^{(t)}$ *is* $2^{\lceil \frac{m}{m-t} \rceil - 1}$*-divisible.*

Remark : The theorem means that $C^{(t)}$ has the minimum divisibility.

Proof . $C^{(t)}$ is at least $2^{\lceil \frac{m}{m-t} \rceil - 1}$-divisible, as a subcode of RM$(m-t)$. It remains to prove that $C^{(t)}$ has exactly this divisibility.
According to the theorem of Mac Eliece, (th.2), it suffices to show that there exists $\lceil \frac{m}{m-t} \rceil$ elements of $[0, n[\setminus D_t$ whose sum is n. We distinguish two cases :
Case 1 : $t \leq \lfloor \frac{m}{2} \rfloor$:
Then $C^{(t)}$ is exactly 2-divisible because $s = 2^{\lfloor \frac{m}{2} \rfloor} - 1$ and $n - s$ belong to $[0, n[\setminus D_t$.
Case 2 : $t \geq \lceil \frac{m}{2} \rceil$:
Let $\mathcal{C}$ be the code whose defining set can be deduced from the one of $C^{(t)}$ by changing the primitive root α into $\beta = \alpha^{-1}$. Those two codes are equivalent and so have the same divisibility. The defining set of $\mathcal{C}$ is :

$$\{n - s,\ s \in D_t\}$$

And the parity set, say $\mathcal{U}$, of $\mathcal{C}$ is :

$$[0, n] \setminus \{n - s,\ s \in D_t\} = \{n - s,\ s \notin D_t\}$$

It is worth to notice here that the parity set of $\mathcal{C}$ is $D_t^{\perp}$. But $D_t^{\perp}$ admits $cl(2^{m-t} - 1)$ as maximal elements, that is :

$$D_t^{\perp} = \cup_{i=0}^{m-1} \Delta(2^i(2^{m-t} - 1))$$

So $cl(2^{m-t} - 1) \subset \mathcal{U}$.
Case 2.1 : $m - t \,|\, m$.
$m = (m-t)\,a$. Then, the a elements $2^{i(m-t)}(2^{m-t} - 1)$, $0 \leq i \leq a - 1$, belong to $\mathcal{U}$ and :

$$\sum_{i=0}^{a-1} 2^{i(m-t)}(2^{m-t} - 1) = (2^{m-t} - 1)\frac{1 - 2^m}{1 - 2^{m-t}} = n$$

Case 2.2 : $m - t \not| m$.
$m = (m-t)\,a + r$, $r < m - t$. $\lceil \frac{m}{m-t} \rceil = a + 1$. We have :

$$\sum_{i=0}^{a-1} 2^{i(m-t)}(2^{m-t} - 1) = (\underbrace{0 \ldots 0}_{r} \overbrace{\underbrace{1 \ldots 1}_{m-t} \ldots \underbrace{1 \ldots 1}_{m-t}}^{a \text{ blocks}})$$

Let

$$b = (\underbrace{1 \ldots 1}_{r} 0 \ldots 0) = 2^m - 2^{m-r}$$

b belongs to $\mathcal{U}$ because $r < m - t$ so that $b \ll 2^t(2^{m-t} - 1)$.
The $a + 1$ elements b, $2^{i(m-t)}(2^{m-t} - 1)$, $0 \leq i \leq a - 1$, belong to $\mathcal{U}$ and :

$$b + \sum_{i=0}^{a-1} 2^{i(m-t)}(2^{m-t} - 1) = b + (2^{m-t} - 1)\frac{1 - 2^{(m-t)a}}{1 - 2^{m-t}} = b - 1 + 2^{(m-t)a} = b - 1 + 2^{m-r} = n$$

There exists $\lceil \frac{m}{m-t} \rceil$ elements of the parity set of C whose sum is n. So is C $2^{\lceil \frac{m}{m-t} \rceil - 1}$-divisible, and therefore $C^{(t)}$ also. □

Corollary 1 : Divisibility of a code situated between two consecutive $C^{(t)}$'s

Let $t > 2$, and C be an affine-invariant code with defining set D, such that :

$$C^{(t)} \subseteq C \subset C^{(t-1)} \tag{1}$$

Then, C is $2^{\lceil \frac{m}{m-t} \rceil - 1}$-divisible, ie. the divisibility of C is the one of $C^{(t)}$.

1. If $2 < t < m-2$, and the elements $u_0 = 2^t + 2^{t-1} - 1$ and $v_0 = 2^{t+1} + 2^{t-1} - 1$ belong to D,

$$d_{min}(C) \geq 2^{t+1} - 2^{t-1}$$

2. If $2 < t < m-2$, and either u_0 or v_0 does not belong to D,

$$d_{min}(C) \geq 2^t$$

3. If $t = m-2$,

$$d_{min}(C) \geq 2^{m-1} - 2^{\lfloor \frac{m+2}{2} \rfloor}$$

4. If $t = m-1$, $d_{min}(C) = 2^{m-1}$.

Proof . By (1), we have :

