# Self-dual codes which are principal ideals of the group algebra "F2[F2m,+]"

Pascale Charpin

HAL Id: inria-00074349
https://inria.hal.science/inria-00074349

Submitted on 24 May 2006

# INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

# Self-Dual Codes which are Principal Ideals of the Group Algebra $\mathbb{F}_2[\{\mathbb{F}_{2^m}, +\}]$

Pascale CHARPIN

N° 2325
Août 1994

PROGRAMME 2

*apport de recherche*

# Codes principaux autoduaux de l'algèbre de groupe $\mathbb{F}_2[\{\mathbb{F}_{2^m}, +\}]$

# Self-dual codes which are principal ideals of the group algebra $\mathbb{F}_2[\{\mathbb{F}_{2^m}, +\}]$ *

Pascale CHARPIN**

## Résumé

Cet article est un prolongement du travail de Paul CAMION portant sur les codes autoduaux, idéaux principaux de l'algèbre $\mathbb{F}_2[\{\mathbb{F}_{2^m}, +\}]$. Dans [5], ces codes sont introduits et appelés $H$-codes. Notre principal résultat ici est que les $H$-codes sont aymptotiquement mauvais, au sens de la borne de Gilbert-Varshamov. Pour obtenir ce résultat, nous exhibons d'abord une borne supérieure pour la distance minimale de tout $H$-code donné. Nous caractérisons les $H$-codes extrémaux et montrons que leurs générateurs sont liés à certains ensembles à différence.

## Abstract

This paper follows up CAMION's contribution on self-dual codes which are principal ideals of the algebra $\mathbb{F}_2[\{\mathbb{F}_{2^m}, +\}]$, the so-called $H$-codes. Our main result is that this class of codes does not meet the Gilbert-Varshamov bound. We obtain this result by giving an upper bound on the minimal distance of any $H$-code. We characterize extremal $H$-codes and link up their generators with certain difference sets.

**Keywords:** self-dual codes, extremal codes, group algebra, difference sets.

# Self-dual codes which are principal ideals of the group algebra $\mathbb{F}_2[\{\mathbb{F}_{2^m}, +\}]$

## 1  Introduction

Let $C$ be a binary linear code of length $n$. The code $C$ is said to be *self-dual* if and only if it is equal to its dual; in this case its dimension is $n/2$. A code is said to be $t$-divisible when the distance between codewords is always a multiple of $t$. By convention a $t$-divisible code is not $t'$-divisible for $t' > t$.

Our main reference on self-dual codes is [17, chapter 19], where an extensive study of the work of GLEASON is given. A binary $t$-divisible self-dual code exists for only two values of $t$: $t = 2$ or $4$. When $t = 2$ we say that the code is *even*; when $t = 4$ we say that the code is *doubly-even*. An important result on these self-dual codes was obtained by GLEASON when he established strong constraints on their weight enumerators [14]. Then an upper bound on the minimal distance of these codes appeared; a code which meets this bound is said to be extremal. Many questions on the existence of extremal self-dual codes remain open.

*Binary H-codes* were introduced by CAMION in [5]. They form a class of binary self-dual codes which are principal ideals of a modular algebra of type $\mathbb{F}_2[G]$, $G = \{\mathbb{F}_{2^m}, +\}$. Basic properties of such codes are given in [5]. Above all it is shown that it is very easy to construct an $H$-code; it is sufficient to choose a hyperplane $H$ of $G$ and a codeword x of odd weight whose support is contained in $H$. A generator matrix is directly obtained. The code is even if and only if the weight of x is congruent to 1 modulo 4; otherwise the code is doubly-even. It is also shown in [5] that there are many extremal doubly-even $H$-codes of length 32. In fact many will be equivalent because there are only five extremal codes of length 32 [13, 15]. Our purpose in this paper is to study asymptotic properties of the minimal distance of $H$-codes.

We will denote by $\mathcal{A}$ the algebra $\mathbb{F}_2[G]$. In Section 2, we present the class of H-codes, giving a brief review of properties of the algebra $\mathcal{A}$; more details on codes of $\mathcal{A}$ can be found in [2, 8, 11]. Recall that the powers of the radical of $\mathcal{A}$ are the Reed-Muller codes [4].

Extremal $H$-codes are studied in Section 3. We first give an upper bound on the minimal distance of any $H$-code (Theorem 3). We can then deduce that $H$-codes are asymptotically bad; moreover we prove that there are no extremal $H$-codes of length greater than 32.

The last section treats the extremal $H$-codes of length 32. Our main result is presented in Theorem 5, linking extremal H-codes to difference sets of the abelian group $\{\mathbb{F}_{16}, +\}$.

The usual terminology of coding theory can be found in [17]. In this paper we only treat binary linear codes of length $2^m$. The distance is always the Hamming distance.

# 2 The class of H-codes

## 2.1 The algebra $\mathcal{A}$

Let $G$ be the additive group of the finite field $\mathbb{F}_{2^m}$. We denote by $\mathcal{A}$ the algebra of the group $G$ over the field $\mathbb{F}_2$. An element of $\mathcal{A}$ is a formal sum

$$\mathsf{x} = \sum_{g \in G} x_g X^g, \; x_g \in \mathbb{F}_2 \; .$$

For any $a \in \mathbb{F}_2$, $b \in \mathbb{F}_2$, $\mathsf{x} \in \mathcal{A}$ and $\mathsf{y} \in \mathcal{A}$, we have:

$$a\mathsf{x} + b\mathsf{y} = a \sum_{g \in G} x_g X^g + b \sum_{g \in G} y_g X^g = \sum_{g \in G} (ax_g + by_g) X^g \; ,$$

$$\mathsf{xy} = \sum_{g \in G} x_g X^g \sum_{g \in G} y_g X^g = \sum_{h \in G} \left( \sum_{g \in G} x_g y_{h+g} \right) X^h \; ,$$

