SIAM J. DISCRETE MATH.
Vol. 10, No. 1, pp. 128–145, February 1997

010

ON COSET WEIGHT DISTRIBUTIONS OF THE 3-ERROR-CORRECTING BCH-CODES*

PASCALE CHARPIN† AND VICTOR ZINOVIEV‡

Abstract. We study the coset weight distributions of the 3-error-correcting binary narrow-sense BCH-codes and of their extensions, whose lengths are, respectively, $2^m - 1$ and 2^m, m odd. We prove that all weight distributions are known as soon as those of the cosets of minimum weight 4 of the extended code are known. We point out that properties of the cosets which are orphans yield interesting properties on the other cosets. We describe the classes of cosets which are equivalent under the affine permutations. At the end we produce significant numerical results, proving that the number of distinct weight distributions of cosets increases with the length of the codes.

Key words. BCH-codes, uniformly packed codes, coset, coset weight distribution, orphan, affine permutation

AMS subject classifications. 94B15, 51E30

PII. S089548019529443X

1. Introduction.

This paper was initiated by the papers of Camion, Courteau, Fournier, and Kanetkar [6]; Camion, Courteau, and Montpetit [7]; and Charpin [9], [10]. Charpin showed in [10] that there are eight distinct weight distributions of cosets of 2-error-correcting binary primitive BCH-codes of length $2^m - 1$, m even, and of length 2^m for the extended such codes. For the length $2^m - 1$, m odd, it is well known [3], [20] that there are four such distinct weight distributions. We examine here the coset weight distributions of the 3-error-correcting binary narrow-sense BCH-codes of length $2^m - 1$ with m odd, also extended or not. The results of this paper were announced in [11].

We denote by B the 3-error-correcting BCH-code and by $\widehat{B}$ its extension. For length 32 the coset weight distribution of $\widehat{B}$ was given by Camion, Courteau, and Montpetit [7]; this code is in fact the self-dual Reed–Muller code $[32, 16, 8]$ and there are eight distinct weight distributions for its cosets. Our main result is that *the number of weight distributions of cosets of $\widehat{B}$ (respectively, of B) increases with the value of m*. Of course, we suppose that this property holds also when m is even, although we do not study this case here. At any rate, we prove that the code $\widehat{B}$ gives us an example of an infinite class of codes whose dual distance is constant while the number of distinct lines in the distance matrix increases with the length.

In section 2, we present the fundamental equations which give as solutions the coefficients of the distance matrices of B and $\widehat{B}$. Throughout the equations $(A.i)$ and $(E.i)$, what is easy and what is hard appear clearly, and the next sections are in fact a precise explanation of both aspects.

We begin in section 3 with the easy cases. They are globally the cosets of weight 1, 2, 3, and 5. We don't know all about the cosets of B of weight 3 and 5, but we prove that any unsolved problem about these cosets is an unsolved problem about the cosets of $\widehat{B}$ of weight 4 and 6. We consider these last cases as the hard cases. In

* Received by the editors November 8, 1995; accepted for publication (in revised form) March 15, 1996.

http://www.siam.org/journals/sidma/10-1/29443.html

† Institut National de Recherche en Informatique et en Automatique, Codes, Domaine de Voluceau-Rocquencourt, BP 105-78153, Le Chesnay, France (pascale.charpin@inria.fr).

‡ Institute for Problems of Information Transmission of the Russian Academy of Sciences, Bol'shoi Karetnyi 19, Moscow 101447, Russia.

section 4 we study the action of affine permutations on cosets of $\widehat{B}$. It is natural to do that because it is well known that the code $\widehat{B}$ is invariant under these permutations. We characterize the classes of equivalent cosets by their syndromes, and we give some properties about the cosets of weight 4. The cosets of weight 4 and 6 are studied in section 5. We point out the significant role of the cosets of $\widehat{B}$ which are orphans, taking here the terminology of [5]. In section 6 we summarize our results, showing clearly that our problem is reduced to the study of the weight distributions of cosets of $\widehat{B}$ of weight 4. By using the classification of section 4, we were able to compute the full weight distribution for length 128. That is given by Table 5 in section 7. We found 12 distinct weight distributions for the cosets of $\widehat{B}$. Moreover, we found at least 18 distinct weight distributions for the length 512. At the end we give several conjectures.

The *distance* and the *weight* are the Hamming distance and the Hamming weight. The weight of any code word x is denoted by $wt(x)$, and the distance between any two code words x and y is denoted by $d(x, y)$. Denote by K the Galois field of order 2. Let C be any binary code of length n. Recall that the *covering radius* of C, generally denoted by ρ, is the following distance:

$$\rho = \max_{x \in K^n} \min_{c \in C} \{ \; d(x, c) \; \}.$$

Let $D = x + C$ be a coset of C. *The weight of the coset* D is the minimum weight of the code words of D. *A leader* of D is a code word of D of minimum weight.

2. The fundamental equations. Let C be any code of length n over K and let ρ be its covering radius. We will say that such a code is *uniformly packed*, in the sense of [3], if there exist rational numbers $\alpha_0, \ldots, \alpha_\rho$ such that for any $v \in K^n$

$$\sum_{k=0}^{\rho} \alpha_k \; f_k(v) \; = \; 1, \tag{1}$$

where $f_k(v)$ is the number of code words at distance k from v. Let B denote here the 3-error-correcting primitive binary BCH-code of length $n = 2^m - 1$, where m is odd, and let $B^\perp$ denote as usual the dual code of B. The minimal distance of B is $d = 7$. It was shown by Kasami [17] that the *external distance* of B, i.e., the number of nonzero weights in $B^\perp$, is $s = 5$ (see also [19], p. 669). According to the well-known result due to Delsarte [12], we have the following inequality for the covering radius of B:$\rho \le 5$. But on the other hand, we know from the result of Gorenstein, Peterson, and Zierler [14] that for these codes $\rho \ge 5$. Hence we have $\rho = 5$ for the code B. Note that this result was obtained by Helleseth [15], who proved even more: all binary 3-error-correcting BCH-codes have covering radius 5 (essential steps in this result also belong to Assmus and Mattson [1] and van der Horst and Berger [16]). Now we use the following result from the paper of Bassalygo and Zinoviev [4, Theorem 1]: *the code* C *is a uniformly packed code* (*in the sense of* [3]) *if and only if the covering radius* ρ *of* C *is equal to the external distance* s: $\rho = s$. Therefore B is a uniformly packed code in the sense of [3]. Note that Goethals and Van Tilborg [13] have previously showed that the code B is a *uniformly packed code of order* $j = 2$ (see [13, 21]). From this last paper we have the following parameters α_i for the code B:

$$\begin{aligned} &\alpha_0 = \alpha_1 = 1, \\ &\alpha_2 = \alpha_3 = -120/(n-1)(n-7), \\ &\alpha_4 = \alpha_5 = 120/(n-1)(n-7). \end{aligned} \tag{2}$$

Now let $\widehat{B}$ be the 3-error-correcting primitive binary extended BCH-code of length $N = 2^m$, where m is odd; $\widehat{B}$ is obtained from B by overall parity check. Assume that the position we add to the code words of B is always the first position of $\widehat{B}$. The minimal distance of $\widehat{B}$ is $d = 8$, of course. Now we can use the following result [4, Theorem 2]: *an extension of a binary uniformly packed code with parameters α_i, $i \in [0, \rho]$, is a uniformly packed code if and only if the parameters α_i satisfy*

$$\alpha_{\rho-2i} \;=\; \alpha_{\rho-2i-1},\;\; i = 0, 1, \ldots, [(\rho-1)/2],$$

where $[a]$ denotes the integer part of a. Applying this to the code B, the condition above becomes $\alpha_5 = \alpha_4$, $\alpha_3 = \alpha_2$, and $\alpha_1 = \alpha_0$. So we deduce from (2) that the code $\widehat{B}$ is uniformly packed with covering radius 6. Note that the external distance of the code $\widehat{B}$ (respectively, of B) is equal to its covering radius. Then, by applying the general result of Assmus and Pless, *the weight distribution of cosets of weight* 5 *in B is uniquely determined, as are the weight distributions of cosets of weight* 5 *and* 6 *in* $\widehat{B}$ [2, Corollary 1–2].