$$D_{t-1} \subset D \subseteq D_t$$

Thus

$$D = (D_{t-1}) \cup I$$

where $I \neq \emptyset$, and $I \subset \{s \in [0, n[,\ s \text{ has } t-1 \text{ consecutive ones but not } t\}$.
We claim that $cl(2^{t-1} - 1) \subset I$:
Indeed, let $s \in I$. Then s is of the following form :

$$(\epsilon \ldots \epsilon 0 \underbrace{1 \ldots 1}_{t-1} \underbrace{0 \epsilon \ldots \epsilon}_{z})$$

where $\epsilon \in \{0, 1\}$. Then,

$$2^z(2^{t-1} - 1) \ll s$$

and as D is let fixed by the Δ map (ie. C is affine-invariant), $2^z(2^{t-1} - 1)$ belongs to D. C being a code over $GF(2)$, $cl(2^{t-1} - 1) \subset D$.
Let now $s \in [0, n[$, with $w(s) = t - 1$.
-If $s \in cl(2^{t-1} - 1)$, then $s \in I$.
-If s and $cl(2^{t-1} - 1)$ are not related (ie. $\forall u \in cl(2^{t-1} - 1), s \not\ll u$ and $u \not\ll s$), s has not $t-1$ consecutive ones, so s is in $D_{t-1} \setminus \{0\}$.
In both cases, s belongs to D, ie D contains all the elements of weight $t - 1$. But, over $\mathbb{F}_2$,

the weight coincides with the 2-weight. Thus C is necessarily a subcode of RM$(m-t)$. The exact divisibility of C follows immediately.

1. Suppose $2 < t < m-2$ and u_0, v_0 belong to D. We shall show that the intervals $[0, 2^t - 1[$ and $[2^{t+1}, 2^{t+1} + 2^t - 1[$ are included in D, and then apply lemma 1.
First, as the elements of weight less than or equal to $t-1$ all belong to D, we immediately have : $[0, 2^t - 2] \subset D$.
Now what are the elements of $[2^{t+1}, 2^{t+1} + 2^t - 1[$ that have $t-1$ consecutive ones in their binary representation? They are exactly v_0 and $2u_0$. (The other members of this interval have no $t-1$ consecutive ones, so that they belong to $D_{t-1} \subset D$.) As v_0 and u_0 belong to D, $cl(u_0)$ and $cl(v_0)$ also, and thus $[2^{t+1}, 2^{t+1} + 2^t - 1[\subset D$. By the same reasoning as in the proof of theorem (4), we conclude that the minimum weight of C is at least $2^{t+1} - 2^{t-1}$.

2. Suppose $2 < t < m-2$ and either one or both u_0 and v_0 do not belong to D. Then $[2^{t+1}, 2^{t+1} + 2^t - 1[$ is not a subset of D, and it is easy to see that there are no intervals of length $2^t - 1$ included in D except $[0, 2^t - 1[$. Thus applying lemma 1 does not give a better estimate than the one we have by inclusion of C in RM$(m-t)$.

3. If $t = m-2$, then (1) implies that the defining-set, say $D^\perp$, of $C^\perp$ is such that

$$\{0\} \cup cl(1) \cup cl(3) \subseteq D^\perp \subset \{0\} \cup cl(1) \cup cl(3) \cup cl(5) \cup cl(7)$$

But, as C is affine-invariant, we can only have two possibilities for $D^\perp$, namely :
$D^\perp = \{0\} \cup cl(1) \cup cl(3)$, in which case $C = DEB(5)$, or,
$D^\perp = \{0\} \cup cl(1) \cup cl(3) \cup cl(5)$, and then $C = DEB(7)$.
In both cases, the minimum weight of C is at least the minimum weight of the dual of the extended 3-error correcting BCH code, that is $2^{m-1} - 2^{\lfloor \frac{m+2}{2} \rfloor}$.

4. If $t = m-1$, then C is the Reed-Muller code of order one, so that $d_{min}(C) = 2^{m-1}$. □

In terms of duals of extended BCH codes, the above corollary becomes

Corollary 2 : Divisibility of the dual of an extended BCH code

Let $d \geq 3$, and l_d such that :

$$2^{l_d} + 1 \leq d < 2^{l_d+1} + 1 \tag{2}$$

Then, $DEB(d)$ is $2^{\lceil \frac{m}{l_d} \rceil - 1}$-divisible.

Let $t_d = m - l_d$.

1. If $\lfloor \frac{m}{2} \rfloor \leq l_d < m-2$, and $d < 2^{l_d+1} - 3$,

$$d_{min}(DEB(d)) \geq 2^{t_d+1} - 2^{t_d-1} \tag{3}$$

2. If $\lfloor \frac{m}{2} \rfloor \leq l_d < m-2$, and $d \geq 2^{l_d+1} - 3$,

$$d_{min}(DEB(d)) \geq 2^{t_d}$$

3. If $l_d = m-2$ and $m \geq 4$, let d_0 denote the largest designed distance strictly less than $2^{m-1}-1$, that is , the largest integer d such that $d < 2^{m-1}-1$ and d is the smallest element of its cyclotomic coset. Then :
   If m is odd and $d \leq d_0$, $d_{min}(DEB(d)) \geq 6$.
   If m is even and $d < d_0$, $d_{min}(DEB(d)) \geq 6$.

