The Coset Distribution of Triple-Error-Correcting Binary Primitive BCH Codes

Pascale Charpin, *Member, IEEE*, Tor Helleseth, *Fellow, IEEE*, and Victor A. Zinoviev

***Abstract*—Binary primitive triple-error-correcting Bose–Chaudhuri–Hocquenghem (BCH) codes of length $n = 2^m - 1$ have been the object of intensive studies for several decades. In the 1970s, their covering radius was determined in a series of papers to be $\rho = 5$. However, one problem for these codes that has been open up to now is to find their coset distribution. In this paper this problem is solved and the number of cosets of each weight in any binary primitive triple-error-correcting BCH code is determined. As a consequence this also gives the coset distribution of the extended codes of length $N = 2^m$ with minimum distance 8.**

***Index Terms*—Bose–Chaudhuri–Hocquenghem (BCH) codes, coset distribution, covering radius.**

I. Introduction

Let GF(2^m) denote the finite field with 2^m elements. A binary linear $[n, k]$-code C is a k-dimensional subspace of GF$(2)^n$. The Hamming distance between two vectors is the number of components in which they differ. The minimum distance of the code is the smallest Hamming distance between any two distinct codewords in the code. A coset of the code C is the set of vectors $a + C$ for some $a \in$ GF$(2)^n$. The coset leader for a coset of a linear code is a vector of smallest weight in the coset. The weight of a coset is the weight of a coset leader. For an optimal complete decoding algorithm for a linear code, where all codewords are sent equally often, the errors which are corrected are exactly the coset leaders. An important problem in determining the performance of a linear code is therefore to determine the distribution of the cosets of the code (i.e., to determine the number of cosets of each weight).

The family of triple-error-correcting binary primitive Bose–Chaudhuri–Hocquenghem (BCH) codes of length $n = 2^m - 1$ has been thoroughly studied since the 1960s. The weight distribution of these codes was determined by Kasami [9] for odd m. For even m the method of Kasami did not work. Berlekamp [2, Table 16.5], [3] and [4] gave the weight distribution of the extended codes for even values of m. The covering radius of a code is the maximum weight of a coset leader. In the 1970s, the covering radius of these codes were shown in a series of papers by Assmus and Mattson [1], van der Horst and Berger [8] and Helleseth [7] to be $\rho = 5$. However, one problem for the triple-error-correcting binary primitive BCH codes that has been open up to now is to find the coset distribution of these codes.

We will assume throughout the rest of this paper that $m \geq 5$ since the number of cosets of the binary triple-error-correcting code in this case is 2^{3m} (cf. MacWilliams and Sloane [10, p. 262]), while the case $m = 4$ is degenerated in the sense that it only contains $2^{5m/2}$ cosets, since α^5 has a minimum polynomial of degree $m/2 = 2$. Let K_i denote the number of cosets of weight i. Since the code is triple-error-correcting the values of K_0, K_1, K_2 and K_3 are immediately given by

$$K_0 = 1, \quad K_1 = \binom{n}{1}, \quad K_2 = \binom{n}{2}, \quad K_3 = \binom{n}{3}.$$

Since the covering radius of the code is known to be 5, it is therefore sufficient to determine K_4 and K_5. Some partial results were given by van der Horst and Berger [8] who came up with the following bounds for K_4 and K_5:

$$K_4 \leq \frac{1}{6}n(5n^2 + 10n - 3) \text{ and } K_5 \geq \frac{4}{3}n(n + 2)$$

and they conjectured that equality holds for $m \geq 8$. They were able to prove this conjecture for $8 \leq m \leq 12$ using a computer search. They further verified that the conjecture does not hold for $m = 5, 6$ and 7. The main result of this paper is to show that their 30-year-old conjecture holds and therefore to prove the following theorem.

