JOURNAL OF COMBINATORIAL THEORY, Series A 67, 223–244 (1994)

On Self-Dual Affine-Invariant Codes

PASCALE CHARPIN AND FRANÇOISE LEVY-DIT-VEHEL

INRIA, Domaine de Voluceau, Rocquencourt,
BP 105, 78153 Le Chesnay Cedex, France

Communicated by V. Pless

Received February 16, 1993

An extended cyclic code of length 2^m over $GF(2)$ cannot be self-dual for even m. For odd m, the Reed–Muller code $[2^m, 2^{m-1}, 2^{(m+1)/2}]$ is affine-invariant and self-dual, and it is the only such code for $m=3$ or 5. We describe the set of binary self-dual affine-invariant codes of length 2^m for $m=7$ and $m=9$. For each odd m, $m \geqslant 9$, we exhibit a self-dual affine-invariant code of length 2^m over $GF(2)$ which is not the self-dual Reed–Muller code. In the first part of the paper, we present the class of self-dual affine-invariant codes of length 2^{rm} over $GF(2^r)$, and the tools we apply later to the binary codes.

1. INTRODUCTION

In this paper, codes are assumed to have symbols from the Galois field $K = GF(2^r)$, $r \geqslant 1$. Only primitive extended cyclic codes will be considered. Thus the length of the codes will be $N = 2^{rm}$, $m \geqslant 3$. We denote by $\mathbf{G}$ the Galois field of order 2^{rm}. The *distance* will always be the Hamming distance.

A self-dual code is an $[N, N/2]$ code over K which equals its dual. An affine-invariant code is a code invariant under the group of affine permutations on $\mathbf{G}$; in particular, it is an extended cyclic code. For example, the generalized Reed–Muller (GRM) codes are affine-invariant. In this paper we study affine-invariant self-dual codes.

For even m, there is no extended cyclic self-dual code of length N over K. So we restrict ourselves to the case of *odd m*. There is an infinite class of self-dual GRM-codes. For instance the binary Reed–Muller (RM) codes with parameters $[2^m, 2^{m-1}, 2^{(m+1)/2}]$ give an infinite class of affine-invariant self-dual codes. The binary case is more interesting because the codes are doubly-even while self-dual extended cyclic codes over $GF(4)$ are not even. We are interested here in the following question: do there exist affine-invariant self-dual codes which are not Reed–Muller codes?

0097-3165/94 $6.00

In Section 2, we discuss the class of affine-invariant self-dual codes. Following the work of Kasami *et al.* [10], we consider the identification of affine-invariant codes of length N with antichains of the interval $[0, n]$, where $n = N - 1$, [5, 6, 7]. We characterize weak self-duality in terms of those antichains. We are then able to present, in Section 3, an infinite class of self-dual affine-invariant codes of length 2^m over $GF(2)$, which is not the RM class. For $m \leqslant 9$, we describe a method that allows us to exhibit all self-dual affine-invariant codes of length less than or equal to 512. For m in $\{3, 5\}$, there is only one such code, the RM-code. Using the classification of Pless *et al.*, we prove that, up to equivalence, there are precisely three such codes of length 128; using a recent result on equivalent cyclic codes [8][15], we prove that there are seventy non-equivalent self-dual affine-invariant codes of length 512.

2. Preliminaries

2.1. *Extended Cyclic Self-Dual Codes*

Let $\mathscr{R}$ be the quotient algebra $K[Z]/(Z^n - 1)$, where $n = 2^{rm} - 1$. A cyclic code C^* of length n over K is an ideal of $\mathscr{R}$. Such a code is said to be *primitive*. The symbols of any codeword $c^* \in C^*$ can be labelled by the non-zero elements of the finite field $\mathbf{G}$ and we shall do so below.

We denote by $\mathscr{A}$ the group algebra $K[\mathbf{G}]$, which is the set of formal polynomials

$$x = \sum_{g \in \mathbf{G}} x_g X^g, \qquad x_g \in K,$$

with

$$0 = \sum_{g \in \mathbf{G}} 0 X^g, \qquad 1 = \sum_{g \in \mathbf{G}} X^g, \qquad aX^g + bX^g = (a+b) X^g.$$

and

$$\sum_{g \in \mathbf{G}} x_g X^g \sum_{g \in \mathbf{G}} y_g X^g = \sum_{h \in \mathbf{G}} \left(\sum_{g \in \mathbf{G}} x_g y_{g+h} \right) X^h. \tag{1}$$

We consider the extension C of the code C^* in the algebra $\mathscr{A}$. Let α be a primitive root of unity in $\mathbf{G}$. Then the extension is given as follows: each codeword $c^* \in \mathscr{R}$, $c^* = \sum_{i=0}^{n-1} c_i^* Z^i$, is extended to $c \in \mathscr{A}$ where

$$c = c_0 X^0 + \sum_{g \in \mathbf{G}^*,\, g = \alpha^i} c_g X^g, \qquad c_0 = \left(\sum_{i=0}^{n-1} c_i^* \right), \qquad c_{\alpha^i} = c_i^*.$$

Now consider the set I of those k's such that α^k is a zero of the cyclic code C^*. Then the codeword c is an element of C if and only if it satisfies:

$$\sum_{g \in \mathbf{G}} c_g = 0 \qquad \text{and} \qquad \sum_{i=0}^{n-1} c_{\alpha^i} (\alpha^k)^i = 0, \qquad \text{for all} \quad k \in I.$$

Therefore we can identify precisely an extended cyclic code in $\mathscr{A}$.

DEFINITION 1. *Let* $S = [0, n]$; we denote by q the order 2^r of the finite field K. An extended cyclic code C in $\mathscr{A}$ is uniquely defined by a subset T of S such that $0 \in T$ and T is a union of cyclotomic cosets of q modulo n. Let us define for all $s \in S$ and for all $x \in \mathscr{A}$:

$$\phi_s(x) = \sum_{g \in \mathbf{G}} x_g \, g^s \in \mathbf{G}.$$

In particular, $\phi_0(x) = \sum_{g \in \mathbf{G}} x_g$. Then we have that

$$C = \{x \in \mathscr{A} \mid \phi_s(x) = 0, \text{ for all } s \in T\}.$$

We say that T is the defining set of the code C.

Let C be an extended cyclic code in $\mathscr{A}$; we denote by $C^\perp$ the *dual* of C:

$$C^\perp = \{y \in \mathscr{A} \mid \langle x, y \rangle = 0, \text{ for all } x \in C\}, \qquad \text{where} \quad \langle x, y \rangle = \sum_{g \in \mathbf{G}} x_g \, y_g.$$

If $C \subset C^\perp$, the code C is said to be *weakly self-dual*. If $C = C^\perp$, the code C is said to be *self-dual*. It is clear that there is no cyclic self-dual code, because if 1 is a zero of such a code it cannot be a zero of its dual. However, the extension of a cyclic code can be self-dual.