4. If $l_d < \lfloor \frac{m}{2} \rfloor$, a lower bound on $d_{min}(DEB(d))$ is given by the Carlitz-Uchiyama bound [Sl.] :

Theorem 7 *If C is the dual of the BCH code of length 2^m-1 and of designed distance $d = 2r+1$, with $2r-1 < 2^{\lceil \frac{m}{2} \rceil}+1$, then the weight of every nonzero codeword of C satisfies :*

$$2^{m-1} - (r-1)2^{m/2} \leq w \leq 2^{m-1} + (r-1)2^{m/2}$$

Remarks : This theorem is applicable here because if C is a cyclic code with defining set T, whose extension C_e is affine-invariant, then C_e has the same minimum weight as the cyclic code with defining set $T \cup \{0\}$.
Corollary 2 states that the dual of a BCH code has the divisibility of the largest $C^{(t)}$ code it contains (here $t = t_d$).

Proof . By (2), and according to the characterization of the $C^{(t)}$ codes in terms of duals of BCH codes, we deduce :

$$\forall d \geq 3, \;\; C^{(t_d)} \subseteq DEB(d) \subset C^{(t_d-1)} \tag{4}$$

where $t_d = m - l_d$ and, if $l_d \leq \lfloor \frac{m}{2} \rfloor$, then $C^{(t_d)} = DEB(2^{l_d}+1)$, and if $l_d > \lfloor \frac{m}{2} \rfloor$, then $C^{(t_d)} = DEB(\sum_{i=1}^{a} 2^{m-it_d}+1-\delta_{r,0})$, with $m = at_d + r$, $r < t_d$.
The divisibility of $DEB(d)$ is then an immediate consequence of corollary 1.

Note that we distinguish the cases $l_d < m-2$ and $l_d = m-2$ because, if $l_d < m-2$, then $2^{l_d+1}-3$ is the smallest element of its cyclotomic coset, so that $2^{l_d+1}-3$ is the designed distance of a BCH code. Indeed, $2^{l_d+1}-3 = (\underbrace{0..0}_{\geq 2}\underbrace{1\ldots1}_{l_d-1}01)$. and any cyclic shift of $2^{l_d+1}-3$ has strictly less than two consecutive zeroes in the leftmost part of its binary representation. But if $l_d = m-2$, $2^{l_d+1}-3$ is not the smallest element of its cyclotomic coset, so that the condition $d < 2^{l_d+1}-3$ does not ensure that $2^{l_d+1}-3$ does not belong to $\cup_{s<d} cl(s)$.

1. Let $\lfloor \frac{m}{2} \rfloor \leq l_d < m-2$, and suppose $d < 2^{l_d+1}-3$.
In the same spirit as in the proof of part one of corollary 1, we want to show that $u_{0,d}$ and $v_{0,d}$ belong to the defining-set $U(d)$ of $DEB(d)$, where $u_{0,d} = 2^{t_d} + 2^{t_d-1} - 1$ and $v_{0,d} = 2^{t_d+1} + 2^{t_d-1} - 1$.
First, if $x \in [0,n]$, we shall denote by $(x)_0$, the smallest element of the cyclotomic coset of two modulo n containing x.
We have :

$$n - v_{0,d} = 2^m - 2^{t_d+1} - 2^{t_d-1} = 2^{t_d-1}(2^{m-t_d+1} - 5)$$

so that

$$(n - v_{0,d})_0 = 2^{m-t_d+1} - 5 = 2^{l_d+1} - 5$$

But $d < 2^{l_d+1} - 3$, that is $d \leq 2^{l_d+1} - 5$, and so

$$(n - v_{0,d})_0 \notin \cup_{s<d} cl(s)$$

or

$$(n - v_{0,d})_0 \in [0, n] \setminus \cup_{s<d} cl(s)$$

thus

$$v_{0,d} \in \{n - z, z \in [0, n] \setminus \cup_{s<d} cl(s)\} = U(d)$$

The same reasoning holds for $u_{0,d}$:

$$n - u_{0,d} = 2^m - 2^{t_d} - 2^{t_d-1} = 2^{t_d-1}(2^{m-t_d+1} - 3)$$

$$(n - u_{0,d})_0 = 2^{m-t_d+1} - 3$$

$d < 2^{m-t_d+1} - 3$ so that $u_{0,d} \in U(d)$.

2. Let $\lfloor \frac{m}{2} \rfloor \leq l_d < m - 2$. If $d = 2^{l_d+1} - 3$, then $2^{l_d+1} - 5 = (n - v_{0,d})_0$ belongs to $\cup_{s<d} cl(s)$, and so $v_{0,d}$ does not belong to $U(d)$.
If $d = 2^{l_d+1} - 1$, then both $(n - v_{0,d})_0$ and $(n - u_{0,d})_0$ belong to $\cup_{s<d} cl(s)$, so that neither $v_{0,d}$ nor $u_{0,d}$ belong to $U(d)$.