Theorem 1: Let K_i denote the number of cosets with a coset leader of weight i in a triple-error-correcting binary primitive BCH code of length $n = 2^m - 1$ where $m \geq 8$. Then the distribution of the cosets is given by

$$\begin{aligned} K_0 &= 1 \\ K_1 &= \binom{n}{1} \\ K_2 &= \binom{n}{2} \\ K_3 &= \binom{n}{3} \\ K_4 &= \frac{1}{6}n(5n^2 + 10n - 3) \\ K_5 &= \frac{4}{3}n(n + 2). \end{aligned}$$

One should observe that an even harder problem is the "full" problem to find the weight distribution of the vectors in any coset of the binary primitive triple-error-correcting codes (or their extended codes). This problem has been studied in the papers by Charpin and Zinoviev [6] and Charpin, Helleseth, and Zinoviev [5]. This problem remains open for even m while it was solved (i.e., expressed in terms of some exponential sums) for odd m in these papers.

II. Cosets of BCH Codes of Length $n = 2^m - 1$

The proof of our main result in Theorem 1 will be rather self-contained. We will apply and simplify some of the techniques developed in van der Horst and Berger [8] in combination with some new ideas needed to prove their conjecture. The focus of the very long and technical paper by van der Horst and Berger [8] was to construct a complete decoding algorithm for the triple-error-correcting BCH code. Their studies of the complete decoding algorithm was partially motivated by the desire to use the triple-error-correcting BCH code in source coding. We will mainly focus on the distribution of the weights of the cosets in order to prove their conjecture.

The binary triple-error-correcting primitive BCH code has parity-check matrix H defined by

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ 1 & \alpha^3 & \alpha^6 & \dots & \alpha^{3(n-1)} \\ 1 & \alpha^5 & \alpha^{10} & \dots & \alpha^{5(n-1)} \end{bmatrix}$$

Manuscript received January 19, 2005; revised November 14, 2005. This work was supported by INRIA-Rocquencourt, by the Norwegian Research Council, and by the Russian fund of fundamental research under Project Number 03-01-00098. The material in this correspondence was presented in part at the 2005 IEEE International Symposium on Information Theory, Adelaide, Australia, September 2005.

P. Charpin is with INRIA, Codes, Domaine de Voluceau-Rocquencourt, Le Chesnay 78153, France (e-mail: pascale.charpin@inria.fr).

T. Helleseth is with The Selmer Center, Department of Informatics, University of Bergen, Bergen N-5020, Norway (e-mail: tor.helleseth@ii.uib.no).

V. A. Zinoviev is with the Institute for Problems of Information Transmission, Russian Academy of Sciences, Moscow 101447, Russia (e-mail: zinov@iitp.ru).

Communicated by A. E. Ashikhmin, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2006.871605

where α is an element of order $n = 2^m - 1$ in GF(2^m), i.e., the code consists of all binary codewords $\boldsymbol{c} = (c_0, c_1, \ldots, c_{n-1}) \in \text{GF}(2)^n$ such that $\boldsymbol{c}H^{tr} = \boldsymbol{0}$.

The syndrome $\boldsymbol{s}$ of a received vector $\boldsymbol{r}$ is

$$\boldsymbol{s} = \boldsymbol{r}H^{tr} = (S_1, S_3, S_5)$$

where $\boldsymbol{r} = (r_0, r_1, \ldots, r_{n-1})$ and H^{tr} denotes the transpose of the matrix H.

The decoding starts by computing the syndrome of the received vector and then finding a coset leader in the coset with the same syndrome $\boldsymbol{s} = (S_1, S_3, S_5)$. The vectors in a coset all have the same syndrome and our problem is to find a coset leader, i.e., a vector of smallest possible weight with this syndrome. Therefore we need to find nonzero and distinct elements $X_1, X_2, \ldots, X_w$ (the error-locations) in GF(2^m) with the smallest possible w such that

$$S_i = \sum_{j=1}^{w} X_j^i \tag{1}$$

for $i = 1, 3, 5$. Equivalently, we need to determine a locator polynomial

$$\sigma(X) = \prod_{i=1}^{w}(X + X_i) = X^w + \sigma_1 X^{w-1} + \cdots + \sigma_w$$

of minimal weight w, such that (1) holds with nonzero and distinct X_i's in GF(2^m).