THEOREM 1. *Let C be an extended cyclic code in $\mathscr{A}$ with defining set T. Denote by $T^\perp$ the defining set of the dual of C. Then $T^\perp = \{s \in S \mid n - s \notin T\}$. Moreover:*

(i) *C is weakly self-dual if and only if T satisfies: $n - s \notin T$ implies $s \in T$.*

(ii) *C is self-dual if and only if T satisfies: $n - s \notin T$ is equivalent to $s \in T$.*

Proof. Let D be the extended cyclic code with defining set $I = \{s \in S \mid n - s \notin T\}$. Recall that $N = n + 1$. It is obvious that

$$\dim C + \dim D = 2N - (|T| + |I|) = N = \dim \mathscr{A}.$$

Hence D is the dual of C if and only if $\langle x, y\rangle = 0$, for any $x \in C$ and any $y \in D$. Let $xy = \sum_{g \in \mathbf{G}} a_g X^g$. Note that from (1), $\langle x, y\rangle = \sum_{g \in \mathbf{G}} x_g y_g = a_0$. Moreover

$$\phi_n(xy) = \phi_n\left(\sum_{h \in \mathbf{G}} x_h \sum_{g \in \mathbf{G}} y_g X^{h+g}\right) = \sum_{h \in \mathbf{G}} x_h \sum_{g \in \mathbf{G}} y_g (h+g)^n$$
$$= \sum_{i=0}^{n} \binom{n}{i} \sum_h x_h h^i \sum_g y_g g^{n-i} = \sum_{i=0}^{n} \binom{n}{i} \phi_i(x)\, \phi_{n-i}(y).$$

When $x \in C$ and $y \in D$, we have: if $i \notin T$ then $n - i \in I$. That means that for any i, $\phi_i(x)$ or $\phi_{n-i}(y)$ equals zero. But by definition, $\phi_n(xy) = \sum_{g \neq 0} a_g$. It is clear that the sum of the a_g's is zero, since the sums of the y_g's is zero. It follows that $a_0 = 0$. Thus we have proved that $D = C^\perp$. Now properties (i) and (ii) are easily deduced from the definition of $T^\perp$, since C is weakly self-dual (respectively self-dual) if and only if $T^\perp \subset T$ (respectively $T^\perp = T$). ∎

COROLLARY 1. *Let C be an extended cyclic code of length 2^{rm} over the finite field of order 2^r. If m is even then C cannot be self-dual.*

Proof. Suppose that $m = 2t$, $t \geqslant 1$. Recall that $q = 2^r$ and $n = 2^{mr} - 1$. In this case we can exhibit an element s of S such that s and $n - s$ belong to the same cyclotomic coset:

$$s = \sum_{i=0}^{t-1} (q-1)\, q^i \qquad \text{and} \qquad n - s = \sum_{i=t}^{m-1} (q-1)\, q^i = q^t s,$$

and this means that the defining set of C cannot satisfy condition (ii) of Theorem 1. ∎

From now on when we consider a self-dual code, we always assume that m is odd. By the Gleason–Pierce Theorem a self-dual code over K in which the distance between two codewords is always a multiple of l is [13, p. 597]

- either a binary or a quaternary code if $l = 2$ (the code is said to be *even*),
- or a binary code if $l = 4$ (the code is said to be *doubly-even*).

For extended cyclic codes the property holds.

PROPOSITION 1. *Let C be a self-dual extended cyclic code over K. If $K = GF(2)$ then C is doubly-even. If $K = GF(4)$ then C is not even.*

Proof. The first assertion is a property of such extended *duadic codes* [11, Theorem 5].

To prove the second assertion notice that, since C is an extended cyclic code over $GF(4)$, $r=2$ and C is of length 2^{2m}. According to [12, Thm. 35], the length $k+1$ of an even formally self-dual code over $GF(4)$ is such that k and $2^{2i-1}+1$ are relatively prime, for all $i=1, 2, \ldots$. But this hypothesis is not satisfied by the length of C, since 3 divides $2^{2m}-1$. ∎

2.2. *Affine-Invariant Self-Dual Codes*

A K-subspace of $\mathscr{A}$ is said to be *affine-invariant* if its automorphism group contains the group of the affine permutations on $\mathbf{G}$. Such a permutation $\sigma_{u,v}$ acts on the elements of $\mathscr{A}$

$$\sigma_{u,v}: \sum_{g\in\mathbf{G}} x_g X^g \mapsto \sum_{g\in\mathbf{G}} x_g X^{ug+v}, \qquad u, v\in\mathbf{G}, u\neq 0. \tag{2}$$

Then an affine-invariant code of $\mathscr{A}$ is clearly an extended cyclic code and an ideal of the algebra $\mathscr{A}$. Since dual codes have the same automorphism group, the dual of an affine-invariant code is affine-invariant. Moreover, the dual of an affine-invariant code equals its annihilator. This follows easily from the definition of the multiplication in $\mathscr{A}$:

$$xy=\sum_{g\in\mathbf{G}}\left(\sum_{h\in\mathbf{G}} x_h y_{h+g}\right)X^g=\sum_{g\in\mathbf{G}}\langle x, X^g y\rangle X^g.$$

Kasami *et al.* characterized affine-invariant codes by a combinatorial property of their defining sets [10]. We will define a partial order on S and present their result in this context.

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

$$\text{for all } s, t \text{ in } S: s\ll t \qquad \text{if and only if} \quad s_i\leqslant t_i,\ i\in[0, rm-1].$$

This defines the poset $(S, \ll)$. When $s\ll t$, s is said to be a descendant of t and t to be an ascendant of s. A minimal (resp. maximal) element s of a subset $I\subset S$ is an element of I whose strict descendants (resp. ascendants) are not in I. 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 set of non-related elements of S. Now let us define the map:

$$\Delta: I\subset S\mapsto \Delta(I)=\bigcup_{t\in I}\{s\in S, s\ll t\}=\bigcup_{t\in I}\Delta(t),$$

where we have denoted $\Delta(\{t\})$ simply by $\Delta(t)$. For a discussion and proof of the following result see either [7] or [10].

THEOREM 2. *Let C be the extended cyclic code in $\mathscr{A}$ with defining set T. Then, C is affine-invariant if and only if $\Delta(T) = T$.*

Let $T \subset S$. The antichain consisting of the minimal elements of $S \setminus T$ is called the *border* of T and is denoted by $F(T)$. Equivalently:

$$F(T) = \{s \in S \setminus T \mid \Delta(s) \setminus \{s\} \subset T\}. \tag{3}$$

Let C be an extended cyclic code with defining set T. For simplicity we will say that $F(T)$ is *the border of the code C*. If the code is affine-invariant then it is uniquely defined by its border; for the proof of the following result see [6, 7].

THEOREM 3. *Let $q = 2^r$, $K = GF(q)$. Each antichain of $(S, \preccurlyeq)$, invariant under multiplication by $q \bmod n$, is the border of one and only one affine-invariant code of length 2^{rm} over K.*

For our purposes, the most interesting class of affine-invariant codes is the class of GRM-codes of length $N = 2^{rm}$ over $K = GF(q)$, $q = 2^r$. So we recall the definition and some properties of GRM-codes.

DEFINITION 3. Let $s \in S$. The q-weight of s is $\omega_q(s) = \sum_{i=0}^{m-1} s_i$, where $\sum_{i=0}^{m-1} s_i q^i$ is the q-ary expansion of s. Let $v \in [1, m(q-1)[$ and $\mu = m(q-1) - v$.