3. Let $l_d = m - 2$ (ie. $t_d = 2$).
We already quoted that $2^{m-1} - 3$ is not the smallest element of its cyclotomic coset.
For $m \geq 4$, it is easy to see that d_0 is given by the following forms, depending on the parity of m :

$$\text{For even } m, \quad d_0 = (0\underbrace{1\ldots1}_{\frac{m}{2}-1}0\underbrace{1\ldots1}_{\frac{m}{2}-1})$$

$$\text{For odd } m, \quad d_0 = (0\underbrace{1\ldots1}_{\frac{m-3}{2}}0\underbrace{1\ldots1}_{\frac{m-1}{2}-1})$$

We shall treat the case m odd first. We want to show that the intervals $[0, 2]$, and $[2^{\frac{m+1}{2}}, 2^{\frac{m+1}{2}} + 2]$ are included in the defining-set $U(d)$ of $DEB(d)$, whenever $d \leq d_0$. For if $d < d_0$, then $DEB(d) \subset DEB(d_0)$ or equivalently $U(d) \supset U(d_0)$, it suffices to show these inclusions for $d = d_0$.
First, $[0, 2]$ is obviously included in $U(d_0)$, and also $2^{\frac{m+1}{2}}$. Now why does $2^{\frac{m+1}{2}} + 1$ belong to $U(d_0)$?
As $d_0 \notin \cup_{s<d_0} cl(s)$, we have $cl(n - d_0) \subset U(d_0)$. But

$$n - d_0 = (10\ldots01\underbrace{0\ldots0}_{\frac{m-1}{2}})$$

so that $2^{\frac{m+1}{2}} + 1$ belongs to $cl(n - d_0)$ and we are done.
Now $2^{\frac{m+1}{2}} + 2 = 4(n - d_0)$ so $2^{\frac{m+1}{2}} + 2 \in U(d_0)$.
We conclude by applying lemma 1 (with $d = 3$, $z = 2^{\frac{m+1}{2}}$), and argue in the same way as in the proof of th.4.

For the case m even, we shall show that the intervals $[0,2]$ and $[2^{\frac{m}{2}}, 2^{\frac{m}{2}}+2]$ belong to $U(d)$ as soon as $d < d_0$.
Recall that $d_0 = (0\underbrace{1\ldots1}_{\frac{m}{2}-1}0\underbrace{1\ldots1}_{\frac{m}{2}-1})$. We can easily see that the largest designed distance strictly less than d_0 is

$$\delta = d_0 - 2^{\frac{m}{2}-1} = (0\underbrace{1\ldots1}_{\frac{m}{2}-2}0\underbrace{1\ldots1}_{\frac{m}{2}})$$

As before, it is sufficient to show the inclusions for $d = \delta$. Clearly, $[0,2]$ and $2^{\frac{m}{2}}$ belong to $U(\delta)$.
As $\delta \notin \cup_{s<\delta} cl(s)$, we have $cl(n-\delta) \subset U(\delta)$. But

$$(n-\delta)_0 = (\underbrace{0\ldots0}_{\frac{m}{2}}1\underbrace{0\ldots0}_{\frac{m}{2}-2}1) = 2^{\frac{m}{2}-1}+1$$

so that $2^{\frac{m}{2}}+2 \in cl(n-\delta) \subset U(\delta)$.
Finally,

$$n-(2^{\frac{m}{2}}+1) = 2(0\underbrace{1\ldots1}_{\frac{m}{2}-1}0\underbrace{1\ldots1}_{\frac{m}{2}-1}) = 2d_0$$

As $d_0 > \delta$ and d_0 is the smallest element of its coset, we have that $cl(d_0) \notin \cup_{s<\delta} cl(s)$. Then it follows that $2^{\frac{m}{2}}+1 \in U(\delta)$.
Note that in the case where $d > d_0$ if m is odd (that is, in fact, $d = 2^{m-1}-1$), or in the case $d \geq d_0$ for even m (ie. $d = d_0$ or $d = 2^{m-1}-1$), we can only conclude that $d_{min}(DEB(d)) \geq 4$.

4. If $l_d < \lfloor \frac{m}{2} \rfloor$, then $l_d+1 \leq \lfloor \frac{m}{2} \rfloor$, so $d < 2^{\lfloor \frac{m}{2} \rfloor}+1$. We can then apply the Carlitz-Uchiyama bound. □

Remark :
If m is even and $d = 2^{\frac{m}{2}}+1$, then the bound given by (3) is better than the Carlitz-Uchiyama bound. Indeed, the C.U. bound in this case gives $d_{min}DEB(d) \geq 2^{\frac{m}{2}}$, and (3) gives $d_{min}DEB(d) \geq 2^{\frac{m}{2}+1} - 2^{\frac{m}{2}-1}$.