From now on, the notation for the parameters of codes B and $\widehat{B}$ will be as follows: we will use the same symbols for both codes, but for $\widehat{B}$ all the corresponding symbols will have a hat. The parameters $\widehat{\alpha}_i$ of the code $\widehat{B}$ are connected with the parameters α_i. This connection is given by [4, Theorem 2]. That is,

$$\widehat{\alpha}_{\rho-2i} \;=\; \alpha_{\rho-2i}, \quad i = 0, 1, \ldots, [\rho/2]$$

and for $i = 0, 1, \ldots, [(\rho+1)/2]$,

$$\widehat{\alpha}_{\rho-2i+1} \;=\; ((\rho+1-2i)\alpha_{\rho-2i} \;+\; (n-\rho+2i)\alpha_{\rho-2i+2}\,)/(n+1),$$

where by convention $\alpha_{-1} = \alpha_{\rho+1} = \alpha_{\rho+2} = 0$. We have

$$\begin{array}{ll} \widehat{\alpha}_0 = \widehat{\alpha}_1 = 1, & \widehat{\alpha}_2 = 2(N-68)/N(N-8), \\ \widehat{\alpha}_3 = -120/(N-2)(N-8), & \widehat{\alpha}_4 = 120/N(N-2), \\ \widehat{\alpha}_5 = -\widehat{\alpha}_3, & \widehat{\alpha}_6 = 720/N(N-2)(N-8). \end{array} \tag{3}$$

Recall that $N = 2^m$ denotes here the length of the code $\widehat{B}$.

Let D be any coset of B. Recall that the *weight of* D is the minimum weight of the code words of D. Since the covering radius of B is 5, the weight i of B is in the range $[0, 5]$. We will denote by $\mu_{i,j}$ the number of code words of weight j in such a coset of weight i:

$$\mu_{i,j} = \texttt{card}\ \{\ x \in D \mid wt(x) = j\ \}.$$

Similarly, we will denote by $\widehat{\mu}_{i,j}$ the number of code words of weight j in a coset of $\widehat{B}$ of weight i, $i \in [0, 6]$.

For a coset D with weight distribution

$$\mu_{i,i},\ \mu_{i,i+1}, \ldots,\ \mu_{i,n}$$

we denote by $A_i(x)$ the weight polynomial of D:

$$A_i(x) \;=\; \sum_{k=i}^{n} \mu_{i,k}\ x^k. \tag{4}$$

To write out a general expression for the polynomial $A_i(x)$ we need some results from [3], which we give, for simplicity, only for the binary case. First denote by $P_u(n,\xi)$ the Krawtchouk polynomial of degree u:

$$P_u(n,\xi) = \sum_{j=0}^{u} (-1)^{u-j} \binom{n-\xi}{j} \binom{\xi}{u-j},$$

where

$$\binom{a}{b} = \frac{a(a-1)\dots(a-b+1)}{b!}$$

for any real a. Lloyd's type theorem for the uniformly packed codes asserts (Theorem 1 in [3]) that the existence of a uniformly packed code C of length n with the parameters $\alpha_i, i = 0,1,\dots,\rho$, implies that the Lloyd polynomial $L_\rho(n,\xi)$,

$$L_\rho(n,\xi) = \sum_{i=0}^{\rho} \alpha_i \; P_i(n,\xi),$$

has ρ distinct integer roots between 0 and n. Denote by ξ_i the ith root of $L_\rho(n,\xi)$, where $i = 0,1,\dots,\rho$. Now suppose that D is an arbitrary coset of C of weight i with the weight polynomial $A(x)$ of type (4). We want to know the weight distribution of D (or, in other words, to know the coefficients of $A_i(x)$).

Theorem 2 in [3] gives us the following result: *the weight polynomial $A_i(x)$ of a coset (of weight i) of a uniformly packed code C, with the roots ξ_j of the Lloyd polynomial $L_\rho(n,\xi)$, might be written in the following general form:*

$$A_i(x) = \frac{|C|(1+x)^n}{2^n} + \sum_{j=1}^{\rho} c_{i,j}(1+x)^{n-\xi_j}(1-x)^{\xi_j},$$

where $|C|$ is the cardinality of the code C and $c_{i,j}$ are constants depending on the initial known coefficients of $A_i(x)$ and therefore determined by solving the corresponding system of linear equations. So to know the weight polynomial $A_i(x)$ of C we must know any ρ numbers $\mu_{i,j}$ for $j \in [0,n]$ enough to find the unknown values $c_{i,j}$ from the corresponding equations.

Now we return to our BCH-codes B and $\widehat{B}$. The determination of the coset weight distribution of B is reduced to the resolution of the following equations, considered separately. In other words, if we consider the weight distribution of the coset of weight i, then we use the equation $(A.i)$:

$$\begin{array}{ll}
(A.1) & \alpha_1\,\mu_{1,1} = 1, \\
(A.2) & \alpha_2\,\mu_{2,2} + \alpha_5\,\mu_{2,5} = 1, \\
(A.3) & \alpha_3\,\mu_{3,3} + \alpha_4\,\mu_{3,4} + \alpha_5\,\mu_{3,5} = 1, \\
(A.4) & \alpha_4\,\mu_{4,4} + \alpha_5\,\mu_{4,5} = 1, \\
(A.5) & \alpha_5\,\mu_{5,5} = 1,
\end{array}$$

where the numbers α_i are given above by (2). These equations are obtained from (1) for each weight $i \in [1,5]$ for the case when the vector v is a zero vector. Each equation

$(A.i)$ corresponds to the weight distributions of cosets of minimum weight i, implying $\mu_{i,j} = 0$ for $j < i$. Moreover, since the minimum weight of B is 7, the sum of two weights in a given coset cannot be less than 7.

Now consider the corresponding equations for the code $\widehat{B}$. By the definition of the extension, a coset of $\widehat{B}$ has either only even weights or only odd weights. Therefore, in the same manner as we obtained the equations $(A.i)$, we obtain from (1) the equations $(E.i)$ corresponding to the weights $i \in [1,6]$ of the cosets of $\widehat{B}$:

$$\begin{array}{ll}
(E.1) & \widehat{\alpha}_1\, \widehat{\mu}_{1,1} \;=\; 1, \\
(E.2) & \widehat{\alpha}_2\, \widehat{\mu}_{2,2} \;+\; \widehat{\alpha}_6\, \widehat{\mu}_{2,6} \;=\; 1, \\
(E.3) & \widehat{\alpha}_3\, \widehat{\mu}_{3,3} \;+\; \widehat{\alpha}_5\, \widehat{\mu}_{3,5} \;=\; 1, \\
(E.4) & \widehat{\alpha}_4\, \widehat{\mu}_{4,4} \;+\; \widehat{\alpha}_6\, \widehat{\mu}_{4,6} \;=\; 1, \\
(E.5) & \widehat{\alpha}_5\, \widehat{\mu}_{5,5} \;=\; 1, \\
(E.6) & \widehat{\alpha}_6\, \widehat{\mu}_{6,6} \;=\; 1.
\end{array}$$

From the results of Kasami [17] and Bassalygo and Zinoviev [4] we have all the roots $\widehat{\xi}_i$ of the Lloyd polynomial $\widehat{L}_6(N,\xi)$ for the code $\widehat{B}$ (these roots are exactly the values of nonzero weights in the dual code $\widehat{B}^{\perp}$):

$$\begin{array}{ll}
\widehat{\xi}_1 \;=\; N/2 \;-\; \sqrt{2N}, & \widehat{\xi}_2 \;=\; N/2 \;-\; \sqrt{N/2}, \\
\widehat{\xi}_3 \;=\; N/2, & \widehat{\xi}_4 \;=\; N/2 \;+\; \sqrt{N/2}, \\
\widehat{\xi}_5 \;=\; N/2 \;+\; \sqrt{2N}, & \widehat{\xi}_6 \;=\; N.
\end{array}$$

Note that the five roots of the Lloyd polynomial $L_5(n,\xi)$ for the code B are the first five roots $\widehat{\xi}_i, i \in [1,5]$, of $\widehat{L}_6(N,\xi)$. This is so because the all-one vector, which corresponds to the root $\widehat{\xi}_6$, cannot belong to the code $B^{\perp}$.

Now we give some definitions and notation which we will use in the next sections.

Let $v \in K^n$, $v = (v_1, \ldots,\ v_n)$. The *support* of v is

$$\mathrm{supp}(v) = \{\ \ell \mid v_\ell \neq 0\ \}.$$

Note that the Hamming weight $wt(v)$ of v is equal to the cardinality of the support of v.