The GRM-code of length N over K and of order v, denoted by $C_v(m, q)$, is the extended cyclic code in $\mathscr{A}$ with defining set:

$$T_v = \{s \in S \mid \omega_q(s) < \mu\}.$$

PROPOSITION 2. *Every GRM-code is affine-invariant. Let t and r be, respectively, the quotient and the remainder of μ upon division by $q-1$; the minimum weight of $C_v(m, q)$ is $d_v = q^t(r+1)$. The dual of $C_v(m, q)$ is $C_{m(q-1)-v-1}(m, q)$.*

When m is odd there exists one self-dual GRM-code, with parameters:

$$v = \frac{m(q-1)-1}{2} \left(\text{or} \quad \mu = \frac{m(q-1)+1}{2} \right) \qquad \text{and} \qquad d_v = q^{(m-1)/2}(q/2+1).$$

Proof. GRM-codes were introduced by Kasami *et al.* They obtained in [9] the results on the minimum weight and the dual; they proved in [10] that GRM-codes are affine-invariant. The order v of a self-dual GRM-code must satisfy $v = m(q-1) - v - 1$ or equivalently $\mu = m(q-1) - \mu + 1$, which yields the first equality. The second is obvious from the fact that $\mu = (m-1)(q-1)/2 + q/2$. We give in Table I the parameters of self-dual GRM-codes of length less then 2^{14}. ∎

TABLE I

The Self-Dual GRM-Codes of Length $N=q^m$ over $GF(q)$, $q=2^r$; $\mu=m(q-1)-v$, Where v is the order; d Is the Minimum Weight

N	m	q	μ	v	d	N	m	q	μ	v	d
4	1	4	2	1	3	512	9	2	5	4	32
8	3	2	2	1	4	512	3	8	11	10	40
8	1	8	4	3	5	512	1	512	256	255	257
16	1	16	8	7	9	1024	5	4	8	7	48
32	5	2	3	2	8	1024	1	1024	512	511	513
32	1	32	16	15	17	2048	11	2	6	5	64
64	3	4	5	4	12	2048	1	2048	1024	1023	1025
64	1	64	32	31	33	4096	3	16	23	22	144
128	7	2	4	3	16	4096	1	4096	2048	2047	2049
128	1	128	64	63	65	8192	13	2	7	6	128
256	1	256	128	127	129	8192	1	8192	4096	4095	4097

Note. When $q=N$, the GRM is also an extended Reed–Solomon code.

2.3. *The Weak-Self-Dual Condition*

It follows from Theorem 3 that we can obtain all self-dual affine-invariant codes by determining all corresponding antichains. It is difficult, however, to obtain a characterization. For instance the antichains corresponding to the binary RM-codes are easily obtained:

$$K=GF(2), \qquad v\in[1,m]: F(T_v)=\{s\in S \mid \omega_2(s)=m-v\}, \tag{4}$$

but we do not have such a simple formulation for the non-binary case (cf. [5, Chap. 3]). Weak self-duality can be viewed as a property of antichains and, from this point of view, we can easily study the codes of small lengths, as we will see in the examples below.

THEOREM 4. *Let F be an antichain of $(S, \preccurlyeq)$. Then F is the border of a weakly self-dual affine-invariant code if and only if:*

$$\text{for all } f \text{ in } F \text{ and for all } f' \text{ in } F \qquad \text{then} \quad f' \notin \Delta(n-f). \tag{5}$$

In other words, an affine-invariant code is weakly self-dual if and only if its border satisfies (5).

Proof. Let C be an affine-invariant code with defining set T and border F. It follows from Theorem 1 and the definition of the border, (3), that the set $n-F=\{n-f \mid f\in F\}$ is the set of maximal elements of $T^{\perp}$. Then C is weakly self-dual if and only if the set $n-F$ is included in T. Equivalently, for all $f\in F$, the set $\Delta(n-f)\cap F$ is empty. ∎

COROLLARY 2. *Let C be an affine-invariant weakly self-dual code over K with defining set T. Let* $\mathrm{cl}(s)$ *be the cyclotomic coset of q modulo n which contains s (where q is the order of K). Then we have*

$$\mathrm{cl}(s) \text{ does not satisfy } (5) \Rightarrow \mathrm{cl}(s) \subset T.$$

Proof. Note that $\mathrm{cl}(s)$, as every cyclotomic coset, is an antichain. Set $F = \mathrm{cl}(s)$. Since F does not satisfy (5), there exist $f \in F$ and $f' \in F$ such that $f' \ll n - f$.

Suppose $F \not\subset T$. Then $f \notin T$, and so $n - f \in T$. But C is affine-invariant and f', being a descendent of $n - f$, is also in T. Thus $\mathrm{cl}(f) = F \subset T$, a contradiction. ∎

EXAMPLE 1. There is only one binary self-dual code of length 32 which is affine-invariant; that is the RM-code [32, 16, 8]. Indeed the cyclotomic cosets of 2 modulo 31 are:

(1 2 4 8 16) (3 6 12 24 17) (5 10 20 9 18)

(7 14 28 25 19) (11 22 13 26 21) (15 30 29 27 23).

Only three of them satisfy (5); they are

(7 14 28 25 19), (11 22 13 26 21), and (15 30 29 27 23).

We have the relations $7 \ll 15$ and $11 \ll 15$; moreover the antichain

(7 14 28 25 19 11 22 13 26 21)

is the border of the RM-code of order 2, which is self-dual. Clearly if we take, for instance, only the class of 7, we obtain a code which is strictly included in the self-dual RM-code. Hence there is only one antichain which defines an affine-invariant code of dimension 16.

Note that we easily obtain the same result for length 8.

EXAMPLE 2. *There are at most nine self-dual affine-invariant codes of length* 64 *over* $GF(4)$. Let T be the defining set of a self-dual affine-invariant code C of length 64 over $GF(4)$. There are twenty-two cyclotomic cosets of 4 modulo 63; five of them do not satisfy (5); they are the cosets containing 1, 2, 3, 6 and 9 (we quote here the smallest element of each coset). From Corollary 2, T must contain those cosets. But if s is in T, then $n - s$ is not. So we eliminate five cosets:

$$\{\mathrm{cl}(s) \mid s \in \{15, 27, 30, 31, 47\}\}.$$

There remain twelve cosets which are divided in two classes, the cl(s)'s and the corresponding cl($n-s$)'s:

$$s \in \{5, 7, 10, 13, 21, 22\} \quad \text{and} \quad n-s \in \{43, 14, 23, 11, 42, 26\}.$$

Let $I = \{0, 1, 2, 3, 6, 9\}$. Thus T is the union of the cosets containing the elements of $I \cup J$, where J must be composed of six of the twelve cosets above, with the constraints: $s \in T \Rightarrow n-s \notin T$, and $s \in T \Rightarrow \Delta(s) \subset T$. We obtain eighteen distinct sets J. But the mapping $\mu_2 : i \mapsto 2i \pmod n$ has clearly the property that $\mu_2(T)$ is the defining set of a self-dual affine-invariant code equivalent to the code defined by T. Then the number of inequivalent codes defined in this way is at most nine. We give below the defining sets and the borders of the nine codes. For the defining set, we only indicate the set J, since $T = \{0, 1, 2, 3, 6, 9\} \cup J$. We denote by δ the BCH-bound of the code; the value of δ is $s+1$ where s is the smallest element of the border. Among T and $\mu_2(T)$ we choose the defining set which gives the best BCH-bound.