The following table gives the divisibility of all duals of extended BCH codes of designed distance d, of lengths 64, 128, 256. It also gives the lower bound on their minimum distance given by corollary 2. The star following some d's means that the corresponding codes are $C^{(t)}$ codes.
Length 64

d	divisibility	lower bound
3*	32	32
5*	4	24
7	4	16
9*, 11	2	12
13, 15	2	8
21*, 23	2	6
27, 31	2	4

Length 128

d	divisibility	lower bound
3*	64	64
5*	8	56
7	8	48
9*, 11	4	24
13, 15	4	16
19*, 21, 23, 27	2	12
29, 31	2	8
43*, 47, 55	2	6
63	2	4

Length 256

d	divisibility	lower bound
3*	128	128
5*	8	112
7	8	96
9*	4	80
11	4	64
13	4	48
15	4	32
17*, 19, 21, 23, 25, 27	2	24
29, 31	2	16
37*, 39, 43, 45, 47, 51, 53, 55, 59	2	12
61, 63	2	8
85*, 87, 91, 95, 111	2	6
119, 127	2	4

Remark : The class of $C^{(t)}$ codes gives the exact divisibility of some affine-invariant codes. We saw that if $C^{(t)} \subsetneq C \subset C^{(t-1)}$, then C has exactly the same divisibility as $C^{(t)}$, that is $2^{\lceil \frac{m}{m-t} \rceil - 1}$, which is also the divisibility of $RM(m-t)$. If we look at the situation of C among the RM codes, we can only conclude that C has at least the divisibility of $RM(m-t)$.

5 The $C^{(t)}$ codes as ideals of the modular algebra $\mathcal{A}$

Recall that $\mathcal{A}$ is the modular group algebra $\mathsf{F}_2[\{\mathsf{F}_{2^m}, +\}]$. By theorem 1, an affine invariant code is an extended cyclic code which is an ideal of $\mathcal{A}$.
If P denotes the ideal of $\mathcal{A}$ consisting of elements $x = \sum_{g \in \mathsf{F}_{2^m}} x_g X^g$ such that $\sum_{g \in \mathsf{F}_{2^m}} x_g = 0$, the product ideal P^j is the Reed Muller code of order $m-j$. The sequence $(P^j)_j$, is a decreasing sequence of ideals of $\mathcal{A}$.

Definition 4 *Let U be an ideal of $\mathcal{A}$.*

1. *The depth of x is the integer j such that : $x \in P^j$ and $x \notin P^{j+1}$. In the same way, the depth of U is the integer j such that : $U \subset P^j$ and $U \not\subset P^{j+1}$.*

2. *$x = \{x_1, \ldots, x_k\}$, $x_i \in \mathcal{A}$, is a generating system (GS) of U if $U = x_1\mathcal{A} + \ldots + x_k\mathcal{A}$. x is a minimal generating system (MGS) of U, if the cardinality of every GS of U is greater than or equal to k. k is then called the size of U.*

3. *U is a constant depth type ideal (CDT), if every MGS of U consists of elements of the same depth.*

Theorem 8 *$\forall t \in [2, m-1]$, $C^{(t)}$ is CDT, and its size is m.*

So $C^{(t)}$ can be expressed as a sum of principal ideals of $\mathcal{A}$, in the following way :

$$C^{(t)} = x_1\mathcal{A} + \ldots + x_m\mathcal{A}, \quad x_i \in C^{(t)} \setminus P^{t+1}.$$

For example, x_i can be chosen to be the extension of the word $Z^{i-1}g_t(Z)$, where $g_t(Z)$ is the generator polynomial of the punctured $C^{(t)}$ code.

Theorem 8 is easily derived from the following result, due to P. Charpin [Ch.1] :

Theorem 9 *Let U be an affine-invariant code. Let j be the depth of U, and F, its border. Then :*

$$U \text{ is } CDT \Leftrightarrow (f \in F \Rightarrow \omega(f) = j)$$

6 Numerical results

The following table sums up the parameters of the $C^{(t)}$ codes for several lengths. In the first column, we have the bound given by th.4. In the second one, we have the Carlitz-Uchiyama bound, which is negative for the first values of t. The divisibility of $C^{(t)}$ is that of theorem 6. Its depth is defined in def. 4. For the dimension of $C^{(t)}$, see prop. 2. best low.b. is the best lower bound on the minimum distance of $C^{(t)}$. For $t \leq \lfloor \frac{m}{2} \rfloor$, it is the one of theorem 4; for $t \geq \lceil \frac{m}{2} \rceil$, when m is odd, and $t > \frac{m}{2}$ when m is even, the Carlitz-Uchiyama bound is better (For m even and $t = \frac{m}{2}$, the Carlitz-Uchiyama bound is the extended BCH bound, that is $2^{\frac{m}{2}}$, and by th. 4, we have the better estimate $2^{\frac{m}{2}+1} - 2^{\frac{m}{2}-1}$).
The asterisque means that low.b. is the true minimum distance.
Let us precise several things for $m = 6$:
$C^{(2)}$ is one of the codes listed by Chen in [Pe.We].
The authors of [Ch.Au.Se2] proved that there was no word of weight strictly less than 14 in the dual of the BCH code of designed distance 9, and they found by the Newton's identities that there was a codeword of weight 14 that was an idempotent of the code. So the minimum weight of $C^{(3)}$ is exactly 14 (see the first remark following th. 7).