We will use here the terminology of [5], where special cosets, so-called *orphans*, are introduced.

DEFINITION 2.1. *Let C be an arbitrary linear code C of length n and let D be a coset of C of weight i. Let D' be the coset*

$$D' = D \;+\; v^{(j)},$$

where $v^{(j)}$ denotes a binary vector with exactly one nonzero position at the jth coordinate.

If the weight of D' is $i-1$, then D' is said to be a child of D.

If the weight of D' is $i+1$, then D' is said to be a parent of D.

The coset D is said to be an orphan if and only if it has no parent. In other words, an orphan of C is a coset D with the following property:

$$\bigcup_{v \text{ is a leader of } D} \mathrm{supp}(v) = \{\ 1, \ldots, n\ \}.$$

Notation. From now on let us denote by $\mathcal{D}$ (respectively, by $\widehat{\mathcal{D}}$) the full set of the cosets of B (respectively, of $\widehat{B}$). We will denote by $\mathcal{D}_i$ (respectively, by $\widehat{\mathcal{D}}_i$) the subset of $\mathcal{D}$ (respectively, of $\widehat{\mathcal{D}}$) which consists of all the cosets of weight i.

The number of cosets of B will be denoted by Γ and the number of such cosets of minimum weight i will be denoted by $\Gamma(i)$. Similarly, for the extended code $\widehat{B}$, a notation is as follows:

$$\widehat{\Gamma} \;=\; |\widehat{\mathcal{D}}| \quad \text{and} \quad \widehat{\Gamma}(i) \;=\; |\widehat{\mathcal{D}}_i|.$$

3. Cosets weight distribution: The easy cases. Since the dimension of both codes B and $\widehat{B}$ is $2^m - 3m - 1$, $m \geq 5$, we obviously obtain

$$\Gamma = 2^{3m} \quad \text{and} \quad \widehat{\Gamma} = 2^{3m+1}.$$

The weight distribution of B is known, due to Kasami, who in [17] gave the weight distribution of the dual of B. In fact, we use here the table given in [19, p. 669]; it is the weight distribution of $B^{\perp}$. Since we also need the weight distribution of $\widehat{B}$, we give the weight distribution of the dual code in Table 1.

TABLE 1
The weight distribution of the dual of the binary 3-error-correcting extended BCH-code of length 2^m, m odd.

Weights	Number of code words
0	1
$2^{m-1} \pm 2^{(m+1)/2}$	$2^{m-3}(2^m-1)(2^{m-1}-1)/3$
$2^{m-1} \pm 2^{(m-1)/2}$	$2^{m-1}(2^m-1)(5.2^{m-1}+4)/3$
2^{m-1}	$(2^m-1)(5.2^{2m-1}+7.2^{m-2}(2^{m-1}-1)+2^{m+2}+6)/3$
2^m	1

Remark. Recall that a *tactical configuration* $T(n, w, \ell, \beta)$ is a set of binary vectors of length n and weight w such that any ℓ, $1 \leq \ell \leq w$, positions are simultaneously occupied by ones in precisely β vectors of $T(n, w, \ell, \beta)$. If $\beta = 1$, a configuration $T(n, w, \ell, 1)$ is called a *Steiner system* and is denoted by $S(n, w, \ell)$.

Let B_7 be the set of code words of weight 7 in B and $\widehat{B}_8$ be the set of code words of weight 8 in $\widehat{B}$. Using equation (1) for arbitrary vectors v of weights 2 and 3 we have immediately the following: *the set $\widehat{B}_8$ is a tactical configuration $T(N, 8, 3, \beta)$ and the set B_7 is a tactical configuration $T(n, 7, 2, \beta)$, where*

$$\beta \;=\; \frac{1-\widehat{\alpha}_3}{\widehat{\alpha}_5} \;=\; \frac{(N-2)(N-8)}{120} \;+\; 1. \tag{5}$$

This result can be also deduced from Theorem 3 in [4].

3.1. Cosets of minimum weights 1, 2, and 3. Since the minimum distance of codes B and $\widehat{B}$ are, respectively, 7 and 8, any coset of weight i, $1 \leq i \leq 3$, has only one code word of weight i. So the number of such cosets of weight i is exactly the number of code words of weight i in the ambient space. That is, for cosets of B and $\widehat{B}$

$$\Gamma(1) = n, \quad \Gamma(2) = n(n-1)/2, \quad \text{and} \quad \Gamma(3) = n(n-1)(n-2)/6, \tag{6}$$

$$\widehat{\Gamma}(1) = N, \quad \widehat{\Gamma}(2) = N(N-1)/2, \quad \text{and} \quad \widehat{\Gamma}(3) = N(N-1)(N-2)/6. \tag{7}$$

The condition $\widehat{\mu}_{i,i} = 1$ for $i \in [1, 3]$ immediately gives us the solution of the corresponding equations $(E.i)$. We then obtain the values of $\widehat{\mu}_{2,6}$ and $\widehat{\mu}_{3,5}$. Similarly, the condition $\mu_{i,i} = 1$ for $i \in [1, 2]$ immediately gives us the solution of the corresponding equations $(A.i)$. We can then obtain the value of $\mu_{2,5}$. Note that $\mu_{2,5}$ and $\widehat{\mu}_{3,5}$ are also given by the remark above. These results can be summarized as follows.

PROPOSITION 3.1. *There is only one coset weight distribution for the cosets of B of weight 1 and 2. The number of code words of weight 5 in the coset of weight 2 is $\mu_{2,5} = \beta$ (see (5)).*

There is only one coset weight distribution for the cosets of $\widehat{B}$ of weight 1, 2, and 3. The number of code words of weight 6 in the coset of weight 2 is

$$\widehat{\mu}_{2,6} = \frac{1 - \widehat{\alpha}_2}{\widehat{\alpha}_6} = \frac{(N-2)(N^2 - 10N + 136)}{720}.$$

The number of code words of weight 5 in the coset of weight 3 is $\widehat{\mu}_{3,5} = \beta$ (see (5)).

Finally, we cannot describe the set $\mathcal{D}_3$ of cosets of B of weight 3; we only know its cardinality. Moreover, according to (2), by using $(A.2)$ and $(A.3)$ we can state the following relation:

$$\mu_{3,4} + \mu_{3,5} = \mu_{2,5}, \tag{8}$$

where $\mu_{2,5}$ is known to be equal to β. Note also that $\mu_{2,5} = \widehat{\mu}_{3,5}$. Hence we can conclude that *to describe $\mathcal{D}_3$ is equivalent to describing $\widehat{\mathcal{D}}_4$*. Indeed, a coset of $\mathcal{D}_3$ can be seen as a shortened coset of $\widehat{\mathcal{D}}_4$, with

$$\mu_{3,4} = \widehat{\mu}_{4,4} - 1.$$

Such a coset of $\widehat{\mathcal{D}}_4$ must have a leader which has zero in its first position (this position is the parity check position of $\widehat{B}$). We will explain in section 4 that any coset of $\widehat{\mathcal{D}}_4$ is equivalent to such a coset.

3.2. Cosets of minimum weight 5. All cosets of $\mathcal{D}_5$ have the same weight distribution—it is immediate from $(A.5)$(see also [1]). However, we are not able to give the cardinality of $\mathcal{D}_5$; we only can say that it is equal to the cardinality of $\widehat{\mathcal{D}}_6$.

PROPOSITION 3.2. *There is only one weight distribution for the cosets of $\mathcal{D}_5$. Any coset of $\mathcal{D}_5$ is an orphan, and it contains*

$$\mu_{5,5} = \frac{1}{\alpha_5} = \frac{(n-1)(n-7)}{120}$$

code words of weight 5. Moreover, the cardinality of $\mathcal{D}_5$ is equal to the number of cosets of $\widehat{B}$ of weight 6:

$$\Gamma(5) = \widehat{\Gamma}(6).$$

Proof. The value $\mu_{5,5}$ follows from $(A.5)$. From Definition 2.1, we know that an orphan is a coset without parent. Since the covering radius of B is 5, it is clear that any coset $G \in \mathcal{D}_5$ is an orphan. Now for any coset $H \in \widehat{\mathcal{D}}_6$, we obtain a coset $G \in \mathcal{D}_5$ by deleting one position of H. We always delete the first position, which corresponds to the overall parity checking position of $\widehat{B}$. Two such cosets G and G' are distinct, as soon as we got two distinct cosets H and H'. Actually, this correspondence is one-to-one: by the definition of the extension, two distinct cosets of $\mathcal{D}_5$ cannot give the same extension. So $\Gamma(5) = \widehat{\Gamma}(6)$. $\square$

Now for $\widehat{\mathcal{D}}_5$, equations $(E.i)$ involve a full description. Moreover, we will end this section by explaining some links between $\widehat{\mathcal{D}}_5$ and $\widehat{\mathcal{D}}_4$.