The set J	The border	δ
5, 7, 13, 21, 22, 23	10	11
5, 7, 10, 11, 22, 42	13, 14, 21, 26	14
5, 7, 10, 13, 21, 26	11, 14, 22, 42	12
5, 7, 10, 11, 21, 26	13, 14, 22, 42	14
5, 7, 10, 13, 26, 42	11, 14, 21, 22	12
5, 7, 10, 13, 22, 42	11, 14, 21, 26	12
5, 7, 10, 13, 21, 22	11, 14, 23, 26, 42	12 (GRM)
5, 7, 10, 11, 21, 22	13, 14, 26, 42	14
5, 7, 10, 11, 26, 42	13, 14, 21, 22	14

Among the nine codes obtained, we recognize the GRM-code of order 4, with defining set the union of those cyclotomic cosets with first elements 0, 1, 2, 3, 6, 9 and 5, 7, 10, 13, 21, 22. Its minimum weight is exactly 12. However, we note that the minimal distance of four codes, among the nine codes, is at least 14.

3. The Class of Binary Self-Dual Affine-Invariant Codes

From now on we assume that $K = GF(2)$ and that m is odd. Recall that $n = 2^m - 1$ and $S = [0, n]$. For any $s \in S$, we denote by cl(s) the cyclotomic coset of 2 modulo n containing s. Clearly the elements of a coset have the same 2-weight, the so-called 2-*weight of the cyclotomic coset*. Note that a set composed with cyclotomic cosets of same 2-weight is an antichain. We will

examine separately the self-dual affine-invariant codes of length 128 and 512. But, in all cases our search starts with the following simple properties, easily deduced from Theorem 4.

PROPOSITION 3. *Let T be the defining set of a weakly self-dual affine-invariant code of length 2^m over K with m odd. Then T contains necessarily*:

(i) *The* cl(s) *containing an s such that* $s \leqslant 2^{(m-1)/2} - 1$.

(ii) *The* cl(s) *containing* an $s = \sum_{i=0}^{m-1} s_i 2^i$ *which satisfies*

$$s_{m-1} = 0 \qquad \textit{and} \qquad \{s_1 = 1 \Rightarrow s_2 = 0\}$$

and

$$\{i > 1,\ s_i = 1 \Rightarrow s_{i-1} = s_{i+1} = 0\}.$$

In particular every cyclotomic coset with 2-weight equal to 2 is contained in T. Moreover, when $m > 7$, every cyclotomic coset with 2-weight equal to 3 is contained in T.

Proof. We identify any $s \in S$ with the list of symbols of its 2-expansion.

(i) Let

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

It is easy to see that cl(t) does not satisfy property (5). Now if $s \leqslant t$ then $s \ll t$, which implies that cl(s) also cannot satisfy (5). From Corollary 2, cl(s) is contained in T.

(ii) The general form of s is as follows: s = (..., 0, 1, 0, ..., 0, 1, 0, ..., 0). Then we have obviously $2s \ll n - s$. That means that cl(s) does not satisfy property (5).

Every cyclotomic coset with 2-weight equal to 2 contains an s which satisfies the hypothesis of (i) or of (ii). For a 2-weight equal to 3, the cases which are not covered by (i) or (ii), are for an s with the following form:

$$s = (\underbrace{1, 1, 0, \ldots, 0}_{(m-1)/2}, \underbrace{0, \ldots, 1, \ldots, 0, 0}_{(m+1)/2}).$$

Clearly, for $m > 7$, s satisfies: $4s \ll n - s$. Hence cl(s) does not satisfy (5).

Remark. For $m = 9$, we found cyclotomic cosets of 2-weight 4 that satisfy property (5) (see Example 3). But it is natural to conjecture that for a sufficiently large m, no cyclotomic coset of 2-weight 4 satisfies (5); more precisely there certainly is a relation between m and the 2-weight k such that no cyclotomic coset of 2-weight k satisfies (5).

3.1. *The Self-Dual Binary Affine-Invariant Codes of Length* 128

From Example 1 we know that for length 32 only the RM-code is self-dual and affine-invariant. Now the next length is 128. The following result proves that, in this case, we obtain three self-dual non-equivalent affine-invariant codes.

THEOREM 5. *There are three non-equivalent self-dual affine-invariant codes of length* 128 *over GF*(2), *denoted by* R_i, $i \in \{1, 2, 3\}$. *They have the same parameters* [128, 64, 16]. *They are*

1. R_1, *the Reed–Muller code with border* $\{s \mid \omega_2(s) = 4\}$.
2. R_2, *the code whose border is* cl(11).
3. R_3, *the code whose border is* cl(13).

Proof. In order to prove the theorem, we exhibit those cyclotomic cosets that satisfy property (5). From these cosets, we form all possible antichains, and we keep those that satisfy (5). For each of them, we compute the corresponding defining set. Such a defining set of cardinality 64 corresponds to a self-dual affine-invariant code. We found only three such defining sets. The defining sets of the codes R_2 and R_3 are

$$T(R_2) = \{0, \text{cl}(1), \text{cl}(3), \text{cl}(5), \text{cl}(7), \text{cl}(9), \text{cl}(13), \text{cl}(19), \text{cl}(21), \text{cl}(29)\}.$$

$$T(R_3) = \{0, \text{cl}(1), \text{cl}(3), \text{cl}(5), \text{cl}(7), \text{cl}(9), \text{cl}(11), \text{cl}(19), \text{cl}(21), \text{cl}(23)\}.$$

Let R_i^* denote the punctured code R_i, $i = 2$ or 3. The idempotents of those codes are, respectively,

$$E_2(Z) = \sum_{s \in U_2} Z^s, \qquad U_2 = \{\text{cl}(i) \mid i \in \{1, 3, 5, 15, 19, 21, 23, 29, 55\}\}$$

and

$$E_3(Z) = \sum_{s \in U_3} Z^s, \qquad U_3 = \{\text{cl}(i) \mid i \in \{13, 15, 27, 29, 31, 43, 47, 55, 63\}\}.$$

By a suitable coordinate permutation, $\mu_a : i \to ai \pmod n$ on each set U_i, we can recognize these idempotents among those given in Table II of [14]. For R_2^*, the corresponding splitting is exactly the defining set of R_2^*:

$$\{\text{cl}(i) \mid i \in \{1, 3, 5, 7, 9, 13, 19, 21, 29\}\}.$$

For R_3^*, we found:

$$\{\text{cl}(i) \mid i \in \{1, 3, 7, 9, 11, 21, 23, 27, 47\}\}.$$

Thus we can conclude that the codes R_i, $i \in \{1, 2, 3\}$, are not equivalent. Using Table II, we also know that the minimum weight of these codes is 16. We prove this in another way below (see Appendix A and B). ▮

Using Newton's identities, we can characterize the set of minimum weight codewords of the codes R_2 and R_3. The following results prove that these codes have remarkable properties. Recall that, in this section, $\mathbf{G} = GF(2^7)$.