The Newton identities give a relation between the coefficients of the locator polynomial $\sigma(X)$ and the error-locations via

$$\begin{aligned} S_1 + \sigma_1 &= 0 \\ S_2 + \sigma_1 S_1 + 2\sigma_2 &= 0 \\ S_3 + \sigma_1 S_2 + \sigma_2 S_1 + 3\sigma_3 &= 0 \\ &\cdots \\ S_i + \sigma_1 S_{i-1} + \sigma_2 S_{i-2} + \cdots + i\sigma_i &= 0 \end{aligned}$$

for $i \leq w$. For $i > w$ then

$$S_i + \sigma_1 S_{i-1} + \cdots + \sigma_{w-1} S_{i-w+1} + \sigma_w S_{i-w} = 0.$$

We use the convention that $\sigma_i = 0$ when $i > w$.

The Newton identities imply

$$\begin{aligned} S_1 &= \sigma_1, \\ S_3 &= \sigma_1 S_1^2 + \sigma_2 S_1 + \sigma_3, \\ S_5 &= \sigma_1 S_1^4 + \sigma_2 S_3 + \sigma_3 S_1^2 + \sigma_4 S_1 + \sigma_5. \end{aligned}$$

Throughout this correspondence, we define the trace function from GF(2^m) to GF(2) by

$$Tr(x) = \sum_{i=0}^{m-1} x^{2^i}.$$

A. The Cosets of Weight $w = 1$

The locator polynomial of a coset leader of weight 1 is

$$\sigma(X) = X + S_1$$

since the syndrome (S_1, S_3, S_5) is given by $S_j = X_1^j$ for $j = 1, 3, 5$. The cosets of weight 1 are therefore the n cosets with syndromes of the form $\left(S_1, S_1^3, S_1^5\right)$ where $S_1 \neq 0$.

B. The Cosets of Weight $w = 2$

The locator polynomial of a coset leader of weight 2 corresponding to the error-locations X_1 and X_2 leads to a syndrome given by $S_j = X_1^j + X_2^j$ for $j = 1, 3, 5$. Note that $S_1 \neq 0$ since the error-locations are distinct. We obtain by simple direct calculations from the Newton identities that $S_3 = S_1^3 + \sigma_2 S_1$ and $S_5 = S_1^5 + \sigma_2 S_3$.

Comparing the two expressions for σ_2, we have

$$\sigma_2 = (S_3 + S_1^3)/S_1 = \left(S_5 + S_1^5\right)/S_3.$$

Since $\sigma_1 = S_1$, the locator polynomial in the case of a coset leader of weight 2 is given by

$$\sigma(X) = X^2 + S_1 X + \left(S_3 + S_1^3\right)/S_1. \tag{2}$$

This polynomial has two distinct nonzero zeros in GF(2^m) when $S_1 \neq 0$, $S_3 \neq S_1^3$ and $Tr\left(\left(S_3 + S_1^3\right)/S_1^3\right) = 0$.

Note that the two expressions for σ_2 lead to the following relations between the syndrome components

$$M = S_3^2 + S_1^3 S_3 + S_5 S_1 + S_1^6 = 0.$$

Observe that there are n choices of $S_1 \neq 0$ and $(n-1)/2$ choices of $S_3 \neq S_1^3$ such that $Tr\left(\left(S_3 + S_1^3\right)/S_1^3\right) = 0$. Therefore the cosets with syndromes (S_1, S_3, S_5) where $S_1 \neq 0$, $S_3 \neq S_1^3$, $Tr\left(\left(S_3 + S_1^3\right)/S_1^3\right) = 0$ and S_5 is such that the condition $M = 0$ holds are all the $\binom{n}{2}$ cosets of weight 2.