PROPOSITION 3.3. *There are*

$$\widehat{\Gamma}(5) = N(N-1)(5N+8)/6$$

distinct cosets of $\widehat{B}$ *of weight* 5. *All of these cosets have the same weight distribution and each of them contains*

$$\widehat{\mu}_{5,5} \;=\; (N-2)(N-8)/120 \tag{9}$$

vectors of weight 5. *Note that* $\widehat{\mu}_{5,5} = \mu_{5,5}$.

Proof. All cosets of minimum weight 3 have the same weight polynomial. We know from $(E.3)$ that the number of the code words of weight 5 in the coset of minimum weight 3 is

$$\widehat{\mu}_{3,5} = \beta,$$

where β is defined in (5). From the equation $(E.5)$ we have $\widehat{\mu}_{5,5} \;=\; 1/\widehat{\alpha}_5$. Taking into account the value of $\widehat{\alpha}_5$ in (3) we obtain (9). Now the total number of binary vectors of length N and weight 5 is

$$T \;=\; \binom{N}{5},$$

and we have

$$T = \widehat{\Gamma}(5)\;\widehat{\mu}_{5,5} \;+\; \widehat{\Gamma}(3)\;\widehat{\mu}_{3,5}.$$

Then we can compute $\widehat{\Gamma}(5)$ using the value of $\widehat{\Gamma}(3)$ given by the equation (7). □

PROPOSITION 3.4. *Let* $G \;\in\; \widehat{\mathcal{D}}_5$, *let* F *be a child of* G, *that is,*

$$F \;=\; G \;+\; v^{(j)}, \quad F \in \widehat{\mathcal{D}}_4$$

for some $j \;\in\; \{\; 1,\ldots,\; N\;\}$, *and let* $k_j(G)$ *denote the weight of the* j*th column of the binary matrix formed by the leaders of* G. *Then the weight distribution of* F *is defined by* $\widehat{\mu}_{4,4} \;=\; k_j(G)$, *where* $k_j(G) \;<\; N/4$.

Proof. Consider the jth column of the matrix formed by all the leaders of G. So we have $k_j(G)$ vectors $u_s,\ s = 1,\ldots,k_j(G)$, which have "1" at jth position. Then the coset F has weight 4 and the $k_j(G)$ vectors

$$u_s \;+\; v^{(j)},\; s \;=\; 1,\ldots,k_j(G)$$

are the only vectors in F that have weight 4. Hence, such a coset F is not an orphan since it has some parent. That gives the inequality at the statement, completing the proof. □

Note that any $F \in \widehat{\mathcal{D}}_4$, which is not an orphan, is a child of some coset of $\widehat{\mathcal{D}}_5$. In this section we have proved that each unsolved problem on cosets of B can be seen as an unsolved problem on cosets of $\widehat{B}$. We will see in section 5 that the general problem we treat here is reduced to the determination of the weight distribution of cosets of $\widehat{\mathcal{D}}_4$, more precisely to the determination of the possible values of $\widehat{\mu}_{4,4}$. The proposition above suggests an equivalent point of view: we know all about the weight distribution of cosets of $\widehat{\mathcal{D}}_5$, but we do not know, for such a coset, how much leaders have for one given position in its support.

4. Equivalent cosets. At the end of this paper we will give numerical results on the coset weight distributions of the code $\widehat{B}$ for $m = 7$ and $m = 9$. We obtain these results with the aid of a computer; however, the computation was possible because of some properties on the equivalent cosets. In this section we want to present these properties and their corollaries.

Let K and $\mathbf{G}$ be, respectively, the fields of order 2 and of order N. Since we treat primitive binary codes, we can consider extended codes as K-subspaces in the group algebra of the additive group of $\mathbf{G}$. This representation is more convenient when we want to describe the permutations on cosets which conserve the code $\widehat{B}$. So, in this section, the ambient space is the group algebra $\mathcal{A} = K[\{\mathbf{G}, +\}]$ and a code word is a formal sum:

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

Recall that the code $\widehat{B}$ is invariant under the affine permutations on $\mathbf{G}$. That means that any permutation

$$\sigma_{u,v} \ : \sum_{g \in \mathbf{G}} x_g X^g \quad \longmapsto \quad \sum_{g \in \mathbf{G}} x_g X^{ug+v} \ , \quad u \neq 0, \ u \in \mathbf{G}, \ v \in \mathbf{G}$$

is an automorphism of the code $\widehat{B}$ [18]. Therefore, for any coset $D = x + \widehat{B}$, we have obviously $\sigma_{u,v}(D) = \sigma_{u,v}(x) + \widehat{B}$. Let us define, for any integer $s \in [0, N-1]$, the mapping $\phi_s(x)$,

$$\phi_s : A \ \rightarrow \ \mathbf{G}, \ \phi_s(x) \ = \ \sum_{g \in \mathbf{G}} x_g g^s, \tag{10}$$

where by convention $\phi_0(x) = \sum_{g \in \mathbf{G}} x_g$.

DEFINITION 4.1. *The extended* 3*-error-correcting BCH-code* $\widehat{B}$ *is the following subspace of* $\mathcal{A}$*:*

$$\widehat{B} = \{ \ x \mid \phi_s \ (x) = 0, \ s \in \{0\} \cup cl(1) \cup cl(3) \cup cl(5) \ \},$$

where $cl(t)$ *is the cyclotomic coset of* 2 *(mod* n*) containing* t *and* $m \geq 5$*. So the dimension of* $\widehat{B}$ *equals* $N - 3m - 1$*, where* $N = 2^m$ *and* $n = N - 1$*.*

DEFINITION 4.2. *There are* 2^{3m+1} *cosets of* $\widehat{B}$*. Each coset* $x + \widehat{B}$ *is uniquely defined by its so-called syndrome:*

$$S(x) = (\ \phi_0(x), \ \phi_1(x), \ \phi_3(x), \ \phi_5(x) \ ).$$

When $\phi_0(x) = 0$*, all weights of the coset are even and we will say that the coset is even*; *otherwise, all weights of the coset are odd and we will say that the coset is odd.*

We will see that our problem is in fact the determination of the weight distributions of the cosets of $\widehat{B}$ of weight 4. Moreover, the odd cosets can be studied simply from the even cosets. For this reason we now study even equivalent cosets. Recall that we denote by $\widehat{\mathcal{D}}$ the set of all cosets of $\widehat{B}$.

LEMMA 4.3. *Let us define the following subsets of* $\widehat{\mathcal{D}}$*:*

$$\mathcal{B}_1 = \{ \ x + \widehat{B} \mid \phi_0(x) = 0 \ \ and \ \ \phi_1(x) \neq 0 \ \}, \tag{11}$$

$$\mathcal{B}_2 = \{ \ x + \widehat{B} \mid \phi_0(x) = 0 \ \ and \ \ \phi_1(x) = 0 \ \}, \tag{12}$$

$$\mathcal{B}_3 = \{\ x + \widehat{B} \mid \phi_0(x) = \phi_1(x) = \phi_3(x) = 0\ \}. \tag{13}$$

Then $\mathcal{B}_1$ is contained in the Reed–Muller code $R(m-1,m)$ of order $m-1$ and not contained in $R(m-2,m)$; $\mathcal{B}_2$ is contained in $R(m-2,m)$; $\mathcal{B}_3$ is contained in the extended 2-error correcting BCH-code.