Length 2^6.

t	b.of th.4	CU b.	divisibility	depth	dim.	best low.b.
2	6		2	2	46	8*
3	12	8	2	3	25	14*
4		24	4	4	13	24*
5		32	32	5	7	32*

Length 2^7.

t	b.of th.4	CU b.	divisibility	depth	dim.	best low.b.
2	6		2	2	99	6
3	12		2	3	57	12
4	24	30.06	4	4	29	32
5		52.69	8	5	15	56*
6		64	64	6	8	64*

Length 2^8.

t	b.of th.4	CU b.	divisibility	depth	dim.	best low.b.
2	6		2	2	209	6
3	12		2	3	125	12
4	24	16	2	4	65	24
5	48	80	4	5	33	80
6		112	8	6	17	112*
7		128	128	7	9	128*

Length 2^9.

t	b.of th.4	CU b.	divisibility	depth	dim.	best low.b.
2	6		2	2	436	6
3	12		2	3	271	12
4	24		2	4	145	24
5	48	97.61	4	5	73	100
6	96	188.12	4	6	37	192
7		233.37	16	7	19	240*
8		256	256	8	10	256*

Length 2^{10}.

t	b.of th.4	CU b.	divisibility	depth	dim.	best low.b.
2	6		2	2	901	6
3	12		2	3	581	12
4	24		2	4	316	24
5	48	32	2	5	161	48
6	96	288	4	6	81	288
7	192	416	8	7	41	416
8		480	16	8	21	480*
9		512	512	9	11	512*

Appendix

We give here another proof of theorem 4. More precisely, we show that, for $2 \leq t < m-2$, $d_{min}C^{(t)} > 2^t$; And, by the theorem of Kasami (th.5), we conclude in the same way.
We first need a lemma.

lemma 2 *Let t, $2 \leq t < m-2$, and $i_0 = 2^t - 1$.*
Denote by J_t the set $J_t = \{2^t - 2^i,\ 0 \leq i \leq t\}$. Let $1 \leq r < i_0$. Then :
1- If $r \in J_t$, $r + i_0 \in D_t$ and $w(r + i_0) = t$.
2- If $r \notin J_t$, $w(r + i_0) < t$.

Proof . 1- We have: $i_0 = (0 \ldots 0 \overbrace{1 \ldots 1}^{t})$. r is of the form $r = 2^t - 2^i$, $0 < i < t$.
$i_0 + r = 2^t - 1 + 2^t - 2^i = (0 \ldots 0 \underbrace{1 \ldots 1}_{t-i} 0 \underbrace{1 \ldots 1}_{i})$. And $0 < t - i < t$ if $0 < i < t$. So $r + i_0$ has not t consecutive ones and is of weight t.
2- If $r \notin J_t$, $r < i_0$, we can easily see that there is at least two zeroes in the rightmost t digits of $r + i_0$, and in the remaining $m - t$ digits, there is at most one one. □

Let $2 \leq t < m-2$. We denote by $C^{(t)*}$, the punctured $C^{(t)}$ code, and we suppose that there exists $x \in C^{(t)*}$, such that $w(x) = 2^t - 1$. Let $\sigma_x(Z) = \sum_{i=0}^{2^t-1} \sigma_i Z^i$, $\sigma_0 = 1$, be the locator polynomial of x.
As $C^{(t)} \subset RM(m-t)$, $x \in RM(m-t)^*$. Thus (see [Ka,Li,Pe 1]):

$$\sigma_j = 0\ \forall j \notin J_t = \{2^t - 2^i,\ 0 \leq i \leq t\}$$

And so $\sigma_x(Z)$is of the form :

$$\sigma_x(Z) = \sum_{i=0}^{t} \sigma_{2^t-2^i} Z^{2^t-2^i}$$

As in lemma 2, we denote by $i_0 = 2^t - 1$. If $A_i = x(\alpha^i)$, where α is a primitive element of $\mathbb{F}_{2^m}$, the σ_i's and the A_i's are related by the Newton's identities :

$$\forall r,\ A_{i_0+r} + \sum_{k=1}^{r} A_{i_0+r-k}\sigma_k = 0$$

According to lemma 2, if $1 \leq r < i_0$ et $r \notin J_t$, $A_{i_0+r} = x(\alpha^{i_0+r}) = 0$ because $r + i_0 \in D_t$ ($w(r + i_0) < t$). The Newton's equations then give ([Ch,Au,Sel]) :

$$r \in J_t \Rightarrow \sigma_r = \frac{A_{i_0+r}}{A_{i_0}},$$

But if $r \in J_t$, with $1 \leq r < i_0$, then $i_0 + r \in D_t$. So the only nonzero coefficients of $\sigma_x(Z)$ are $\sigma_0 = 1$ et σ_{i_0}, so that :

$$\sigma_x(Z) = \sigma_{2^t-1} Z^{2^t-1} + 1$$

We prove that the word x cannot be a word of $C^{(t)*}$, by showing that the aforementioned polynomial cannot be the locator polynomial of a word of $C^{(t)*}$.