The additive and multiplicative unit elements are $0 = \sum_{g \in G} 0 \, X^g$ and $1 = X^0$. In this paper, the algebra $\mathcal{A}$ is the ambient space of the codes. A code of $\mathcal{A}$ is an $\mathbb{F}_2$-subspace. A codeword is an element of $\mathcal{A}$. Note that an ideal of $\mathcal{A}$ is a code invariant under the multiplication by $X^g$, for any $g \in G$. The scalar product is $< \mathsf{x}, \mathsf{y} >= \sum_{g \in G} x_g y_g$. The dual of a code $C$ will be denoted by $C^\perp$. If $C$ is an ideal, the annihilator of $C$ is:

$$Ann \; C = \{ \, \mathsf{x} \in \mathcal{A} \mid \mathsf{xy} = 0 \; \text{for all} \; \mathsf{y} \in C \, \} \; .$$

Since $\mathsf{xy} = \sum_{h \in G} < \mathsf{x}, X^h \mathsf{y} > X^h$, the following proposition is obvious:

**Proposition 1** *Let $C$ be an ideal of $\mathcal{A}$. Then $Ann \; C = C^\perp$.*

Since $G$ is an elementary abelian 2-group and $a^2 = a$ for $a \in \mathbb{F}_2$. we have for any element $\mathsf{x}$ of $\mathcal{A}$:

$$\mathsf{x}^2 = \left( \sum_{g \in G} x_g X^g \right)^2 = \sum_{g \in G} x_g X^{2g} = \left( \sum_{g \in G} x_g \right) X^0 \; .$$

That means that $\mathsf{x}$ is invertible in $\mathcal{A}$ if and only if its weight is odd. The set of non invertible codewords is the only maximal ideal of $\mathcal{A}$, its so-called *radical*. We will denote by $\mathcal{P}$ the radical of $\mathcal{A}$; that is

$$\mathcal{P} = \{ \, \mathsf{x} \in \mathcal{A} \mid \sum_{g \in G} x_g = 0 \, \} = \{ \, \mathsf{x} \in \mathcal{A} \mid \mathsf{x}^2 = 0 \, \} \; .$$

For any $j \in [1, m]$ we define the ideal which is the $j$-power of $\mathcal{P}$. The ideal $\mathcal{P}^j$ is generated linearly by elements of the form $\prod_{i=1}^{j} \mathsf{x}_i$ where $\mathsf{x}_i \in \mathcal{P}$. For any basis $\{e_1, \ldots, e_m\}$ of $G$, the $2^m$ elements

$$\left\{ \; \prod_{i=1}^{m} (X^{e_i} + 1)^{\lambda_i} \mid \lambda_i \in \{0, 1\} \; \right\}$$

form a linear basis for $\mathcal{A}$. Moreover, for all $j \in [1, m]$, the elements of

$$\mathcal{B}^j = \left\{ \prod_{i=1}^{m} (X^{e_i} + 1)^{\lambda_i} \mid j \leq \sum_{i=1}^{m} \lambda_i \, , \, \lambda_i \in \{0, 1\} \right\} \tag{1}$$

form a linear basis of $\mathcal{P}^j$ (by convention, $\mathcal{P}^0 = \mathcal{A}$) [8]. We now define a useful parameter of an element or of a subset of $\mathcal{A}$:

**Definition 1** *Let* $x \in \mathcal{A}$ *; let* $U$ *be a subset of* $\mathcal{A}$. *Let* $j \in [0, m]$.

- *We will say that the depth of* x *equals* $j$ *if and only if* x *is in* $\mathcal{P}^j$ *and not in* $\mathcal{P}^{j+1}$.

- *We will say that the depth of* $U$ *equals* $j$ *if and only if* $U$ *is included in* $\mathcal{P}^j$ *and not included in* $\mathcal{P}^{j+1}$.

In the following we will use several representations of codewords of depth 1. Two of them are given in Lemma 1. It is clear, by means of the basis $\mathcal{B}^0$, that a codeword z of depth 0 is of the form:

$$z = X^0 + z' = 1 + z' \, , \quad z' \in \mathcal{P} \, . \tag{2}$$

**Lemma 1** *Let* $x \in \mathcal{A}$ *be a codeword of depth* 1. *By using the basis* $\mathcal{B}^1$*(cf. (1)), we have:*

$$x = \sum_{i=1}^{m} a_i (X^{e_i} + 1) + y \, , \quad y \in \mathcal{P}^2 \, , \quad a_i \in \mathbb{F}_2 \, , \tag{3}$$

*where at least one* $a_i$ *is not zero. Set* $h = \sum_{i=1}^{m} a_i e_i$. *Then*

$$x = (X^h + 1) + x' \, , \quad x' \in \mathcal{P}^2 \, . \tag{4}$$

*Proof:* We can assume that $a_1 \neq 0$ in (3). Since $e_1 = h + \sum_{i=2}^{m} a_i e_i$, we have

$$\begin{aligned}
X^{e_1} + 1 &= X^h \prod_{i=2}^{m} X^{a_i e_i} + 1 = ((X^h + 1) + 1) \left( \prod_{i=2}^{m} ((X^{e_i} + 1)^{a_i} + 1) \right) + 1 \\
&= (X^h + 1) + \sum_{i=2}^{m} a_i (X^{e_i} + 1) + y \, , \quad y \in \mathcal{P}^2 \, .
\end{aligned}$$

Then, according to (3), $x = (X^h + 1) + y$ .
□

BERMAN proved in [4] that the powers of the radical of $\mathcal{A}$ are the Reed-Muller codes (RM-codes). More precisely:

$$\mathcal{P}^j = R(m - j, m) \, , \quad \text{for all } j \in [1, m] \, , \tag{5}$$

where $R(m - j, m)$ is the RM-code of length $2^m$ and order $m - j$ (see an easy proof in [1]).