Proof. Recall the definition of the Reed–Muller code of length N and order r, denoted by $R(r,m)$. For any $t \in [0,n]$ let us define the 2-weight of t to be $\omega_2(t) = \sum_{i=0}^{m-1} t_i$, where

$$t \ = \ \sum_{i=0}^{m-1} t_i 2^i$$

is the binary expansion of t. Let I_r be the set of integers from $[0,n]$ such that $\omega_2(t) < m-r$. The code $R(r,m)$ is the set of code words x satisfying $\phi_t(x) = 0$ for all $t \in I_r$. We have $I_{m-1} = \{0\}$ and $I_{m-2} = \{0\} \cup cl(1)$. The extended 2-error correcting BCH-code is the set of code words satisfying $\phi_t(x) = 0$ for t in $\{0\} \cup cl(1) \cup cl(3)$. ∎

LEMMA 4.4. *Let u and v be in $\mathbf{G}$, where $u \neq 0$. Consider a coset $x + \widehat{B}$ whose syndrome is $S(x) = (0,\delta,\gamma,\lambda)$. Then the syndrome of the coset $\sigma_{u,v}(x) + \widehat{B}$ is as follows:*

$$S(\sigma_{u,o}(x)) = (0,\ u\delta,\ u^3\gamma,\ u^5\lambda) \tag{14}$$

and

$$S(\sigma_{1,v}(x)) = (0,\ \delta,\ \gamma + \delta v^2 + \delta^2 v,\ \lambda + \delta v^4 + \delta^4 v). \tag{15}$$

Proof. For any code word $x = \sum_{g\in\mathbf{G}} x_g X^g$, we have

$$\phi_t(\sigma_{u,o}(x)) = \sum_{g\in\mathbf{G}} x_g (ug)^t = u^t \phi_t(x).$$

Thereby (14) follows immediately. Now $\phi_t(\sigma_{1,v}(x)) = \phi_t(X^v x)$. So, for $t = 1, 3$ and 5 we obtain

$$\begin{aligned}
\phi_1(X^v x) &= \sum_{g\in\mathbf{G}} x_g (g+v) = \phi_1(x) + v\ wt(x) = \phi_1(x) = \delta,\\
\phi_3(X^v x) &= \sum_{g\in\mathbf{G}} x_g (g+v)^3 = \phi_3(x) + v^2\phi_1(x) + v(\phi_1(x))^2 = \gamma + \delta v^2 + \delta^2 v,\\
\phi_5(X^v x) &= \sum_{g\in\mathbf{G}} x_g (g+v)^5 = \phi_5(x) + v^4\phi_1(x) + v(\phi_1(x))^4 = \lambda + \delta v^4 + \delta^4 v,
\end{aligned}$$

where the sums are computed modulo 2. Then we obtain (15), therefore completing the proof. ∎

Let us define an equivalence relation Δ on the set $\widehat{\mathcal{D}}$ of the cosets of $\widehat{B}$. Let u and v be any elements in $\mathbf{G}$, where $u \neq 0$; for any $D_1 \in \widehat{\mathcal{D}}$ and any $D_2 \in \widehat{\mathcal{D}}$,

$$D_1 \Delta D_2 \quad \Leftrightarrow \quad \exists\ \ u, v, u \neq 0 \ \text{ such that }\ D_1 = \sigma_{u,v}(D_2). \tag{16}$$

From now on, D_1 *is equivalent to* D_2 means that $D_1 \Delta D_2$. For a given D, we are interested in the number of cosets D_1 such that $D \Delta D_1$. Moreover, we want to characterize explicitly the cosets D_1 by its syndromes. We here study even cosets; hence the syndrome of D will always be of the form $(0, \delta, \gamma, \lambda)$, and the weight of such a coset should be 2, 4, or 6.

Since m is odd then 3 (respectively, 5) and $2^m - 1$ are relatively prime. Hence it follows from (14) that there are always $N-1$ distinct cosets $\sigma_{u,0}(D)$, $u \in \mathbf{G}^*$. Suppose that $\delta = 0$, meaning $D \in \mathcal{B}_2$. It follows from (15) that $\sigma_{1,v}(D) = D$ for any v. In this case the coset D is an *orphan*, because each coordinate position is covered by at least one leader of D (see Definition 2.1). The weight of D could be 4 or 6. When it is 4 the supports of two leaders cannot intersect, proving that the number of leaders is $N/4$. Since $\mathcal{B}_2$ is contained in $R(m-2, m)$, the support of any code word of weight 4 is an affine subspace of dimension 2. As there are $(N-1)(N-2)/6$ linear subspaces of dimension 2, there are the same number of cosets of weight 4 in $\mathcal{B}_2$. On the other hand, there are N^2 cosets in $\mathcal{B}_2$, implying that the number of cosets of weight 6 in $\mathcal{B}_2$ is

$$N^2 - \ (N-1)(N-2)/6 - 1 = (N-1)(5N+8)/6.$$

Moreover, by definition, $\mathcal{B}_3$ is composed of $N-1$ cosets of weight 6, if we except $\widehat{B}$ itself.

So we have proved the following.

PROPOSITION 4.5. *Let $D \in \mathcal{B}_2$. Then D is an orphan and*

$$\texttt{card}\ \{\ D_1 \mid D \Delta D_1\ \} = \texttt{card}\ \{\ \sigma_{u,0}(D) \mid u \in \mathbf{G}^*\ \} = N - 1.$$

When the weight of D is 4, D has $N/4$ leaders.

There are $(N-2)/6$ nonequivalent cosets of weight 4 and $(5N+8)/6$ nonequivalent cosets of weight 6 in $\mathcal{B}_2$.

There is only one coset D of weight 6 in $\mathcal{B}_3$ up to equivalence. The cosets of $\mathcal{B}_3$ are $\sigma_{u,0}(D)$, $u = \alpha^k$, whose syndromes are $(0, 0, 0, \alpha^k)$ (α denotes here a primitive element of $\mathbf{G} = GF(2^m)$).

Suppose now that $\delta \neq 0$; i.e., we consider cosets D in $\mathcal{B}_1$. It comes from (15) that D is invariant under a permutation $\sigma_{1,v}$ if and only if

$$\delta v^2 + \delta^2 v = 0 \quad \text{and} \quad \delta v^4 + \delta^4 v = 0.$$

The mapping $v \ \rightarrow \ \ \delta v^2 + \delta^2 v$ is linear; its kernel has dimension 1. Hence it takes exactly 2^{m-1} distinct values. Since m is odd, we obtain the same result for the mapping $v \ \rightarrow \ \delta v^4 + \delta^4 v$. In both cases the kernel is $\{0, \delta\}$; so, by applying $\sigma_{1,v}$, we obtain exactly 2^{m-1} different syndromes. Suppose that the weight of D is 4. Whenever D contains the code words a whose support is $\{\ a_1,\ a_2,\ a_3,\ a_4\ \}$, it contains also the word $X^\delta a$ whose support is $\{\ a_1+\delta,\ a_2+\delta,\ a_3+\delta,\ a_4+\delta\ \}$. These code words do not intersect. Indeed, the equalities $a_1 = a_2 + \delta$ and $a_3 = a_4 + \delta$ would imply $\sum_{i=1}^4 a_i = 0$, meaning that D is contained in $R(m-2, m)$ (i.e., $\delta = 0$). So we have proved the following.

PROPOSITION 4.6. *The set $\mathcal{B}_1$ contains $N^2(N-1)$ elements. For any $D \in \mathcal{B}_1$ we have*

$$\texttt{card}\ \{\ D_1 \mid D \Delta D_1\ \} = N(N-1)/2.$$

So there are $2N$ classes of nonequivalent cosets in $\mathcal{B}_1$.

The permutation $\sigma_{1,v}$ leaves a coset D with the syndrome $(0, \delta, \gamma, \lambda)$ invariant if and only if $v = \delta$. Therefore, when the weight of D is 4, the number of leaders in D is even: whenever D contains a word a, it contains also the word $X^\delta a$, which cannot be equal to a.

There are $N(N-1)/2$ distinct code words of weight 2 and each coset of weight 2 contains only one code word of weight 2. All cosets of weight 2 are in $\mathcal{B}_1$, because the minimum weight of $R(m-2, m)$ is 4. Since the group of the $\sigma_{u,v}$ is doubly transitive, they are equivalent. The syndromes can be calculated from the formulas of Lemma 4.4.

PROPOSITION 4.7. *The cosets of weight 2 are in $\mathcal{B}_1$. The corresponding syndromes are of the form*

$$(\; 0, \; u, \; u^3 + uv^2 + u^2 v, \; u^5 + uv^4 + u^4 v \;), \quad u \in \mathbf{G} \backslash \{0\}, \quad v \in \mathbf{G}.$$

These cosets are the $\sigma_{u,v}(D)$, where D is the coset whose leader is $1 + X$ and whose syndrome is $(0, 1, 1, 1)$.