Let $\lambda = \sigma_{i_0}$. λ is a nonzero element of F_{2^m} because λ is the i_0-th elementary symmetric function of the α^{i_j}'s, that is $\lambda = \alpha^{i_1} \ldots \alpha^{i_{2^t-1}}$, where $i_1, \ldots, i_{2^t-1}$ are the positions of the nonzero coordinates of x.
By the change of variable $Y = Z^{-1}$ and multiplying by Y^{2^t-1}, we can bring the polynomial $\sigma_x(Z)$ to the following form :

$$\sigma_x(Z) = Z^{2^t-1} + \lambda$$

The zeroes of the locator polynomial are the elements α^{n-i_j}, where the i_j's have been previously defined. So $\sigma_x(Z)$ must divide $z^{2^m-1} + 1$ in $\mathsf{F}_{2^m}[Z]$.

lemma 3 *(The proof is deferred until the end of the appendix).*

$$Z^{2^t-1} + \lambda \,|\, Z^{2^m-1} + 1 \Leftrightarrow t \,|\, m \;\; and \;\; \exists j, \;\; \lambda = \alpha^{(2^t-1)j}$$

So, if $t \not| m$, then $\sigma_x(Z)$ cannot be the locator polynomial of a word of $C^{(t)*}$ of weight $2^t - 1$.
Let us examine the case $t \,|\, m$.
$t \,|\, m \Leftrightarrow 2^t - 1 \,|\, 2^m - 1$. Let s be defined by $2^m - 1 = (2^t - 1)s = i_0 s$, and suppose λ is of the form $\alpha^{i_0 j}$, $1 \leq j \leq s$. Then the zeroes of $\sigma_x(Z) = Z^{i_0} + \lambda$ are :

$$\lambda^{\frac{1}{i_0}} < \alpha^s >= \{\alpha^j, \alpha^{j+s}, \ldots, \alpha^{j+s(i_0-1)}\}.$$

The codeword x is therefore

$$x = X^{n-j} + X^{n-(j+s)} + \ldots + X^{n-(j+s(i_0-1))}$$

where $n = 2^m - 1$.
$x = R(X^{-1})$, where $R(X)$ is the following polynomial :

$$R(X) = X^j + X^{j+s} + \ldots + X^{j+s(i_0-1)} = X^j(1 + X^s + \ldots + X^{s(i_0-1)})$$

On the other hand, we have :

$$X^{2^m-1} + 1 = (X^s + 1)(X^{s(i_0-1)} + \ldots + X^s + 1)$$

So the zeroes of $R(X)$ are 0 with multiplicity j and α^l, $l \in [1, n[\backslash\{i_0, 2i_0, \ldots, (s-1)i_0\}$ The zeroes of x are then :

$$\{0\} \cup \{\alpha^l, \; l \in [1, n[\backslash\{n - i_0, n - 2i_0, \ldots, n - (s-1)i_0\}\}$$

We have the easily checked set equality :

$$\{i_0, 2i_0, \ldots, (s-1)i_0\} = \{n - i_0, n - 2i_0, \ldots, n - (s-1)i_0\},$$

so that $x(\alpha^l) \neq 0$ for $l \in \{i_0, 2i_0, 3i_0, \ldots, (s-1)i_0\}$. But :

$$3i_0 = 3(2^t - 1) = (0 \ldots 010\underbrace{1 \ldots 1}_{t-2}01)$$

$3i_0 \in D_t \setminus \{0\}$ because it has not t consecutive ones. Therefore, we cannot have simultaneously $x \in C_t^*$ and $x(\alpha^{3i_0}) \neq 0$.

Finally, whenever $t \mid m$ or not, $\sigma_x(Z)$ cannot be the locator polynomial of a word of weight $2^t - 1$ in $C^{(t)*}$. So the minimum weight of $C^{(t)*}$ is strictly greater than $2^t - 1$, and the one of $C^{(t)}$ strictly greater than 2^t.

Proof of lemma 3 :
Suppose $t \mid m$, $\lambda = \alpha^{i_0 j}$, $i_0 = 2^t - 1$ and $2^m - 1 = i_0 s$.
$\lambda^{-1} = (\alpha^{-j})^{i_0} = (\alpha^{n-j})^{i_0}$, so the order of λ^{-1} divide s. We have :

$$Z^{2^m-1} + 1 = (Z^{i_0} + \lambda)(\lambda^{-1})((\lambda^{-1} Z^{i_0})^{s-1} + \ldots + \lambda^{-1} Z^{i_0} + 1)$$

Indeed,

$$(\lambda^{-1} Z^{i_0})^{s-1} + \ldots + \lambda^{-1} Z^{i_0} + 1 = \frac{1 - (\lambda^{-1} Z^{i_0})^s}{1 - \lambda^{-1} Z^{i_0}} = \frac{1 - Z^{i_0}}{1 - \lambda^{-1} Z^{i_0}}$$

and the result follows by multiplying the last equality by λ^{-1}, recalling the fact that $-1 = +1$ in $\mathbf{F}_2$.