**Remark 1:** From well-known properties of RM-codes or by using the bases $\mathcal{B}^j$, it follows easily that :

1. $\mathcal{P}^{m+1} = \{0\}$ and $\mathcal{P}^m = \{ a \sum_{g \in G} X^g \mid a \in \mathbb{F}_2 \}$ ;

2. The minimal distance of $\mathcal{P}^j$ equals $2^j$.

3. $(\mathcal{P}^j)^{\perp} = Ann \, \mathcal{P}^j = \mathcal{P}^{m-j+1}$ ;

4. Since $\mathcal{P}^{m-1}$ is the RM-code of order 1, the set $\mathcal{P}^{m-1} \backslash \mathcal{P}^m$ contains the elements of $\mathcal{A}$ whose supports are the affine hyperplanes of $G$ ;

5. Any ideal of $\mathcal{A}$ of depth $j$ contains $\mathcal{P}^m$ and is such that its intersection with $\mathcal{P}^k$, $k \geq j$ is not empty.

The *support* of a codeword $x = \sum_{g \in G} x_g X^g$ is:

$$supp(x) = \{ g \in G \mid x_g = 1 \} .$$

Recall that the cardinal of $supp(x)$ is the *weight* of x, which we will denote by $\omega(x)$. We will use also the notation $\mathbb{F}_2 G$ instead of $\mathcal{A}$. More generally the notation $\mathbb{F}_2 V$, where $V$ is an $\mathbb{F}_2$-subspace of $G$, will appear. It is because we will often need to study some codeword whose support is contained in some $V$. For instance the *restriction* of x to $V$ is $x' = \sum_{g \in V} x_g X^g$ and we can identify it with a codeword of the algebra $\mathbb{F}_2 V$. The following lemma will be very useful for the proof of Theorem 3.

**Lemma 2** *Let $V$ be a subspace of $G$ of dimension $k$. Let $W$ be a subset of $G$ of $2^{m-k}$ elements, which contains one representative of each coset of $V$ : $W$ is such that $G$ is equal to $\cup_{h \in W}(h + V)$. Let x in $\mathcal{A}$ and $y = \sum_{g \in V} X^g$. Let us denote by $x(h)$, $h \in W$, the restriction of $X^h x$ to $V$. So x can be written as follows :*

$$x = \sum_{h \in W} x(h) X^h \quad , \quad x(h) \in \mathbb{F}_2 V .$$

*Then either $x(h)$ is invertible and the restriction of yx to $h + V$ equals $yX^h$ or $x(h) \in \mathcal{P}$ and the restriction of yx to $h + V$ equals 0. The weight of yx equals $\lambda 2^k$, where $\lambda$ is the number of $h \in W$ such that $x(h)$ is invertible.*

*Proof.* The codeword y can be considered as an element of $\mathbb{F}_2 V$ ; it is the all-one vector of $\mathbb{F}_2 V$. Note that, for any basis $(e_1, \ldots, e_k)$ of $V$, y equals $\prod_{i=1}^{k}(X^{e_i} + 1)$. So $y \in \mathcal{P}^k$ and $\mathcal{P}^{k+1} \cap \mathbb{F}_2 V = \{0\}$. We have

$$yx = \sum_{h \in W} yx(h) X^h \quad , \quad yx(h) \in \mathcal{P}^k \cap \mathbb{F}_2 V .$$

Whenever $x(h) \in \mathcal{P}$ the product $yx(h)$ is zero, since its depth is $k + 1$. If $x(h)$ is invertible, then $x(h) = 1 + z$ , $z \in \mathcal{P}$, which yields $yx(h) = y$.
$\square$

## 2.2 Principal ideals of depth 1

The definition of the $H$-codes and the properties given in this section are mainly due to CAMION [5]. We denote by $(x)$ the principal ideal generated by an element $x$ of $\mathcal{A}$. That is

$$(x) = \{ yx \mid y \in \mathcal{A} \} .$$

A generator of $(x)$ is an element $yx$ such that $y$ has depth 0 (i.e. is invertible); all generators have the same depth. Since the ideal $(x)$ equals $(yx)$ for all such $y$, we always will consider $x$ as a formal generator that we can fix when it is necessary. In accordance with Proposition 1, an element $z$ is in the dual of the ideal $(x)$ if and only if it is in its annihilator. So

$$(x)^{\perp} = Ann\ (x) = \{ z \in \mathcal{A} \mid zx = 0 \} .$$

The algebra $\mathcal{A}$ itself is the only principal ideal of depth 0. When $x \in \mathcal{P}$ , then $x^2 = 0$ which yields that the ideal $(x)$ is contained in its dual ; the dimension of $(x)$ is less than or equal to $2^{m-1}$.

From now on we assume that $x$ has depth 1 – i.e. $x \in \mathcal{P} \backslash \mathcal{P}^2$ . We assume that $x$ is written as in (3); we can suppose, without loss of generality, that $a_1 = 1$. Hence the restriction of $x$ to the hyperplane $H$ generated by $(e_2, ..., e_m)$ is invertible. Indeed set $z = \sum_{g \in H} X^g$ ; using (3), with $a_1 = 1$, we obtain:

$$zx = \prod_{i=2}^{m}(X^{e_i} + 1)\, x = \prod_{i=1}^{m}(X^{e_i} + 1) = \sum_{g \in G} X^g ,$$

which implies, with the notation of Lemma 2, that

$$x = x(0)X^0 + x(h)X^h , \quad h \notin H ,$$

where $x(0)$ and $x(h)$ are invertible elements of $\mathbb{F}_2 H$. Note that if $x \in \mathcal{P}^2$ the product $zx$ is zero for any hyperplane $H$. By multiplying $x$ by $x(0)$, we obtain a generator of $(x)$ of the form

$$X^0 + x'X^h , \quad h \notin H , \quad x' \text{ invertible} , \quad x' \in \mathbb{F}_2 H . \tag{6}$$

Now it is clear that the set $\{ X^g + (x'X^g)X^h \mid g \in H \}$ is a linearly independent subset of $(x)$ containing $2^{m-1}$ elements. Since $dim\ (x) \leq 2^{m-1}$ , it is a basis of $(x)$. More generally the set $\{ X^g x \mid g \in H \}$ it is a basis of $(x)$. Then we have proved the following theorem.