PROPOSITION 4. *The minimum weight of the codes R_2 and R_3 is* 16 *and the number of codewords of weight* 16 *equals* 127×8, *which is the number of distinct affine subspaces generated by the group of affine-permutations of* $\mathbf{G}$ *acting on a* 4*-dimensional subspace of* $\mathbf{G}$. *More precisely*:

1. *The set of minimum weight codewords of R_2 consists of the codeword $x^{(2)}$ whose locators are the roots of the linearized polynomial of* $\mathbf{G}[Z]$:

$$\begin{aligned} Q_2(Z) &= Z^{16} + Z^8 + Z^4 + Z \\ &= Z(Z+1)(Z^7 + Z + 1)(Z^7 + Z^6 + Z^5 + Z^4 + Z^3 + Z^2 + 1) \end{aligned}$$

and all $\sigma(x^{(2)})$, where σ is an affine permutation of $\mathbf{G}$.

2. *The same property holds for the code R_3, with the linearized polynomial being*

$$\begin{aligned} Q_3(Z) &= Z^{16} + Z^4 + Z^2 + Z \\ &= Z(Z+1)(Z^7 + Z^6 + Z^5 + Z^4 + 1)(Z^7 + Z^3 + 1). \end{aligned}$$

Proof. The reader can find definitions of locators, locator polynomials and Newton's identities in [13, p. 244]. Since the codes concerned are affine-invariant, we can study the set of minimum weight codewords of the punctured code. Indeed if the punctured code C^* has minimum weight δ (δ is always odd in our context), then the code C has minimum weight $\delta + 1$. Let x be a codeword of weight $\delta + 1$ in C, and x^* the punctured word in C^*. Then the weight of x^* is either δ, if 0 is a locator of x, or $\delta + 1$. Moreover there always exists a permutation $\sigma_{1,v}$, defined by (2), and a codeword y^* of weight δ in C^* such that $x = \sigma_{1,v}(y)$.

For our search we use the symbolic computation software Maple. Our method is based on the manipulation of Newton's identities, as it was introduced by Augot *et al.* [2, 3]. For our problem, we want to find a formal representation of the locator polynomial of a minimum weight codeword. The definition of Newton's identities in our context is recalled later (cf. Definition 4). We give in the Appendix A, the characterization of the set of minimum weight codewords of R_3. Here we merely explain our results.

Let x^* be a codeword of weight 15 in R_2^*. We first proved that $\phi_{11}(x)$ must be zero. By shifting x^*, we can suppose that $\phi_{15}(x)=1$, note that, from Definition 1, $\phi_{15}(x)=\phi_{15}(x^*)$. Then we wrote the Newton's identities for any such codeword in order to obtain a formal expression of the locator polynomial. Actually we found only one possible locator polynomial, the polynomial $Q(Z)=Z^{15}+Z^{12}+Z^8+1$. That means that the locators of x are the roots of $Q_2(Z)$. Since Q_2 is a linearized polynomial, then the roots of Q_2 are the elements of a 4-dimensional K-subspace of $\mathbf{G}$. A codeword is uniquely defined by its locator polynomial. Then a codeword of weight 15 in R_2^* is either the codeword defined by Q or a shift of this codeword, i.e., 127 distinct codewords. In the code R_2 the extensions of these 127 codewords have weight 16; each of them produces 8 codewords of weight 16, corresponding to the 8 cosets of a 4-dimensional subspace. In the same way we obtain the set of minimum weight codewords of R_3. ▮

3.2. *An Infinite Class of Self-Dual Binary Affine-Invariant Codes*

Let S_k denote *the maximal antichain of weight k in S.* It is the union of the $\mathrm{cl}(s)$ such that $\omega_2(s)=k$; such antichains are also the borders of RM-codes (cf. (4)). As before, $\mathrm{cl}(s)$ denotes the cyclotomic coset containing s (generally s denotes the smallest element of the coset). The first result in Proposition 3 means that the defining set of a self-dual affine-invariant code contains at least the following antichains

$$S_1, S_2, S_3, S_4\backslash\{l \mid \mathrm{cl}(l) \text{ satisfy (5)}\}.$$

This makes it easy to treat the case $m=9$; the method we use in the following example will be generalized in order to study the full class.

EXAMPLE 3. Assume that $m=9$. Let C be a self-dual affine-invariant code of length 2^9 with defining set T. Because of the preceeding remark, we need only examine the cyclotomic cosets of 2-weight 4. Let $s\in S$ be such that $\omega_2(s)=4$ and suppose $\mathrm{cl}(s)$ satisfies (5). If $s\notin T$, then $n-s\in T$. But $w_2(n-s)=m-w_2(s)=5$. So each time we have such an s not in T, there necessarily is a corresponding cyclotomic coset of 2-weight 5 in T. In other words, the set

$$\{0\}\cup\left(\bigcup_{k\leqslant 3} S_k\right)\cup S_4\backslash\mathrm{cl}(s)\cup\mathrm{cl}(n-s),$$

where $\omega_2(s)=4$, and $\mathrm{cl}(s)$ satisfies (5) is the defining set of a self-dual affine-invariant code. For this value of m, the s such that $\omega_2(s)=4$ with $\mathrm{cl}(s)$ satisfying (5) are 23, 27, 29, 39, 43, 45, 53, 57, 75, 77, and 83.

THEOREM 6. *Let E be the set*

$$E = \{0\} \cup S_1 \cup \cdots \cup S_{(m-3)/3} \cup S_{(m-1)/2} \backslash \mathrm{cl}(s) \cup \mathrm{cl}(n-s),$$

where $\omega_2(s) = (m-1)/2$ and $\mathrm{cl}(s)$ satisfies (5). Then, E is the defining set of an affine-invariant self-dual code of length 2^m over $GF(2)$.

Proof. The set E is clearly a union of cyclotomic cosets of 2 modulo n. We denote by C the code defined by E.

(1) *The code C is affine-invariant.* In accordance with Theorem 2, it suffices to check that E contains all the descendants of its elements. Let $t \in E$. If $t \notin \mathrm{cl}(n-s)$, it is obvious that $\Delta(t) \subset E$. Suppose that $t \in \mathrm{cl}(n-s)$; then $\omega_2(t) = (m+1)/2$. Every element of 2-weight strictly less than $(m-1)/2$ is in E. Moreover a descedant of t of 2-weight $(m-1)/2$ cannot be in $\mathrm{cl}(s)$; indeed:

$$t \in \mathrm{cl}(n-s), \qquad \mathrm{cl}(s) \text{ satisfies } (5) \Rightarrow j \not\preccurlyeq t, \qquad \text{for all } \; j \in \mathrm{cl}(s).$$

(2) *The number of elements of E is 2^{m-1}.* The set E is in fact the defining set of the self-dual RM-code, minus the class of s and plus the class of $n-s$. But it is clear that these classes have the same number of elements.

(3) *The code C is self-dual.* It is easy to check that $t \in E$ if and only if $n - t \notin E$; indeed t is an element of E if and only if it satisfies:

$$\{\omega_2(t) \leqslant (m-1)/2 \text{ and } t \notin \mathrm{cl}(s)\} \qquad \text{or} \qquad t \in \mathrm{cl}(n-s),$$

which is equivalent to

$$\{\omega_2(n-t) \geqslant (m+1)/2 \text{ and } n - t \notin \mathrm{cl}(n-s)\} \qquad \text{or} \quad n - t \in \mathrm{cl}(s),$$

which means $n - t \notin E$. ∎

For the proof of the following corollary, we need the definition of Newton's identities.