C. The Cosets of Weight $w = 3$

In this case, the Newton identities lead to $\sigma_1 = S_1$ and the following two expressions for σ_3:

$$\sigma_3 = S_3 + S_1^3 + \sigma_2 S_1$$

and

$$\sigma_3 S_1^2 = S_5 + S_1^5 + \sigma_2 S_3.$$

Note that if $S_3 = S_1^3$ the first expression substituted into the second one implies $S_5 = S_1^5$, contradicting that $w = 3$. Therefore, $S_3 \neq S_1^3$ and comparing the expressions above leads to

$$\sigma_2 = \frac{S_5 + S_1^2 S_3}{S_3 + S_1^3}$$

and substituting for σ_2 in the expression for σ_3 gives

$$\begin{aligned} \sigma_3 &= S_3 + S_1^3 + \sigma_2 S_1 \\ &= \frac{S_3^2 + S_1^6 + S_5 S_1 + S_1^3 S_3}{S_3 + S_1^3} \\ &= \frac{M}{S_3 + S_1^3} \end{aligned}$$

where

$$M = S_3^2 + S_1^3 S_3 + S_5 S_1 + S_1^6.$$

Hence, the locator polynomial in the case $w = 3$ is

$$\sigma(X) = X^3 + S_1 X^2 + \frac{S_5 + S_1^2 S_3}{S_3 + S_1^3} X + \frac{M}{S_3 + S_1^3}. \tag{3}$$

Note that $M \neq 0$ since $\sigma_3 = X_1 X_2 X_3 \neq 0$ (all X_i are nonzero elements) for the case of an error corresponding to a coset leader of weight 3.

Even though we do not need this fact in this paper it is useful for the decoding algorithm of these codes to observe that it follows from well

known properties of cubic polynomials that a necessary condition for three distinct zeros of the locator polynomial is that

$$Tr\left(\frac{\left(S_5+S_1^5\right)^3}{\left(S_3+S_1^3\right)^5}+1\right)=0.$$

D. The Cosets of Weight $w=5$

We will study the conditions for cosets of weight $w=5$ with a locator polynomial with nonzero distinct zeros X_1, X_2, X_3, X_4 and X_5. The following theorem characterizes some particular cosets of weight 5 in the triple-error-correcting codes with a syndrome (S_1, S_3, S_5) where $S_1 \neq 0$. These will later be shown to be all cosets of weight $w=5$ with $S_1 \neq 0$.

Theorem 2: Let D be a coset with syndrome (S_1, S_3, S_5) such that $S_1 \neq 0$, $M = S_3^2 + S_1^3 S_3 + S_5 S_1 + S_1^6 = 0$, and $Tr\left(\left(S_3+S_1^3\right)/S_1^3\right)=1$. Then D is a coset of weight 5.

Proof: Since the covering radius of the triple-error-correcting BCH code is known to be 5, it is sufficient to show that the weight w of the coset D is at least 5. Since $S_1 \neq 0$ the coset has weight at least 1. By the trace condition in the theorem it follows that $S_3 \neq S_1^3$ and therefore the coset has weight at least 2. Further, since $Tr\left(\left(S_3+S_1^3\right)/S_1^3\right)=1$ it follows that $w \neq 2$ since the locator polynomial (2) for $w=2$ does not have its zeros in GF(2^m) unless $Tr\left(\left(S_3+S_1^3\right)/S_1^3\right)=0$. The coset cannot have weight 3 either, since the locator polynomial (3) for a vector of weight 3 has constant term 0 when $M=0$ and therefore cannot have three distinct nonzero zeros. It follows that the coset has weight at least 4. We therefore assume that the coset has weight 4 and we will show that this is impossible.

From the Newton identities, we obtain

$$\sigma_3 = S_3 + S_1^3 + \sigma_2 S_1$$

and

$$\sigma_4 = \frac{S_5 + S_1^5 + \sigma_2 S_3 + \sigma_3 S_1^2}{S_1}.$$

Substituting for σ_3 in the expression for σ_4 gives

$$\sigma_4 = \frac{S_5 + S_3 S_1^2 + \sigma_2 (S_3 + S_1^3)}{S_1}.$$

Hence, the locator polynomial is

$$\sigma(X) = X^4 + S_1 X^3 + \sigma_2 X^2 + \left(S_3 + S_1^3 + \sigma_2 S_1\right) X + \frac{S_5 + S_3 S_1^2 + \sigma_2\left(S_3 + S_1^3\right)}{S_1}. \quad (4)$$