**Theorem 1** *Let $x$ in $\mathcal{A}$. Recall that $\mathcal{A} = \mathbb{F}_2 G$ where $G$ is the additive group of $\mathbb{F}_{2^m}$.*

*(i) The element $x$ is of depth 1 if and only if there exists a hyperplane $H$ of $G$ such that the restriction of $x$ to $H$ (respectively to $h + H$ , $h \notin H$) is invertible.*

*(ii) Assume that $x$ is of depth 1. Then the ideal $(x)$ is self-dual. Its dimension equals $2^{m-1}$. The code $(x)$ is said to be an $H$-code, where $H$ is a hyperplane of $G$ such that*

$$x = x' + x''X^h , \quad h \notin H , \quad supp(x') \subset H , \quad supp(x'') \subset H ,$$

*where* x′ *and* x″ *are invertible. The set* { $X^g$x | $g \in H$ } *is a basis of* (x). *The generators of* (x) *are the*

$$\sum_{g \in H} a_g \, X^g \text{x} \, , \quad a_g \in \mathbb{F}_2, \quad \text{where} \quad \sum_{g \in H} a_g X^g \text{ is invertible} \, .$$

*There is a generator of* (x) *of the form (6).*

*The H-codes are the principal ideals of depth 1.*

**Remark 2:** Principal ideals of depth 1 of the algebra $K[G]$, $K = \mathbb{F}_{2^r}$ and $G = \mathbb{F}_{2^m}$, are self-dual. WOLFMANN proved that the binary image of such codes, relative to a convenient basis, are binary self-dual codes, which can be doubly-even [19]. For instance an extremal $[64, 32, 12]$ code was constructed in this way [18].

An $H$-code (x) is contained in $\mathcal{P}$; thus it is an even self-dual code. Moreover (x) has a generator matrix all of whose rows have the same weight as x. So it is easy to determine if the code is doubly-even or not, since a binary self-dual code is doubly-even if and only if every row of its generator matrix has a weight divisible by 4.

**Corollary 1** *Let* x *be an element of* $\mathcal{A}$ *of depth 1. Then the principal ideal* (x), *generated by* x, *is an even self-dual code. Moreover* (x) *is doubly-even if and only if the weight of* x *is divisible by* 4.

**Constructing a doubly-even self-dual code of length $2^m$.** We can summarize as follows the construction of the generator matrix of an $H$-code of length $2^m$:

- Choose a hyperplane $H$ of the $\mathbb{F}_2$-vector space $\mathbb{F}_{2^m}$.

- Get a codeword x′ of odd weight whose support is contained in $H$. That means that x′ is an invertible element of $\mathbb{F}_2 H$.

- Compute the $2^{m-1} \times 2^{m-1}$ matrix $M$ whose rows are the codewords $X^h$x′, $h \in H$.

Let $I$ be the $2^{m-1} \times 2^{m-1}$ identity matrix. Then the code with generator matrix $[\, I \mid M \,]$ is an even self-dual $[2^m, 2^{m-1}]$ code. This code is doubly-even if and only if the weight of x′ satisfies : $\omega(\text{x}') \equiv 3 \mod 4$.

## 3 Extremal H-codes

One corollary of GLEASON's result [14] is an upper bound on the minimal distance of the even (respectively doubly-even) self-dual codes. The proof of the following theorem can be found in [17, ch. 19].

**Theorem 2** *The minimum distance of a binary self-dual code with all weights divisible by t (and not by $t' > t$) is at most $d^*$ where:*

- *if $t = 2$ then $d^* = 2[n/8] + 2$ ;*

7

- *if $t = 4$ then $d^* = 4[n/24] + 4$.*

*A self-dual code which has minimal distance $d^*$ is said to be extremal. All extremal even (respectively doubly-even) codes of the same length have the same weight enumerator.*

In this section we want to prove that there are no extremal $H$-codes of length greater than 32. Moreover we point out that the class of $H$-codes is asymptotically bad. In order to do that we first determine an upper bound for the minimal distance of every $H$-code. This bound is given in Table 1 for $m < 14$.

**Theorem 3** *Recall that $\mathcal{A} = \mathbb{F}_2 G$ , with $G = \mathbb{F}_{2^m}$, $m > 0$. Let $(x)$ be an $H$-code in $\mathcal{A}$. Then, for each $i$, $i \geq 0$, such that $i + 2^{i-1} \leq m$ , there exists an element $y$ of $(x)$ whose support is a subspace of $G$ of dimension $m - i$.*

*Let $d$ be the minimal distance of $(x)$ and set*

$$i^* = \max \{ \ i \in \mathbb{N} \mid i + 2^{i-1} \leq m \ \} \ .$$

*Then $d \leq 2^{m-i^*}$ .*

*Proof:* Throughout the proof we will assume that $x$ is an element of depth 1 of $\mathcal{A}$ and we will study the principal ideal $(x)$. We will prove the first part of the theorem by induction on $i$.

The property is satisfied when $i = 0$, for any $m$, since each ideal of $\mathcal{A}$ contains the all-one vector $\sum_{g \in G} X^g$. If $i = 1$ the property is satisfied for any $m > 1$ since $(x)$ contains some codewords whose support is a hyperplane of $G$ (see Remark 1).