Suppose $Z^{2^t-1} + \lambda \mid z^{2^m-1} + 1$ in $\mathbf{F}_{2^m}[Z]$.
Let $f(Z) = Z^{2^t-1} + \lambda$. The zeroes of f are therefore among $< \alpha >$, where α is a primitive element of $\mathbf{F}_{2^m}$, and $< \alpha >$ denotes the cyclic group generated by α. Let α^j be a zero of f. $f(\alpha^j) = 0$ ie $\alpha^{(2^t-1)j} + \lambda = 0$, so $\lambda = \alpha^{(2^t-1)j}$ in $\mathbf{F}_{2^m}$. It remains to show that $t \mid m$, or equivalently that $2^t - 1 \mid 2^m - 1$.
We have :

$$Z^{2^t-1} \equiv \lambda \; mod \; f(Z)$$

and $2^t - 1$ is the smallest integer r such that $Z^r \equiv a \; mod \; f(Z)$, where $a \in \mathbf{F}_{2^m}^*$. Then ([Ni,Li], lemma 3.17,p.89) :

$$ord(f) = (2^t - 1)h,$$

where h is the order of λ in $\mathbf{F}_{2^m}^*$.
$h = ord(\lambda) = \frac{2^m-1}{d'}$, with $d' = (j(2^t - 1), 2^m - 1)$. So

$$ord(f(Z)) = (2^t - 1)\frac{2^m - 1}{d'}$$

Let $d = (2^t - 1, 2^m - 1)$. Then $d' = (j, d)$, if $j \neq 1$, and $d' = d$ otherwise. So $d' \mid d$. As $d \mid 2^t - 1$, we have $d' \mid 2^t - 1$. But as f divides $Z^{2^m-1} + 1$, $ord(f) \mid 2^m - 1$ ([Ni,Li], lemma 3.6, p.85). Therefore

$$d' = 2^t - 1, \text{ and so } d = 2^t - 1 \text{ ie } t \mid m.$$

References

[Ch.1] P. Charpin: Codes cycliques étendus affine-invariants et antichaines d'un ensemble partiellement ordonné.
Discrete Mathematics 80, North-Holland, 1990, p.229-247.

[Ch.2] P. Charpin: Some applications of a classification of affine- invariant codes.
Lect. Notes in Comp. Sci.356, Proceedings of AAECC 5, Springer-Verlag 1987.

[Ch,Au,Se1] P. Charpin, D. Augot, N. Sendrier: Studying the locator polynomial of minimum weight codewords of BCH codes.
IEEE trans. on inf. theory, 1991.

[Ch.Au.Se2] P. Charpin, D. Augot, N. Sendrier: Weights of some binary codes troughout the Newton's identities.
Proceedings of Eurocode '90, November 1990, Springer-Verlag.

[Ka,Li,Pe 1] T. Kasami, S. Lin, W.W. Peterson : New generalizations of the Reed-Muller codes, Part I: Primitive codes.
IEEE Trans. on inf. theory, vol IT 24, no 2, mars 1968, p.189-199.

[Ka,Li,Pe 2] 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, p. 475-496, 1967.

[Ka,To] T. Kasami, N. Tokura :On the weight structure of Reed Muller codes.
IEEE Trans. on Inf. theory, vol IT 16,no 6, nov. 1970, p.752-759.

[Li.Mo] Litsyn S., Moreno C.J., Moreno O. : Divisibility properties and new bounds for cyclic codes and exponential sums in one and several variables, preprint.

[Ma] H.B. Mann: On the number of information symbols in Bose-Chauduri codes.
Information and control 5, 1962, p.153-162.

[Mc El] R.J. Mc Eliece: Weight congruences for p-ary cyclic codes.
Discrete Math. 3 1972, p.177-192.

[Ni,Li] H. Niederreiter, R. Lidl : Finite Fields.
Encyclopedia of math. and its applications, vol.20, Cambridge University Press.

[Pe.We] W.W. Peterson, E.J. Weldon Jr.: Error correcting codes.

[Sl] N.J.A. Sloane, J. Mc Williams: The theory of error correcting codes.
North Holland.

[Wa] H.N. Ward: Divisible codes.
Archiv der Mathematik, vol. 36, 1981, fasc. 6, p.485-494.

Unité de Recherche INRIA Rocquencourt
Domaine de Voluceau - Rocquencourt - B.P. 105 - 78153 LE CHESNAY Cedex (France)

Unité de Recherche INRIA Lorraine Technopôle de Nancy-Brabois - Campus Scientifique
615, rue du Jardin Botanique - B.P. 101 - 54602 VILLERS LES NANCY Cedex (France)
Unité de Recherche INRIA Rennes IRISA, Campus Universitaire de Beaulieu 35042 RENNES Cedex (France)
Unité de Recherche INRIA Rhône-Alpes 46, avenue Félix Viallet - 38031 GRENOBLE Cedex (France)
Unité de Recherche INRIA Sophia Antipolis 2004, route des Lucioles - B.P. 93 - 06902 SOPHIA ANTIPOLIS Cedex (France)

EDITEUR
INRIA - Domaine de Voluceau - Rocquencourt - B.P. 105 - 78153 LE CHESNAY Cedex (France)

ISSN 0249 - 6399

RR_1835