Since this polynomial has four distinct zeros in GF(2^m) it can be factored as

$$\sigma(X) = (X^2 + aX + b)(X^2 + (a+S_1)X + d). \quad (5)$$

Comparing coefficients, we obtain

$$\sigma_2 = d + b + a(a+S_1)$$
$$\sigma_3 = ad + b(a+S_1)$$
$$\sigma_4 = bd.$$

From the first identity, we obtain

$$d = \sigma_2 + b + a(a+S_1)$$

and from the second, we get

$$\begin{aligned}\sigma_3 &= ad + b(a+S_1)\\ &= a\sigma_2 + ab + a^2(a+S_1) + ab + bS_1\\ &= a\sigma_2 + a^2(a+S_1) + bS_1.\end{aligned}$$

Hence,

$$b = \frac{\sigma_3 + a\sigma_2 + a^2(a+S_1)}{S_1}$$

and substituting the value for b in the expression for d above gives

$$d = \frac{\sigma_3 + (a+S_1)\sigma_2 + a(a+S_1)^2}{S_1}.$$

The third identity now gives

$$\left(\sigma_3 + a\sigma_2 + a^2(a+S_1)\right)\left(\sigma_3 + (a+S_1)\sigma_2 + a(a+S_1)^2\right) = \sigma_4 S_1^2.$$

Substituting

$$\sigma_3 = S_3 + S_1^3 + \sigma_2 S_1$$

and

$$\sigma_4 = \frac{S_5 + S_3 S_1^2 + \sigma_2\left(S_3 + S_1^3\right)}{S_1}$$

into this expression, we obtain

$$\begin{aligned}&\left((a+S_1)\sigma_2 + S_3 + S_1^3 + a^2(a+S_1)\right)\\ &\quad\times\left(a\sigma_2 + S_3 + S_1^3 + a(a+S_1)^2\right)\\ &\quad= S_5 S_1 + S_3 S_1^3 + \sigma_2\left(S_3 S_1 + S_1^4\right).\end{aligned}$$

Collecting the coefficients of σ_2^2, σ_2 and the constant term and dividing the resulting expression by $a(a+S_1)S_1^4$ gives

$$\left(\frac{\sigma_2}{S_1^2}\right)^2 + \left(\frac{\sigma_2}{S_1^2}\right) + k = 0 \quad (6)$$

where

$$\begin{aligned}k &= \frac{S_3^2 + S_1^6 + S_5 S_1 + S_3 S_1^3}{S_1^4 a(a+S_1)} + \frac{S_3 + S_1^3}{S_1^3} + \frac{a^2(a+S_1)^2}{S_1^4}\\ &= \frac{M}{S_1^4 a(a+S_1)} + \frac{S_3 + S_1^3}{S_1^3} + \frac{a^2(a+S_1)^2}{S_1^4}\\ &= \frac{M/S_1^6}{x(x+1)} + \frac{S_3 + S_1^3}{S_1^3} + x^2(x^2+1) \quad (7)\end{aligned}$$

and $x = a/S_1$. The trace of k is given by

$$\begin{aligned}Tr(k) &= Tr\left(\frac{M/S_1^6}{x(x+1)} + \frac{S_3 + S_1^3}{S_1^3} + x^4 + x^2\right)\\ &= Tr\left(\frac{M/S_1^6}{x(x+1)} + \frac{S_3 + S_1^3}{S_1^3}\right). \quad (8)\end{aligned}$$

Since $M=0$, the trace condition in the theorem gives

$$Tr(k) = Tr\left(\frac{S_3 + S_1^3}{S_1^3}\right) = 1.$$

This contradicts (6) which only has a solution in GF(2^m) when $Tr(k)=0$, and therefore a coset weight of $w=4$ for D is impossible. Since the code has covering radius 5, we conclude that the coset D has weight 5. □

Remark 1: Note that the number of cosets of weight $w=5$ of this form is $n(n+1)/2$. This follows since there are n choices of $S_1 \neq 0$ and for each nonzero S_1, there are $(n+1)/2$ choices of S_3 such that $Tr\left(\left(S_3+S_1^3\right)/S_1^3\right)=1$. Observe that S_5 is uniquely determined by S_1 and S_3 since $M=0$.