Note that the coset $\sigma_{u,v}(D)$ is equal to the coset $\sigma_{u,v'}(D)$ if and only if $v' = v$ or $v' = v + u$. This gives us $N(N-1)/2$ different cosets of weight 2.

5. Cosets weight distribution: The hard cases.

5.1. Cosets of minimum weight 4. We begin by giving the results we have on cosets of weight 4 of B, the elements of $\mathcal{D}_4$. Moreover we claim that the weight distributions of cosets of $\mathcal{D}_4$ can be precisely obtained from those of the cosets of $\widehat{\mathcal{D}}_4$.

PROPOSITION 5.1. *Let F be any coset of $\mathcal{D}_4$. The weight distribution of F is uniquely defined by the value $\mu_{4,4}$, where $\mu_{4,4}$ is an even number in the interval*

$$2 \;\leq\; \mu_{4,4} \;\leq\; (n+1)/4 \;-\; 2.$$

Moreover,

$$\mu_{4,4} \;+\; \mu_{4,5} \;=\; \mu_{5,5} \;=\; \frac{(n-1)(n-7)}{120}.$$

The coset F can be seen as a shortened coset of $\widehat{\mathcal{D}}_4$ with parameter $\widehat{\mu}_{4,4} = \mu_{4,4}$.

Proof. From equation $(A.4)$ and the equality $\alpha_4 = \alpha_5$ (see (2)) we have for an arbitrary coset F of weight 4

$$\mu_{4,4} \;+\; \mu_{4,5} = \frac{1}{\alpha_5} \;=\; \frac{(n-1)(n-7)}{120}.$$

Extending F, we clearly obtain a coset of weight 4 of $\widehat{B}$, which has as its set of leaders the set of leaders of F. So $\mu_{4,4}$ is even according to Proposition 4.6. Of course, F cannot be an orphan, since n is an odd number, implying $\mu_{4,4} \;<\; n/4$ and therefore $\mu_{4,4} \;<\; (n+1)/4 \;-\; 1$ (because $(n+1)/4 \;-\; 1$ is also odd). ∎

PROPOSITION 5.2. *Let F be any coset of weight 4 of $\widehat{B}$, i.e., $F \in \widehat{\mathcal{D}}_4$. The weight distribution of F is uniquely defined by the value $\widehat{\mu}_{4,4}$, where $\widehat{\mu}_{4,4}$ is an even number in the interval*

$$2 \;\leq\; \widehat{\mu}_{4,4} \;\leq\; N/4.$$

Proof. Suppose that F is an arbitrary coset of $\widehat{B}$ of weight 4:$F \;\in\; \widehat{\mathcal{D}}_4$. Since every weight of F is even we obtain from formula $(E.4)$ the value $\widehat{\mu}_{4,6}$:

$$\widehat{\mu}_{4,6} \;=\; \frac{1 - \widehat{\alpha}_4 \widehat{\mu}_{4,4}}{\widehat{\alpha}_6}. \tag{17}$$

Therefore, the weight distribution of F is uniquely determined from the value $\widehat{\mu}_{4,4}$. Now note that two leaders of F have disjoint supports, since the minimum weight of B is 8. Hence $\mu_{4,4} \leq N/4$. From Proposition 4.6 we have that the number $\widehat{\mu}_{4,4}$ is always even. ∎

It is clear that any coset $F \in \widehat{\mathcal{D}}_4$ with $\widehat{\mu}_{4,4}$ leaders has $N - 4\widehat{\mu}_{4,4}$ different parents from $\widehat{\mathcal{D}}_5$. As we already know from Proposition 4.5, there are at least $(N-1)(N-2)/6$ cosets in $\widehat{\mathcal{D}}_4$ with weight distribution

$$\widehat{\mu}_{4,4} = N/4 \text{ and } \widehat{\mu}_{4,6} = N(N-8)(N-32)/720. \tag{18}$$

These cosets have no parent; they are orphans. There are N different cosets in $\widehat{\mathcal{D}}_3$ which are generated by any such orphan. They are the N children of the orphan. Can two different orphans R and R' give the same children? If yes, that implies that the distance between these two cosets is 2, i.e., that the set of code words

$$R + R' = \{\ x + x' \mid x \in R,\ x \in R'\ \}$$

has minimum weight 2. So, if the set above has minimum weight 4 there is a contradiction. Particularly, if the orphans R and R' are in the RM-code of order $m-2$, the set of the children of R and the set of the children of R' do not intersect. In this way, we obtain at least $N(N-1)(N-2)/6$ cosets of weight 3. In accordance with (7), we have the following.

Proposition 5.3. *Any coset in $\widehat{\mathcal{D}}_3$ is a child of some orphan of $\widehat{B}$ of weight 4 which is contained in the RM-code of order $m-2$.*

5.2. Cosets of minimum weight 6. At the end, we have to study the cosets of $\widehat{\mathcal{D}}_6$. It is the same situation we had for cosets of $\mathcal{D}_5$. Although we know the weight distribution of such cosets, we cannot give the cardinality of $\widehat{\mathcal{D}}_6$. However, we can give a property analogous to those stated in Proposition 5.3.

Proposition 5.4. *All cosets of $\widehat{B}$ of weight 6 have the same weight distribution. Such a coset is an orphan and it contains*

$$\widehat{\mu}_{6,6} \ = \ N(N-2)(N-8)/720 \tag{19}$$

code words of weight 6.

Proof. It is clear that the equation $(E.6)$ has only one solution (it can be deduced also from [1]). That is $\widehat{\mu}_{6,6} = 1/\widehat{\alpha}_6$. We deduce (19) from the formula (3), which gives the value of $\widehat{\alpha}_6$. Then all cosets in $\widehat{\mathcal{D}}_6$ have the same weight distribution. Such cosets are orphans since the covering radius of $\widehat{B}$ is 6. ∎

Now take $F \in \widehat{\mathcal{D}}_6$ and consider its children. They are cosets $G \in \widehat{\mathcal{D}}_5$ such that

$$G \ = \ F \ + \ v^{(i)}$$

for some $i \in [1, N]$. So if we denote

$$\text{supp}(G) \ = \bigcup_{v \text{ is a leader of } G} \text{supp}(v),$$

then we have for such a child of F

$$\text{supp}(G) \ \subseteq \ \{1, \ldots, N\} \ \setminus \ \{i\}.$$

PROPOSITION 5.5. *Let G be any coset from $\widehat{\mathcal{D}}_5$. Then G is not an orphan, and there is $i \in [1, N]$ and a coset $F \in \mathcal{B}_2$ (i.e., a coset of weight 6, which belongs to Reed–Muller code $R(m-2, m)$) such that G is a child of F with $G = F + v^{(i)}$. Moreover, we have*

$$\mathrm{supp}(G) \;=\; \{\, 1, \ldots, N \,\} \setminus \{i\}.$$

Proof. Let F and F' be two arbitrary cosets from $\widehat{\mathcal{D}}_6$. Using the same idea we used for the proof of Proposition 5.3, we can say *if $F + F'$ has minimum weight 4, then the set of the children of F and the set of the children of F' do not intersect.* That is particularly true when we consider cosets in $\mathcal{B}_2$.

From Proposition 4.5 we know that there are $(N-1)(5N+8)/6$ distinct cosets of weight 6 in $\mathcal{B}_2$. Each such coset has exactly N children because any coset of weight 6 is an orphan. Since all children of such cosets are distinct, we obtain $N(N-1)(5N+8)/6$ distinct cosets of weight 5. But from Proposition 3.3 we know that this is exactly the number $\widehat{\Gamma}(5)$ of different cosets of weight 5. Therefore, any coset G from $\widehat{\mathcal{D}}_5$ is a child of some coset F from $\widehat{\mathcal{D}}_6$. We have $G = F + v^{(i)}$ for some i. Clearly, a leader of the coset G cannot have the position i in its support. So G is not an orphan and we have $\mathrm{supp}(G) \subseteq \{\, 1, \ldots, N \,\} \setminus \{i\}$. Suppose now that there is another position j which is not covered by $\mathrm{supp}(G)$. Then there is a contradiction with the fact that any coset of $\mathcal{D}_5$ is an orphan. Indeed, we can suppose that $j = 0$ because of the invariance of cosets of $\mathcal{B}$ under affine permutations. With this hypothesis, shortening G we obtain a coset of B of weight 5 which is not an orphan because ith position is not covered by the nonzero position of its leaders. According to Proposition 3.2 we have a contradiction. ∎

6. Summary of results. In this section we summarize the results we have about the weight distribution of the cosets of the code B and of its extension. These results are explained in sections 3, 4, and 5. In Table 2, the values we know for the number of cosets of a given weight are presented. We give the distance matrices of B and $\widehat{B}$ in Tables 3 and 4. Let C be a code with the dual distance t. Recall that the distance matrix of C is the $u \times (t+1)$ matrix containing the $t+1$ first coefficients of the u distinct weight distributions of cosets of C. The weight distributions of the cosets of C can be fully calculated from these elements [12].