DEFINITION 4. Let $X_1, \ldots, X_w$ be w indeterminates with values in $\mathbf{G}$, σ_i their elementary symmetric functions, A_i their power sum symmetric functions. Then the following identities hold:

$$\begin{cases} r \leqslant w, & (id_r)\colon A_r + A_{r-1}\sigma_1 + \cdots + A_1\sigma_{r-1} + r\sigma_r = 0 \\ r > w, & (id_r)\colon A_r + A_{r-1}\sigma_1 + \cdots + A_{r-w}\sigma_w = 0 \end{cases}$$

These identities are called the Newton's identities.

COROLLARY 3. *Assume that m is odd, $m>7$. Let $\mu=(m+1)/2$ and $v=(m-1)/2$. The defining set of the self-dual RM-code is T_v (cf. Definition 3). Let $\lambda=2^\mu-3$.*

There exists an infinite class of self-dual binary affine-invariant codes that is not equivalent to the class of self-dual RM-codes. That is, for each odd m the code C_m with defining set

$$E_m=\{0\}\cup T_v\backslash \mathrm{cl}(\lambda)\cup \mathrm{cl}(n-\lambda),$$

is a self-dual affine-invariant binary code which is not equivalent to a Reed–Muller code.

Proof. Let $s\in S$ and let the 2-ary expansion of s be $\sum_{i=0}^{m-1} s_i 2^i$. We will identify s with the vector $(s_0, ..., s_{m-1})$. We denote by ρ the smallest element of $\mathrm{cl}(n-\lambda)$. Note that $2\mu-1=m$. We have:

$$\lambda=(\underbrace{1, 0, 1, ..., 1}_{\mu}, \underbrace{0, ..., 0}_{\mu-1})$$

and

$$\rho=(\underbrace{1, ..., 1, 0, 1}_{\mu+1}, \underbrace{0, ..., 0}_{\mu-2})=2^{\mu+1}-2^{\mu-1}-1. \tag{6}$$

It is clear that $\omega_2(\lambda)=(m-1)/2$ and that $\mathrm{cl}(\lambda)$ satisfies condition (5). In accordance with Theorem 6, that means that E_m is the defining set of a self-dual affine-invariant code. The BCH-bound of the punctured code C_m^* equals λ; hence the minimum weight of C_m, denoted by δ, is at least $\lambda+1$. But the code C_m is doubly-even; thus its minimum weight is at least $\lambda+3$ (which is the minimum weight of the self-dual RM-code). The parameters of C_m are then $[2^m, 2^{m-1}, \delta\geqslant 2^\mu]$. From now on, we suppose that $\delta=2^\mu$, and we will prove that C_m cannot be equivalent to the self-dual RM-code.

We study a codeword x of weight $d=\delta-1$ in the code C_m^*. We use Newton's identities in our context: such a codeword is identified with its locators $\{X_i \mid i\in[1, d]\}$, or with its locator polynomial. According to Definition 4, the σ_i's are the coefficients of the locator polynomial and A_i's are the coefficients of the Mattson–Solomon polynomial:

$$\sigma(Z)=\prod_{i=1}^{d}(1-X_iZ)=\sum_{k=0}^{d}\sigma_iZ^i$$

and

$$A_i=\sum_{j=1}^{d}X_j^i=\phi_i(x), \qquad \text{for all} \quad i\in[1, n].$$

Then $A_i = 0$ for all $i \in E_m$. Since $A_i = 0$ for $i \in [1, \lambda[$, we first have

$$(id_1), (id_2), \ldots, (id_{\lambda-1}) \Rightarrow \sigma_i = 0, \qquad \text{for all odd } i \text{ such that } \quad i < \lambda. \tag{7}$$

We consider now the identity $(id_{2\rho})$:

$$(id_{2\rho}) : A_{2\rho} + \sum_{k=1}^{d} A_{2\rho-k}\sigma_k = 0.$$

Since $A_{2i} = A_i^2$ and from (7), it can be rewritten as

$$(id_{2\rho}) : A_\rho^2 + \left(\sum_{j=1}^{(\lambda-1)/2} A_{\rho-j}^2 \sigma_{2j} \right) + A_{2\rho-\lambda}\sigma_\lambda + A_{2\rho-\lambda-1}\sigma_{\lambda+1} + A_{2\rho-d}\sigma_d = 0,$$

where

$$(\lambda-1)/2 = 2^{\mu-1} - 2, \qquad 2\rho - \lambda = 2^{\mu+1} + 1, \qquad \text{and} \qquad 2\rho - d = 2^{\mu+1} - 1. \tag{8}$$

First ρ is an element of E_m; so $A_\rho = 0$. Moreover the 2-weight of $2\rho - \lambda$ and $2\rho - \lambda - 1$ is less than 3; thus these elements are in E_m and the corresponding A_i's are zero. Now, using (6) and (8), we can see that the j's always satisfy $j \ll \rho$; that yields $\rho - j \ll \rho$. Since C_m is affine-invariant, every descendant of ρ is also in E_m. Hence the $A_{\rho-j}^2$'s are zero. Finally we obtain: $(id_{2\rho})$: $A_{2\rho-d}\sigma_d = 0$.

The coefficient σ_d cannot be zero, because we are supposing that a codeword of weight d exists. Then we have proved that every codeword of weight d satisfies $A_{2\rho-d} = 0$. From (8), it is clear that $2\rho - d$ is not in E_m, because $\omega_2(2\rho - d) = \mu + 1$. That means that C_m^* cannot be generated by its minimum weight codewords, while the punctured self-dual RM-code can (see [1, Chap. 5] or [13, p. 281]). ▮

4. Conclusion

In this paper we have proved that there are binary codes other than the RM-codes that are self-dual and affine-invariant. But many questions on the full class of self-dual affine-invariant codes remain open. In the binary case, Theorem 6 can easily be generalized

Theorem 7. *Let us denote by* τ *the number of cyclotomic cosets of* 2*-weight* $(m-1)/2$ *satisfying* (5). *Let*

$$E_i = \{0\} \cup S_1 \cup \cdots \cup S_{(m-3)/2} \cup S_{(m-1)/2} \setminus \left(\bigcup_{k=1}^{k=i} \mathrm{cl}(s_k) \right) \cup \left(\bigcup_{k=1}^{k=i} \mathrm{cl}(n - s_k) \right)$$

where $i \leqslant \tau$, $w_2(s_k) = (m-1)/2$, *and the antichain* $\bigcup_{k=1}^{k=i} \mathrm{cl}(s_k)$ *satisfies the weak-self dual condition* (5). *Then,* E_i *is the defining set of an affine-invariant self-dual code.*

That means that it is easy to construct many self-dual binary affine-invariant codes. It is clear to us that the number of non-equivalent elements of the class increases with m; moreover we conjecture that two distinct binary self-dual affine-invariant codes cannot be equivalent. Indeed using the previous theorem, we are able to describe the full class for the length 512. The proof of the following result is given in Appendix C.

COROLLARY 4. *There are seventy self-dual affine-invariant codes of length* 512. *They are not equivalent.*

We have few numerical results on the minimum distance of the codes defined by Theorem 7. We conjecture that it can be no better than the minimum distance of the corresponding RM-codes although we proved that this property is not true for the codes over $GF(4)$ (see Example 2).