We suppose now that $i > 1$ and that the property is satisfied up to $i - 1$. Hence we assume that

$$(i - 1) + 2^{i-2} \leq m \implies \text{there exists } y \in (x) \text{ such that } supp(y) \text{ is a subspace}$$
$$\text{of } G \text{ of dimension } m - (i - 1) \ . \tag{7}$$

Now we want to prove that the property is satisfied for $i$.

1) We first suppose that $m = i + 2^{i-1}$ . In accordance with (7) there exists an $y \in (x)$ such that $supp(y)$ is a subspace $V$ of $G$ of dimension $k = m - i + 1$. Let $W$ be the set of representatives of cosets of $V$. With notation of Lemma 2 we have

$$x = \sum_{h \in W} x(h) X^h \quad \text{where} \quad x(h) \in \mathcal{P} \cap \mathbb{F}_2 V \ .$$

Indeed $y \in (x)$ implies $yx = 0$ which means that each $x(h)$ is in $\mathcal{P}$ (from Lemma 2). Note that $W$ contains $2^{m-k} = 2^{i-1}$ elements. Whenever $x(h)$ is of depth 1, $x(h)$ can be written as follows (according to (4)):

$$x(h) = (X^{h'} + 1) + x' \quad , \quad h' \in V \backslash \{0\} \ , \quad x' \in \mathcal{P}^2 \ . \tag{8}$$

Let $Q$ be the subspace of $G$ generated by these elements $h'$. Since there are $2^{i-1}$ elements $x(h)$, the dimension of $Q$ is less than or equal to $2^{i-1}$. By hypothesis, the dimension of $V$

| $m$ | $i^*$ | $d \leq$ | $m$ | $i^*$ | $d \leq$ | $m$ | $i^*$ | $d \leq$ |
|---|---|---|---|---|---|---|---|---|
| 2 | 1 | 2 | 3 | 1 | 4 | 4 | 2 | 4 |
| 5 | 2 | 8 | 6 | 2 | 16 | 7 | 3 | 16 |
| 8 | 3 | 32 | 9 | 3 | 64 | 10 | 3 | 128 |
| 11 | 3 | 256 | 12 | 4 | 256 | 13 | 4 | 512 |

Table 1: The upper bound of the minimum distance of any $H$-codes of length $2^m$, $m \leq 13$. Notation is that of Theorem 3.

equals $2^{i-1} + 1$. Hence there exists a hyperplane $V'$ of $V$ containing $Q$. Set $z = \sum_{g \in V'} X^g$ and note that $z \in \mathcal{P}^{k-1} \cap \mathbb{F}_2 V$ ; then we have

$$zx = \sum_{h \in W} zx(h) X^h \quad \text{where} \quad zx(h) \in \mathcal{P}^{k-1+r} \cap \mathbb{F}_2 V ,$$

$r$ being the depth of x($h$). If x($h$) is in $\mathcal{P}^2$ then $zx(h) = 0$. Whenever x($h$) is as in (8) we have $zx' = 0$ and

$$(X^{h'} + 1)z = \sum_{g \in V'} X^{g+h'} + z = 2z = 0 ,$$

since by construction $h' \in V'$. So $zx = 0$ which is equivalent to $z \in (x)$. Since the support of $z$ is the subspace $V'$ whose dimension equals $m - i$, the property is proved for all $i$, when $m = i + 2^{i-1}$.

2) We suppose now that $m > i + 2^{i-1}$ and we assume that the property is satisfied up to $m - 1$. In accordance with (6), there are a hyperplane $H$ of $G$, an invertible element x$'$ of $\mathbb{F}_2 H$ and $h \notin H$ such that $x = X^h + x'$. As $x' = 1 + x''$ with $x'' \in \mathcal{P}$ (see (2)), $x = (1 + X^h) + x''$. We can choose $h$ such that x$''$ has depth 1. Indeed (x) contains the half of elements of $\mathcal{P}^{m-1}$, because $x\mathcal{P}^{m-1} = \{0, \sum_{g \in G} X^g\}$. So there exists a hyperplane $H'$, different from $H$, which is the support of a codeword $z \notin (x)$. Getting $h$ in $H'$ (and not in $H$) we obtain $zx = zx'' \neq 0$ which yields $x'' \in \mathcal{P} \backslash \mathcal{P}^2$. So we have:

$$x = (X^h + 1) + x'' \quad \text{where} \quad x'' \in P \backslash P^2 \text{ and } supp(x'') \subset H .$$

Since x$'' \in \mathbb{F}_2 H$, where $H$ is identified with the additive group of $\mathbb{F}_2^{m-1}$, there exists (by induction on $m$) an element y$''$ in (x$''$) whose support is a subspace of $H$ of dimension $(m - 1) - i$. Then we have y$''$x$'' = 0$ which yields that the codeword y$''$x of (x) equals y$''(X^h + 1)$. Since $h \notin H$, the support of y$''$x is a subspace of $G$ of dimension $m - i$. That completes the proof of the first part of the theorem.

Actually we have stated an upper bound for the minimum distance $d$ of (x). Indeed we have proved that (x) contains a codeword of weight $2^{m-i}$, for any $i$ such that $i + 2^{i-1} \leq m$. Hence $d \leq 2^{m-i^*}$, where $i^*$ is the biggest $i$.
□

**Corollary 2** *Set $N = 2^m$, $m > 1$. Let $d_m$ be the minimal distance of any $H$-code of length $N$. Then the quotient $d_m/N$ approaches zero as $m$ approaches infinity. The class of $H$-codes does not meet the Gilbert-Varshamov bound : $H$-codes are asymptotically bad.*