TABLE 2
The number $\Gamma(i)$ of cosets of B of weight i and the number $\widehat{\Gamma}(i)$ of cosets of $\widehat{B}$ of weight i. We denote by γ the number of cosets of $\widehat{B}$ of weight 4 which are not in $R(m-2, m)$.

i	$\Gamma(i)$	$\widehat{\Gamma}(i)$
1	n	N
2	$n(n-1)/2$	$N(N-1)/2$
3	$n(n-1)(n-2)/6$	$N(N-1)(N-2)/6$
4	?	$(N-1)(N-2)/6 \;+\; \gamma$
5	$= \widehat{\Gamma}(6)$	$N(N-1)(5N+8)/6$
6	0	?

In Table 2, it clearly appears that the knowledge of γ involves the knowledge of any $\widehat{\Gamma}(i)$, implying the knowledge of any $\Gamma(i)$ since we know the total number of cosets. The coefficients of the distance matrix of B (see Table 3) depend only on those of the distance matrix of $\widehat{B}$ (see Table 4). Moreover, we have proved that all

TABLE 3
The distance matrix of the code B of length n, $n = 2^m - 1$, m odd.

0 1 2	3	4	5
1 0 0	0	0	0
0 1 0	0	0	0
0 0 1	0	0	$(n-1)(n-7)/120+1$
0 0 0	1	$\widehat{\mu}_{4,4}-1$	$\widehat{\mu}_{3,5}-\widehat{\mu}_{4,4}+1$
0 0 0	1	$\cdots$	$\cdots$
0 0 0	0	$\widehat{\mu}_{4,4} \le (n-7)/4$	$\widehat{\mu}_{5,5}-\widehat{\mu}_{4,4}$
0 0 0	$\cdots$	$\cdots$	$\cdots$
0 0 0	0	0	$(n-1)(n-7)/120$

TABLE 4
The distance matrix of the code $\widehat{B}$ of length N, $N = 2^m$, m odd.

0 1 2 3	4	5	6
1 0 0 0	0	0	0
0 1 0 0	0	0	0
0 0 1 0	0	0	$(N-2)(N^2-10N+136)/720$
0 0 0 1	0	$(N-2)(N-8)/120+1$	0
0 0 0 0	$\widehat{\mu}_{4,4} \le (N-8)/4$	0	$\widehat{\mu}_{4,6}$
0 0 0 0	$\cdots$	0	$\cdots$
0 0 0 0	$N/4$	0	$N(N-8)(N-32)/720$
0 0 0 0	0	$(N-2)(N-8)/120$	0
0 0 0 0	0	0	$N(N-2)(N-8)/720$

coefficients of the distance matrix of $\widehat{B}$ are known as soon as the possible values of $\widehat{\mu}_{4,4}$ are known (see Proposition 5.2).

Therefore, we conclude that *the problem of the weight distribution of the cosets of the* 3*-error-correcting BCH-codes, extended or not (i.e., B or $\widehat{B}$), is reduced to the problem of the weight distribution of the cosets of weight* 4 *of $\widehat{B}$, which are not in the Reed–Muller code of order $m-2$.*

7. Numerical results and conjectures. For length 128 we have computed the cosets weight distribution of $\widehat{B}$. We give in Table 5 the distance matrix and the number of cosets for each weight. Note that in this case, we obtain 12 distinct weight distributions, whereas we had 8 weight distributions for length 32. So we conjecture that the number of weight distributions increases with the length. We will make our conjecture precise later. Now we want to explain how Table 5 was completed.

- The number of cosets and the corresponding lines of the distance matrix are known for cosets of weight 1, 2, 3, or 5 for any length (see sections 3 and 6).
- So it remains to determine the number of cosets of weight 4 or 6 and the weight distributions of the cosets of weight 4. For the computation of weight distributions we only need to determine the number of leaders. We use the definition of cosets by syndrome (see Definition 4.2).
- We know the number of cosets of weight 4 or 6 contained in $\mathcal{B}_2$, i.e., in $R(m-2,m)$ (see Proposition 4.5). There are 127×21 cosets of weight 4 and 127×108 cosets of weight 6. Such a coset of weight 4 has 32 leaders; it is an orphan. Our numerical results prove that all orphans of weight 4 are in $\mathcal{B}_2$.
- From now on we study the cosets of weight 4 or 6 contained in $\mathcal{B}_1$, i.e., in $R(m-1,m)\backslash R(m-2,m)$. There are 127×2^{14} cosets in $\mathcal{B}_1$, whose 127×64 have

weight 2. So there remain 127×16320 cosets of weight 4 or 6. Actually, we have computed the syndrome of any code word of weight 4 which is not in $R(m-2, m)$. Taking into account the results of section 4 it is sufficient to consider the syndromes

$$(\ 0, \ 1, \ 0, \ \lambda \ ) \quad \text{and} \quad (\ 0, \ 1, \ 1, \ \lambda \ ), \quad \lambda \in GF(128).$$

Indeed, they define $128 + 127$ cosets of weight 4 or 6; the syndrome $(0, 1, 1, 1)$ corresponds to a coset of weight 2. From Proposition 4.6 each of these cosets has 127×64 equivalent cosets. Then we obtain

$$127 \times 64 \times (128 + 127) = 127 \times 16320$$

distinct cosets, and it is exactly the number of cosets of weight 4 or 6 in $\mathcal{B}_1$. So we need to examine a few code words of weight 4; the number of such code words of the same syndrome is the number of leaders.

- We found that 127×192 syndromes correspond to cosets of weight 6. By adding the number of such cosets in $\mathcal{B}_2$, we obtain the total number of cosets of weight 6. There remain 127×16128 cosets of weight 4 in $\mathcal{B}_1$. The number of leaders is even, in accordance with Proposition 4.6. This number takes all even value in the range $[2, 10]$.

TABLE 5

The distance matrix of the 3*-error-correcting extended BCH-code of length* 128; $W_{\min}$ *is the minimum weight of the coset.*

$W_{\min}$	Number of cosets	Number of words of weight: 0	1	2	3	4	5	6
0	1	1	0	0	0	0	0	0
1	128	0	1	0	0	0	0	0
2	$127 \times 64 = 8128$	0	0	1	0	0	0	2667
3	$127 \times 2688 = 341376$	0	0	0	1	0	127	0
4	$127 \times 1792 = 227584$	0	0	0	0	2	0	2648
4	$127 \times 6272 = 796544$	0	0	0	0	4	0	2608
4	$127 \times 5376 = 682752$	0	0	0	0	6	0	2568
4	$127 \times 2240 = 284480$	0	0	0	0	8	0	2528
4	$127 \times 448 = 56896$	0	0	0	0	10	0	2488
4	$127 \times 21 = 2667$	0	0	0	0	32	0	2048
5	$127 \times 13824 = 1755648$	0	0	0	0	0	126	0
6	$127 \times 300 = 38100$	0	0	0	0	0	0	2688

By using Tables 3 and 5, it is very easy to compute the distance matrix of the code B (of length 127). We also easily obtain the number of cosets of B of weight i, $i \in [0, 5]$, by using Table 2. It is more complicated if we want to compute to number of cosets of weight 3 or 4 for each weight distribution. We proceed as follows.