When the codes have symbols from $GF(2^r)$, $r > 1$, it is possible to explore the class of self-dual affine-invariant codes with the tools we have introduced here, but is not so easy to obtain numerical results. When $m = 1$, there is one self-dual extended Reed–Solomon code for every r; it is a principal ideal of the algebra $\mathscr{A}$ [4]. The border of an affine-invariant code which is principal consists of only one element [7]. If the code is also self-dual, it is clear that this element can only be 2^i, $i \in [1, r]$. That means that *any self-dual principal affine-invariant code is equivalent to the self-dual extended RS-code.* This remark shows that by adding one property to the definition, we obtain a complete characterization.

APPENDIX

A. *The Set of the Minimum Weight Codewords of the Code* R_3^* *Characterized by Theorem* 5. Recall that the defining set of R_3^* is:

$$E = \{\mathrm{cl}(i) \mid i \in \{1, 3, 5, 7, 9, 11, 19, 21, 23\}\}.$$

We denote by F the set of "non-zeros":

$$F = \{\mathrm{cl}(i) \mid i \in \{13, 15, 27, 29, 31, 43, 47, 55, 63, 127\}\}.$$

Throughout the appendix, i is the smallest element in $\mathrm{cl}(i)$. The code R_3 is doubly-even. Since the BCH-bound is 13, the minimum weight of R_3^* is at least 15 (the minimum weight of R_3 is at least 16). So we are going to study the codewords of weight 15 in the code R_3^*. We use Newton's identities

in our context: such a codeword x is identified with its locators $\{X_i \mid i \in [1, 15]\}$, or with its locator polynomial. According to Definition 4, the σ_i's are the coefficients of the locator polynomials and the A_i's are the coefficients of the Mattson–Solomon polynomial:

$$\sigma(Z) = \prod_{i=1}^{15} (1 - X_i Z) = \sum_{k=0}^{15} \sigma_i Z^i$$

and

$$A_i = \sum_{j=1}^{15} X_j^i = \phi_i(x), \qquad \text{for all} \quad i \in [1, n[.$$

Then $A_i = 0$ for all $i \in E$. Since $A_i = 0$ for $i \in [1, 13[$, we first have:

$$(id_1), (id_2), ..., (id_{11}) \Rightarrow \sigma_1 = \sigma_3 = \sigma_5 = \sigma_7 = \sigma_9 = \sigma_{11} = 0.$$

We compute the Newton's identities with the preceeding hypothesis. Now we will apply successively Stage I and Stage II, as many times as necessary (Stage I and Stage II are only explained the first time).

STAGE I. Consider the equations consisting of only one term or with two simple terms (i.e., no product in any term). We obtain

$$(id_{13}): A_{13} + \sigma_{13} = 0 \Rightarrow \qquad \sigma_{13} = A_{13}$$
$$(id_{46}): A_{31}\sigma_{15} = 0 \quad \Rightarrow A_i = 0, \qquad \text{for all} \quad i \in \text{cl}(31)$$
$$(id_{50}): A_{35}\sigma_{15} = 0 \quad \Rightarrow A_i = 0, \qquad \text{for all} \quad i \in \text{cl}(13).$$

since $35 \in \text{cl}(13)$ and, by definition, σ_{15} cannot be zero.

STAGE II. Affect the values of the A_i's and the σ_i's which are modified by Stage I; compute again the Newton's identities and reduce it modulo 2.

STAGE I.

$$(id_{15}): A_{15} + \sigma_{15} = 0 \qquad (id_{17}): A_{15}\sigma_2 = 0 \qquad (id_{19}): A_{15}\sigma_4 = 0$$
$$(id_{21}): A_{15}\sigma_6 = 0 \qquad (id_{23}): A_{15}\sigma_8 = 0 \qquad (id_{25}): A_{15}\sigma_{10} = 0.$$

Then $\sigma_{15} = A_{15}$. We can assume that $A_{15} = 1$; indeed any codeword x can be shifted in a codeword of same weight, satisfying this equality. Hence we have: $\sigma_2 = \sigma_4 = \sigma_6 = \sigma_8 = \sigma_{10} = 0$.

STAGE II, STAGE I. $(id_{47}): A_{47} = 0 \Rightarrow A_i = 0$, for all $i \in \text{cl}(47)$.

STAGE II, STAGE I.

$$(id_{45}): A_{45}+1=0 \Rightarrow A_i=1, \quad \text{for all} \quad i \in \text{cl}(43)$$
$$(id_{113}): 1+\sigma_{14}=0 \Rightarrow \quad \sigma_{14}=1,$$

since 45 is an element of cl(43).

STAGE II, STAGE I.

$$(id_{29}): A_{29}+1=0 \Rightarrow A_i=1, \quad \text{for all} \quad i \in \text{cl}(29)$$
$$(id_{57}): 1+\sigma_{12}=0 \Rightarrow \quad \sigma_{12}=1$$
$$(id_{59}): A_{59}+1=0 \Rightarrow A_i=1, \quad \text{for all} \quad i \in \text{cl}(55)$$
$$(id_{104}): A_{89}+1=0 \Rightarrow A_i=1, \quad \text{for all} \quad i \in \text{cl}(27),$$

since $59 \in \text{cl}(55)$ and $89 \in \text{cl}(27)$.

STAGE II, STAGE I. $(id_{63}): A_{63}+1=0 \Rightarrow A_i=1$, for all $i \in \text{cl}(63)$.

STAGE II. At this moment, all the (id_i) are satisfied, and all the σ_i's and the A_i's have values in $GF(2)$. We obtain only one locator polynomial:

$$\sigma(Z)=1+Z^{12}+Z^{14}+Z^{15}.$$

We verify that this polynomial has 15 distinct roots in $GF(2^7)$. Moreover the codeword x has odd weight; then $A_{127}=1$. Thus the codeword x is the primitive idempotent of the cyclic code with non-zeros α^i, where i is in the subset of F:

$$\{\text{cl}(i) \mid i \in \{15, 27, 29, 43, 55, 63, 127\}\}.$$

B. *The Minimum Weight of the Code* R_2^*. Recall that the defining set of R_2^* is

$$E' = \{\text{cl}(i) \mid i \in \{1, 3, 5, 7, 9, 13, 19, 21, 29\}\}.$$

Since the BCH-bound is 11, the minimum weight of R_2^* is at least 11 (the minimum weight of R_2 is at least 12). The weight 12 can be a weight of the doubly-even code R_2. So, in the same way as in Appendix A, we study the codewords of weight 11 in the code R_2^*. The hypothesis is here $A_i=0$, for $i \in E'$, which yields $\sigma_j=0$, for $j \in \{1, 3, 5, 7, 9\}$. Computing the Newton's identities, we obtain

$$(id_{11}): A_{11}+\sigma_{11}=0 \quad \text{and} \quad (id_{80}): A_{69}\sigma_{11}=0,$$

where $69 \in \mathrm{cl}(11)$. Thus $A_{11} = 0$. So there is no codeword of weight 11 in R_2^*; the minimum weight is at least 15. With the method of Appendix A, we can describe the set of words of weight 15.