*Proof:* In accordance with Theorem 3, $d_m \leq 2^{m-i^*}$, where $i^*$ is the biggest $i$ such that $i + 2^{i-1} \leq m$. Then $d_m/N \leq 2^{-i^*}$. By definition $i^*$ approaches infinity as $m$ approaches infinity. Then we have clearly:

$$\lim \frac{d_m}{N} = 0 \ , \quad \text{as} \quad m \to \infty \ .$$

So we have proved that the class of $H$-codes does not meet the Gilbert-Varshamov bound (cf. [17, p.557]). A $H$-code is an $[N, N/2, d_m]$-code; then the rate $k/N$, where $k$ is the dimension of the code, equals $1/2$. Let $\{ C_m \mid m > 1 \}$ be any infinite sequence of $H$-codes. Actually we have proved that such a sequence cannot satisfy

$$1 - K(\frac{d_m}{N}) \leq \frac{1}{2} \quad \text{where} \quad K(s) = -s \log_2(s) - (1 - s) \log_2(s - 1) \ , \tag{9}$$

for all $m$. Indeed $K(2^{-3}) = 0.54$ and $K(2^{-4}) = 0.33$. According with Table 1, that means that (9) is not satisfied for $m \geq 12$.
□

The last corollary of Theorem 3 will give the characterization of extremal $H$-codes. For its proof, we must treat separately length 64.

**Lemma 3** *Any $H$-code of length 64 contains a codeword whose support is a 3-dimensional subspace. Hence its minimal distance is less than or equal to 8.*

*Proof:* Let (x) be an $H$-code of length 64 - i.e. $G$ is the additive group of $\mathbb{F}_{64}$. Let $z \in$ (x) such that the support of $z$ is an hyperplane $V$ of $G$ ; there exists such $z$ from Theorem 3. Since $zx = 0$ , we can write x as follows (see Lemma 2):

$$x = x' + x''X^g \ , \quad g \notin V \ , \quad x' \text{ and } x'' \text{ in } \mathbb{F}_2 V \cap \mathcal{P} \ .$$

According to (4) we have:

$$x' = (X^u + 1) + y' \quad \text{and} \quad x'' = (X^v + 1) + y'' \ ,$$

with $u \in V$, $v \in V$, $y' \in \mathcal{P}^2$, $y'' \in \mathcal{P}^2$. If x' (resp. x'') is in $\mathcal{P}^2$, then $u$ (resp. $v$) is zero. Since x has depth 1, $u$ and $v$ cannot be zero together. Set

$$a' = (X^u + 1)(X^v + 1) \ x' \quad \text{and} \quad a'' = (X^u + 1)(X^v + 1) \ x'' \ .$$

If $u = 0$ or $u = v$ we take another $u$ in $V$ and replace it in the expression of a' and a''. So it is clear that a' and a'' are in $\mathbb{F}_2 V \cap \mathcal{P}^4$. Since $V$ is here the additive group of $\mathbb{F}_{32}$, a' and a'' are element of the Reed-Muller code of order 1 and length 32; the support of such element (when it is a non zero element) is an affine subspace of $V$ of dimension 4 or 5. In all cases there exists $w \neq 0$ such that the codeword

$$a = (X^u + 1)(X^v + 1)(X^w + 1)$$

has weight 8 and satisfies $aa' = 0$ and $aa'' = 0$. That yields $ax = 0$, which means $a \in$ (x), completing the proof.
□

**Corollary 3** *Let* (x) *be an extremal H-code.*

**(i)** *If* (x) *is an even self-dual code then it is a* [4, 2, 2] *code.*

**(ii)** *If* (x) *is a doubly-even self-dual code, then it is either an* [8, 4, 4] *code, a* [16, 8, 4] *code or a* [32, 16, 8] *code.*

*Proof:* **(i)** Assume that (x) is an extremal even self-dual code. In accordance with Theorem 2, its minimal distance $d$ equals $2^{m-2} + 2$. But, from Theorem 3, we know that $d \leq 2^{m-2}$ as soon as $4 \leq m$. When $m = 3$, (x) is a [8, 4, 4] code, which is clearly doubly-even. Indeed its generator matrix is of the form

$$\left[ \begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{array} \right]$$

(see in Section 2.2). So there is only one possibility : $m = 2$ and (x) is a [4, 2, 2] code.

**(ii)** We now assume that (x) is an extremal doubly-even self-dual code. Then , from Theorem 2, its minimal distance $d$ equals $4[\frac{2^{m-3}}{3}] + 4$. From Theorem 3, $d \leq 2^{m-3}$ as soon as $7 \leq m$. So (x) is a code of length $2^m$, with $m \leq 6$. We have seen that it is very easy to construct a doubly-even self-dual [8, 4, 4] code. It is also easy to construct a doubly-even self-dual [16, 8, 4] code. Indeed whenever the weight of x is 4, we are sure that (x) is doubly-even; therefore (x) has minimal distance 4. If $m = 6$ then $d = 12$; but, in this case, we know from Lemma 3 that $d$ is less than or equal to 8. There is no extremal [64, 32, 12] *H*-code. In the following section we will show how to construct a [32, 16, 8] *H*-code.
□

# 4 On generators of extremal *H*-codes of length 32

We first recall the definition of *difference sets* in elementary abelian groups and the theorem of H.B. MANN. An overall review on difference sets can be found in [6] and [16].

**Definition 2** *Let* {$G$, +} *be a finite abelian group and let $D$ be a subset of $G$. Then $D$ is a difference set of $G$ with parameter $\lambda$ if and only if it satisfies:*

$$\text{card } ( D \cap (h + D) ) = \lambda \quad \text{for all } h \text{ in } G \backslash \{0\} .$$

**Theorem 4** [16] *Let* {$G$, +} *be an abelian group of order $2^k$ and let $D$ be a difference set of $G$ with parameter $\lambda$. For any subgroup $V$ of $G$, we denote by $\overline{V}$ the set $G \backslash V$. If $D$ is equal to* {0} $\cup \overline{V}$ *, for any $V$, we will say that $D$ is a trivial difference set. If $D$ is not trivial, then the parameters of $D$ are:*

$$k = 2t , \quad \text{card } D = 2^{t-1}(2^t + \epsilon) \quad \text{and} \quad \lambda = 2^{t-1}(2^{t-1} + \epsilon) ,$$

*where* $\epsilon = \pm 1$.