- Let $x(i)$ be the number of cosets of $\widehat{B}$ of weight 4 such that $\widehat{\mu}_{4,4} = i$, $i < N/4$.
- Then $x(i) = 127 \times 64 \times y(i)$, where $y(i)$ is the number of nonequivalent cosets in the sense of (16); we can suppose that the $y(i)$ cosets have position zero in their support.
- Let F be such a coset. The cardinality of its support is $4i$. Consider the 64 cosets $\sigma_{1,v}(F)$. Among these cosets $2i$ have position zero in their support and $64 - 2i$ have not.
- So we obtain from F, $127 \times 2i$ cosets of weight 3 of B and $127 \times (64 - 2i)$ cosets of weight 4 of B. Multiplying these numbers by $y(i)$, we obtain the number of cosets of weight 3 and 4 whose weight distributions are defined by $\widehat{\mu}_{4,4} = i$.

• From the 127×21 orphans of weight 4, we obtain the same number of cosets of B of weight 3. They correspond to one and only one weight distribution.

Recall that, for length 32, all cosets of weight 4 have the same weight distribution with $\widehat{\mu}_{4,4} = 2$. It is because in this case the code $\widehat{B}$ is exactly the Reed–Muller code of order 2. Any coset of weight 4 is a coset of the RM-code of minimum weight 8. Since the supports of these code words of weight 8 are the affine subspaces of K^5 of dimension 3, it is clear that such a coset cannot contain more than two words of weight 4.

For length 128, we have found six different weight distributions for the cosets of weight 4. For length 512, we made a random exploration of cosets of weight 4. Our numerical results allow us to state the following conjecture.

Conjecture 1. Let $\widehat{B}$ be the extended 3-error-correcting BCH-code of length 512. There are 12 different weight distributions for the cosets of $\widehat{B}$ of weight 4. These distributions are determined by the number $\widehat{\mu}_{4,4}$ of code words of weight 4. This number is

1. $\widehat{\mu}_{4,4} = 128$ for the orphans contained in the RM-code of order 7. (We did not find other cosets corresponding to this value.)
2. $\widehat{\mu}_{4,4} = i$ for all even integers i in the range $[12, 32]$.

So we have shown that the situation here is completely different from those we had for the 2-error-correcting BCH-codes. In both cases the external distance is a constant not depending on the length. The number of weight distributions of cosets is constant for any length for the 2-error-correcting BCH-codes. And that is true not only when m is odd (and codes are completely regular) but also when m is even [10, 20]. For the 3-error-correcting BCH-codes, we strongly conjecture that this number increases with the length. When m is odd these codes are uniformly packed, and we point out this property for $m = 5, 7$, and 9. Moreover, we are able to propose general conjectures.

Conjecture 2. Let $\widehat{B}$ be the extended 3-error-correcting BCH-code of length N, m odd. *Then any coset of $\widehat{B}$ of weight 4, which is an orphan, is contained in the RM-code of order $m-2$.*

Conjecture 3. Denote by G the Galois field of order 2^m, m odd. For any (A, B), where A and B are any elements in G, let us denote by $\mathcal{E}(A, B)$ the following system of three equations, with four variables, on G:

$$\begin{aligned} W + X + Y + Z &= 1, \\ W^3 + X^3 + Y^3 + Z^3 &= A, \\ W^5 + X^5 + Y^5 + Z^5 &= B. \end{aligned}$$

Let $\mathcal{N}(A, B)$ be the number of solutions of $\mathcal{E}(A, B)$ satisfying $X \neq Y \neq Z \neq W$. Consider the (A, B) such that $\mathcal{N}(A, B)$ is not zero and recall that $\mathcal{N}(A, B)$ is always even (see Proposition 4.6). *Then there exist two even integers depending on m, say ℓ_m and u_m, $\ell_m < u_m < 2^{m-2}$, such that*

$$\ell_m \leq N(A, B) \leq u_m.$$

Moreover, for any even value i in the range $[\ell_m, u_m]$, there is an (A, B) such that $\mathcal{N}(A, B) = i$.

Acknowledgments. The authors are indebted to Nicolas Sendrier for computing some numerical results and checking others with his own programs. They are grateful to the anonymous referee who indicated several improvements of the manuscript.

The second author thanks Paul Camion for the possibility to work in INRIA (project CODES) as an invited professor in 1994 and 1995.

REFERENCES

[1] E. F. Assmus, Jr. and H. F. Mattson, Jr., *Some* 3*-error-correcting BCH codes have covering radius* 5, IEEE Trans. Inform. Theory, IT-22 (1976), pp. 348–349.

[2] E. F. Assmus, Jr. and V. Pless, *On the covering radius of extremal self-dual codes*, IEEE Trans. Inform. Theory, IT-29 (1983), pp. 359–363.

[3] L. A. Bassalygo, G. V. Zaitsev, and V. A. Zinoviev, *Uniformly packed codes*, Problems Inform. Transmission, 10 (1974), pp. 9–14.

[4] L. A. Bassalygo and V. A. Zinoviev, *Remark on uniformly packed codes*, Problems Inform. Transmission, 13 (1977), pp. 22–25.

[5] R. A. Brualdi and V. S. Pless, *Orphans of the first order Reed-Muller codes*, IEEE Trans. Inform. Theory, IT-36 (1990), pp. 399–401.

[6] P. Camion, B. Courteau, G. Fournier, and S. V. Kanetkar, *Weight distribution of translates of linear codes and generalized Pless Identities*, J. Inform. Optim. Sci., 8 (1987), pp. 1–23.

[7] P. Camion, B. Courteau, and A. Montpetit, *Coset weight enumerators of the extremal self-dual binary codes of length* 32, Eurocode '92: International Symposium on Coding Theory and Applications, CISM International Centre for Mechanical Sciences Ser. Vol. 339, P. Camion and P. Charpin, eds., Springer-Verlag, Amsterdam, The Netherlands, 1993, pp. 17–30.

[8] P. Camion, B. Courteau, and P. Delsarte, *On r-partition designs in Hamming spaces*, Applicable Algebra in Eng. Comm. and Comput., 2 (1992), pp. 147–162.

[9] P. Charpin, *Tools for cosets weight enumerators of some codes*, in Proceedings of Finite Fields: Theory, Applications and Algorithmes, G. L. Mullen and P. Jau-Shyong, eds., Contemporary Mathematics, Vol. 168, AMS, Providence, RI, 1994.

[10] P. Charpin, *Weight distributions of cosets of* 2*-error-correcting binary BCH codes, extended or not*, IEEE Trans. Inform. Theory, IT-40 (1994), pp. 1425–1442.

[11] P. Charpin and V. A. Zinoviev, *On weight distributions of cosets of* 3*-error-correcting extended BCH codes of length* 2^m*, m odd*, in Proceedings ACCT4 '94 Fourth International Workshop. Algebraic and Combinatorial Coding Theory, Novgorod, Russia, 1994, pp. 66–69.

[12] P. Delsarte, *Four fundamental parameters of a code and their combinatorial significance*, Inform. and Control, 23 (1973), pp. 407–438.

[13] J. M. Goethals and H. C. A. Van Tilborg, *Uniformly packed codes*, Philips Res. Rep., 30 (1975), pp. 9–36.

[14] D. Gorenstein, W. W. Peterson, and N. Zierler, *Two-error-correcting Bose-Chaudhuri codes are quasi-perfect*, Inform. and Control, 3 (1960), pp. 291–294.

[15] T. Helleseth, *All binary* 3*-error-correcting BCH codes of length* $2^m - 1$ *have covering radius* 5, IEEE Trans. Inform. Theory, IT-24 (1978), pp. 257–258.

[16] J. A. van der Horst and T. Berger, *Complete decoding of triple-error-correcting binary BCH codes*, IEEE Trans. Inform. Theory, IT-22 (1976), pp. 138–147.

[17] T. Kasami, *Weight distributions of Bose-Chaudhuri-Hocquenghen codes*, in Combinatorial Mathematics and its Applications, R. C. Bose and T. A. Dowling, eds., Univ. of North Carolina Press, Chapel Hill, NC, 1969.

[18] 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), pp. 475–496.

[19] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*, North–Holland, Amsterdam, The Netherlands, 1986.

[20] N. V. Semakov, V. A. Zinoviev, and G. V. Zaitsev, *Uniformly packed codes*, Problems Inform. Transmission, 7 (1971), pp. 38–50.

[21] H. C. A. Van Tilborg, *Uniformly Packed Codes*, Ph.D. thesis, Tech. Univ. Eindhoven, Eindhoven, The Netherlands, 1976.

[22] X.-D. Hou, *Classification of cosets of the Reed-Muller code $R(m-3, m)$*, Discrete Math., 128 (1994), pp. 203–224.