C. *The Self-Dual Affine-Invariant Codes of Length* 512 *over GF*(2). We give here all self-dual affine-invariant codes of length 512. The codes are given by their defining sets. The method of construction is deduced from Theorem 7. The cyclotomic cosets that do not satisfy (5) are, as quoted at the beginning of Section 3.2, the cyclotomic cosets with 2-weight less than or equal to 3, and the ones of 2-weight 4 except

$$\mathrm{cl}(s),\ s \in I, \qquad I = \{23, 27, 29, 39, 43, 45, 53, 57, 75, 77, 83\}.$$

So we already have eleven (possibly equivalent) self-dual affine-invariant codes, namely those with defining set

$$\text{for all } s, \qquad s \in I\text{: } D_s = \{u \in [0, 511] \mid \omega_2(u) \leqslant 4,\ u \notin \mathrm{cl}(s)\} \cup \mathrm{cl}(n-s).$$

Next we formed all combinations of two cyclotomic cosets:

$$\mathrm{cl}(s) \cup \mathrm{cl}(t) \qquad \text{such that} \quad s \in I,\ t \in I \quad \text{and} \quad \mathrm{cl}(s) \cup \mathrm{cl}(t) \text{ satisfies (5).}$$

We found thirty-three such combinations, that are quoted below:

LIST 1.

s	t	s	t
23	27, 39, 43, 75, 77, 83	43	45, 57, 75, 77
27	29, 43, 45, 53, 83	45	53, 57, 83
29	53, 57, 75, 77, 83	53	75, 77
39	45, 53, 75, 77, 83	57	75, 77, 83

This yields thirty-three self-dual affine-invariant codes, with defining set

$$D_{s,t} = \{u \in [0, 511] \mid \omega_2(u) \leqslant 4,\ u \notin \mathrm{cl}(s),\ u \notin \mathrm{cl}(t)\} \cup \mathrm{cl}(n-s) \cup \mathrm{cl}(n-t)$$

s, t as in List 1.

Among the s's and t's of List 1, we tried and found the elements s, t, r such that the antichain composed with $\mathrm{cl}(s)$, $\mathrm{cl}(t)$ and $\mathrm{cl}(r)$ satisfies property (5):

LIST 2.

s	t	r	s	t	r	s	t	r
23	27	43, 83	27	43	45	39	45	53, 83
23	39	75, 77, 83	27	45	53, 83	39	53	75, 77
23	43	75, 77	29	53	75, 77	43	45	57
27	29	53, 83	29	57	75, 77, 83	43	57	75, 77, 83

And, as before, the following 25 defining sets are defining sets of affine-invariant self-dual codes:

$$D_{s,t,r} = \{u \in [0, 511] \mid w(u) \leqslant 4, u \notin J\} \cup J',$$

where $J = \mathrm{cl}(s) \cup \mathrm{cl}(t) \cup \mathrm{cl}(r)$, $J' = \mathrm{cl}(n-s) \cup \mathrm{cl}(n-t) \cup \mathrm{cl}(n-r)$ and s, t, r as in List 2.

Together with the Reed–Muller code, we obtain at this stage $11 + 33 + 25 + 1 = 70$ affine-invariant self-dual (possibly equivalent) codes of length 512. But since no combination of four cosets containing elements of I can satisfy property (5), the previous list is exhaustive.

Next we want to known if some of them are equivalent. Let ψ be the Euler function. We have

$$\psi(511) = \psi(7)\,\psi(73) = 6 \times 72 = 432 = 3^3 \times 2^4.$$

Then 511 and $\psi(511)$ are relatively prime. Hence two cyclic codes of length 511 are equivalent if and only if they are equivalent by a coordinate permutation $\mu_a: i \to ai$, with a prime to 511 [8, 15]. The mapping μ_α is called a *multiplier*. So we applied the multipliers μ_a, with a prime to 511, to each of the defining-sets of the seventy codes. All the sets obtained by these permutations were different. Then we can conclude that *the seventy self-dual affine-invariant codes of length* 512 *are non-equivalent.*

ACKNOWLEDGMENTS

The authors thank E. F. Assmus Jr. for his helpful suggestions and his careful reading that greatly improved the manuscript. They express their gratitude to V. Pless for useful discussions; in particular she indicated the way to show the nonequivalence of the seventy affine-invariant self-dual codes of length 512. All numerical results were verified by two different programs. The authors are also indebted to N. Sendrier and D. Augot for checking some numerical results with their own programs.

REFERENCES

1. E. F. ASSMUS, JR, AND J. D. KEY, Designs and their codes, *in* "Cambridge Tracts in Mathematics," Volume 103, Cambridge Univ. Press, London/New York, 1992.

2. D. AUGOT, P. CHARPIN, AND N. SENDRIER, The minimum distance of some binary codes via the Newton's Identities, "EUROCODE '90," Lecture Notes in Computer Science, Vol. 514, pp. 65–73, Springer-Verlag, New York/Berlin.
3. D. AUGOT, P. CHARPIN, AND N. SENDRIER, Studying the locator polynomials of minimum weight codewords of BCH-codes, *IEEE Trans. Info. Theory* **38**, No. 3 (May 1992), 960–973.
4. P. CHARPIN, The extended Reed–Solomon codes considered as ideals of a modular algebra, *Ann. Discrete Math.* **17** (1983), 171–176.
5. P. CHARPIN, Codes cycliques étendus invariants sous le groupe affine, Thèse de Doctorat d'Etat, Univ. PARIS VII, 1987.
6. P. CHARPIN, Some applications of a classification of affine-invariant codes, *in* "AAECC5," Lecture Notes in Computer Science, Vol. 356, Springer-Verlag, New York/Berlin.
7. P. CHARPIN, Codes cycliques étendus affines-invariants et antichaînes d'un ensemble partiellement ordonné, *Discrete Math.* **80** (1990), 229–247.
8. W. C. HUFFMAN, V. JOB AND V. PLESS, Multipliers and generalized multipliers of cyclic objects and cyclic codes, *J. Combin. Theory Ser. A* **62** (1993), 183–215.
9. T. KASAMI, S. LIN, AND W. W. PETERSON, New generalisations of the Reed–Muller codes, *IEEE Trans. Inform. Theory* **II-14** (1968), 189–199.
10. T. KASAMI, S. LIN, AND W. W. PETERSON, Some results on cyclic codes which are invariant under the affine group and their applications, *Inform. and Control* **11** (1967), 475–496.
11. J. S. LEON, J. M. MASLEY, AND V. PLESS, Duadic codes, *IEEE Trans. Inform. Theory* **IT-30** (1984), 709–714.
12. F. J. MACWILLIAMS, A. M. ODLYSKO, N. J. A. SLOANE, AND H. N. WARD, Self-dual codes over *GF*(4), *J. Combin. Theory Ser. A* **23** (1978), 288–318.
13. F. J. MACWILLIAMS AND N. J. A. SLOANE, "The Theory of Error Correcting Codes," North-Holland, Amsterdam, 1986.
14. V. PLESS, J. M. MASLEY, AND J. S. LEON, On weights in duadic codes, *J. Combin. Theory Ser. A* **44** (1987), 6–21.
15. V. PLESS, Duadic codes and generaliztions, *in* "Proceedings of EUROCODE '92," Springer-Verlag-Vien, to appear.