From now on $G$ is the additive group of the finite field $\mathbb{F}_{32}$.

**Lemma 4** *Let* (x) *be an $H$-code of length* 32, *where* $x = 1 + X^h x'$ , $h \notin H$, $x'$ *invertible in* $\mathbb{F}_2 H$. *Then* (x) *is a* $[32, 16, 8]$ *code if and only if:*

**(i)** *The weight of* $x'$ *is* 7 *or* 11.

**(ii)** *For all* $z = 1 + X^g$, $g \in H \backslash \{0\}$, *the weight of the product* $zx'$ *is greater than* 2.

*Proof:* Let $[I|M]$ be the generator matrix of (x), where $I$ is the identity matrix and $M = \{ X^u x' \mid u \in H \}$ (see Section 2). Let $y$ in $\mathbb{F}_2 H$; then the product of the vector $y$ by $M$ is in fact the codeword $yx'$. Any codeword of (x) is of the form $(y, yx')$ and its weight equals $\omega(y) + \omega(yx')$. By construction $yx' \neq 0$ whenever $y \neq 0$ ; moreover the depth of $yx'$ is equal to the depth of $y$. So $yx'$ has depth 1 for any $y$ of weight 2.

If (x) has minimal distance 8 it is clear that **(i)** and **(ii)** are satisfied. Note that **(ii)** is not satisfied when $\omega(x')$ is 15.

Suppose now that **(i)** and **(ii)** are satisfied. Condition **(i)** implies that (x) is doubly-even. Then we must only prove that (x) does not contain a codeword of weight 4. First it is impossible to have $\omega(y) = 3$ and $\omega(yx') = 1$ , since we cannot have $\omega(y) = 1$ and $\omega(yx') = 3$. Condition **(ii)** means that $\omega(y) = 2$ and $\omega(yx') = 2$ cannot appear, completing the proof.

□

**Theorem 5** *We denote by $H$ any hyperplane of $G$. Then an $H$-code of length* 32 *is an extremal doubly-even self-dual code (i.e. a* $[32, 16, 8]$ *code) if and only if it has a generator of the form*

$$x = 1 + X^h(1 + y) \ , \quad h \notin H \ , \quad y \in \mathbb{F}_2 H \ , \quad (10)$$

*where the weight of* $1 + y$ *is* 7 *or* 11 *and the support of* $y$ *is a non trivial difference set of $H$, where $H$ is identified with the additive group of* $\mathbb{F}_{16}$.

*Proof:* 1) Let (x) be an $H$-code such that $x$ is of the form (10). Set $D = supp(y)$ and $z = 1 + X^g$, $g \in H \backslash \{0\}$. In accordance with Definition 2 and Theorem 4, we have

$$\text{card } D = 6 \text{ (resp. 10)} \quad \text{and} \quad \text{card } (D \cap (D + h)) = 2 \text{ (resp. 6)} \ .$$

Hence

$$\omega(zy) = \omega(y + X^g y) = 2\text{card } D - 2\text{card } (D \cap (D + h)) = 8 \ .$$

So, for all $h$, the weight of $z + zy$ is greater than 2. From Lemma 4, (x) is extremal.

2) Let $C$ be an extremal $H$-code. According to (4), there is a generator of $C$ of the form

$$a = (1 + X^h) + a' \ , \quad a' \in \mathcal{P}^2 \ .$$

where clearly $h \notin H$; then $a = (1 + X^h)a_1 + a_2$ , where $a_1$ is invertible in $\mathbb{F}_2 H$ and $a_2 \in \mathcal{P}^2 \cap \mathbb{F}_2 H$. Now we obtain another generator of $C$:

$$x = X^h a a_1 = X^h((1 + X^h) + a_1 a_2) = 1 + X^h(1 + y) \ , \quad y \in \mathcal{P}^2 \cap \mathbb{F}_2 H \ .$$

Since $C$ is extremal, the weight of $1 + y$ is 7 or 11. Now we want to prove that the support $D$ of $y$ is a difference set.

It is sufficient to prove that for any $z = 1 + X^g$, $g \in H \backslash \{0\}$, $\omega(zy) = 8$. As $zy \in \mathcal{P}^3 \cap \mathbb{F}_2 H$, $\omega(zy) \in \{0, 8, 16\}$ (the three weights of the Reed-Muller code of order 1 and length 16). We know that $\omega(zy) > 2$. Suppose that $\omega(zy) = 16$. The element $y \in \mathcal{P}^2$ can be identified to a boolean function $f$ on $\mathbb{F}_{2^4}$ ($y = \sum_{g \in G} f(g) X^g$) which is quadratic. Remark that $zy$ corresponds to the function $u \rightarrow f(u) + f(u + h)$. If $f$ is a bent function then the weight of $zy$ is always 8 and the weight of $y$ is 6 or 10 (see [17, p. 426-30]). If $f$ is not a bent function, the kernel of its symplectic form is at least of dimension 2. That means that there exists $g' \in H$, $g' \neq g$, such that $\omega((1 + X^{g'})y)$ is either 0 or 16. It is impossible to have 0; moreover

$$(1 + X^g + 1 + X^{g'})y = (X^g + X^{g'})y = 2 \sum_{g \in H} X^g = 0$$

proves that the value 16 is also not available. Thus we have proved that only weight 8 is possible; $f$ is a bent function and $D$ is a difference set.
$\square$

**Remark 3:** The quadratic bent functions are completely characterized. For instance the general form of these functions is known; from [17, p. 429] we obtain the general form of the generators of the extremal $[32, 16, 8]$ $H$-codes. Let $\{e_1, ..., e_5\}$ be a basis of $G$ and let $H$ be the hyperplane generated by the $e_i$, $i \in [1, 4]$. Then a generator of an extremal $H$-code can be written as follows :

$$x = 1 + X^{e_5}(1 + (X^{e_1} + 1)(X^{e_2} + 1) + (X^{e_3} + 1)(X^{e_4} + 1))$$

where $\omega(x) = 8$. An extremal $H$-code with generator of weight 12 is easily obtained. For instance the following x is such generator:

$$x = 1 + X^{e_5}\left(1 + (X^{e_1} + 1)(X^{e_2} + 1) + (X^{e_3} + 1)(X^{e_4} + 1) + X^{e_4}(\prod_{i=1}^{3}(X^{e_i} + 1))\right).$$

# 5 Conclusion

In this paper we studied a special class of ideals of the algebra $\mathbb{F}_2[\{\mathbb{F}_{2^m}, +\}]$. We gave an upper bound on the minimal distance of these codes which allowed us to prove that they are asymptotically bad. We think that our bound can be improved; maybe it would be possible to find an upper bound for any ideal of the algebra which is self-dual. We conjecture that the minimum-weight codewords of the RM-code $[2^m, 2^{m-1}, 2^{(m+1)/2}]$ are important for this problem. For example, we proved in [12] that all affine invariant self-dual codes of length 128 have minimal distance 16; the value 16 is the upper bound on the minimal distance of $H$-codes and the minimal distance of the RM-code (for the length 128). In all cases there is a codeword of weight 16 whose support is a vector-space of dimension 4.

The complete classification of all binary, self-dual, doubly-even $[32, 16]$ codes is due to CONWAY and PLESS [13]; they proved that there are five non-equivalent extremal codes (another proof was given later in [15]). Two of the five codes are well-known extended cyclic

codes; that is the Reed-Muller code and the quadratic residue code. There are three other extremal codes of length 32, namely the *code F*, the *code G* and the *code U*. We proved that the generator of any extremal [32, 16] *H*-code is completely defined by a quadratic bent function on $\mathbb{F}_{16}$. These functions correspond to the codewords of weight 6 or 10 of the RM-code $R(2, 4)$. All codewords of weight 6 (resp. 10) are equivalent. So there are at most two non-equivalent *H*-codes; from recent explorations it seems that all *H*-codes are equivalent to the code *G*. A full explanation of these facts in a more general context will be presented in a forthcoming paper.

The complete coset weight distributions of the five extremal [32, 16] codes are given in [7] (see also [3] for the quadratic residue code).

# References

[1] E.F. ASSMUS,JR, *On Berman's characterization of the Reed-Muller codes*, published in the same Volume of JSPI.

[2] E.F. ASSMUS,JR & J.D. KEY, *Codes and finite geometries*, INRIA-Report 2027, September 93.

[3] E.F. ASSMUS & V. PLESS *On the covering radius of extremal self-dual codes*, IEEE Trans. on Info. Theory, vol. IT-29, n. 3, May 1983.

[4] S.D. BERMAN *On the theory of group codes*, KIBERNETICA, Vol. 1, n. 1, p. 31-39, 1967.

[5] P. CAMION, *Etude de codes binaires abéliens modulaires autoduaux de petites longueurs*, Revue du CETHEDEC, NS 79-2 (1979) 3-24.

[6] P. CAMION, *Difference sets in elementary abelian groups*, Les Presses de l'Université de Montréal, 1979.

[7] P. CAMION, B. COURTEAU & A. MONTPETIT, *Coset weight enumerators of the extremal self-dual binary codes of length* 32, EUROCODE'92, CISM courses and Lectures 339, pp. 17-30, Springer-verlag, Wien-New York.

[8] P. CHARPIN *Codes idéaux de certaines algèbres modulaires*, Thèse de 3ième cycle, Université Paris 7, 1982.

[9] P. CHARPIN, *The extended Reed-Solomon codes considered as ideals of a modular algebra*, Annals of Discrete Mathematics, 17 ( 1983 ) 171-176.

[10] P. CHARPIN, *On a class of primitive BCH-codes*, IEEE Trans. on Info. Theory, vol. 36, pp. 222-228, Number 1, 1990.

[11] P. CHARPIN, *Représentation des codes cycliques primitifs dans une algèbre modulaire*, IIe Rencontre de Théorie des Représentations, Université de Sherbrooke, Rapport 82, 1991, pp 38-61, I. ASSEM et B. COURTEAU eds.

[12] P. CHARPIN & F. LEVY-DIT-VEHEL, *On self-dual affine-invariant codes*, to appear in Journal of Combinatorial Theory (Series A).

[13] J.H. CONWAY & V. PLESS, *On the enumeration of self-dual codes*, Journal of Combinatorial Theory, Ser. A 28 (1980) 26-53.

[14] A. M. GLEASON, *Weight polynomials of self-dual codes and the MacWilliams identities*, in: Actes Congrés International de Mathématiques, 3 1970 (Gauthier-Villars, Paris, 1971) 211-215.

[15] H. KOCH, *On self-dual, doubly even codes of length 32*, Journal of Combinatorial Theory, Series A, vol. 51, 1989, pp 63-76.

[16] H.B. MANN, *Difference sets in elementary abelian groups*, Illinois Journal of Mathematics, 9(1965), 212-219.

[17] F.J. MACWILLIAMS & N.J.A. SLOANE, *The theory of Error Correcting Codes*, North-Holland 1986.

[18] G. PASQUIER, *A binary extremal doubly-even self-dual code* $[64, 32, 12]$ *obtained by an extended Reed-Solomon code over* $\mathbf{F}_{16}$, IEEE Trans. on Info. Theory, vol. 37, N. 1, 1981.

[19] J. WOLFMANN *A new construction of the binary Golay code* $[24, 12, 8]$ *using a group algebra over a finite field*, Discrete Math. , 31(1980) p.337-338 .

*RR_2325*