The following result can be found in [8]. We include a simpler and more direct proof for the sake of completeness.

Lemma 1: There are $(5n^2+13n)/6$ cosets of weight 5 with $S_1=0$.

Proof: Note that, for $m > 4$, there are $(n+1)^2$ cosets with $S_1=0$. Further, observe that all nonzero cosets with $S_1=0$ must have odd weight. Indeed, as we saw above, it is impossible for cosets of weight 2, since $X_1 \neq X_2$. That cosets of weight 4 with $S_1=0$ are impossible can be seen from the following simple arguments. Assume that some coset D has syndrome $(S_1=0, S_3, S_5)$ and assume that X_1, X_2, X_3, and X_4 are error-locations of some vector of D. Recall, that X_1, X_2, X_3, X_4 are mutually distinct nonzero elements in GF(2^m). Now we see from (1) that for any $h \in$ GF(2^m) a 4-tuple $(X_1+h, X_2+h, X_3+h, X_4+h)$ forms the error-locations for a

vector with the same syndrome $(S_1 = 0, S_3, S_5)$. This can easily be verified by checking the syndrome of this 4-tuple and using that

$$\sum_{i=1}^{4} X_i^2 = \left(\sum_{i=1}^{4} X_i\right)^2 = S_1^2$$

and similarly

$$\sum_{i=1}^{4} X_i^4 = \left(\sum_{i=1}^{4} X_i\right)^4 = S_1^4.$$

Now take $h = X_1$, which is not forbidden. Then we obtain a 3-tuple $(X_2 + X_1, X_3 + X_1, X_4 + X_1)$ which has this syndrome. But this means that D is a coset of weight 3.

The number of nonzero cosets of weight 3 with $S_1 = 0$ are the number of (unordered) ways to select nonzero and distinct X_1, X_2 and X_3 such that $X_1 + X_2 + X_3 = 0$ and is therefore equal to $n(n-1)/6$. This means that the number of cosets of weight 5 with $S_1 = 0$ therefore is $((n+1)^2 - 1) - n(n-1)/6$ (since we cannot choose S_3 and S_5 both equal to zero), which equals $(5n^2 + 13n)/6$. □

Remark 2: Note that adding the number of cosets in Lemma 1 with $S_1 = 0$ to the number of cosets with $S_1 \neq 0$ in Remark 1 obtained from Theorem 2 we obtain the following useful bound

$$\begin{aligned} K_5 &\geq \frac{n(n+1)}{2} + \frac{5n^2 + 13n}{6} \\ &= \frac{4}{3} n(n+2). \end{aligned}$$

E. The Cosets of Weight $w = 4$

To prove the conjecture by van der Horst and Berger [8] it is sufficient to show that all cosets with $S_1 \neq 0$, except for the ones in Theorem 2, have weight at most 4.

In order to prove Theorem 3, we need the following crucial lemma which is proved by Moreno and Moreno [11].

Lemma 2: Let $\overline{F}$ be the algebraic closure of $F = \mathrm{GF}(2^m)$. Let $f(x), g(x) \in F[x]$ where $deg\, f < r = deg\, g$ and $g(x)$ is a polynomial with t distinct zeros in $\overline{F}$. Let L denote the set of zeros of $g(x)$ in F. If $\frac{f(x)}{g(x)} \neq h(x)^2 + h(x)$ for any rational function $h(x) \in \overline{F}(x)$, then

$$\left| \sum_{x \in F \setminus L} (-1)^{\mathrm{Tr}\left(\frac{f(x)}{g(x)}\right)} \right| \leq (t + r - 2)\sqrt{2^m} + 1.$$

Based on this lemma we are able to prove the following theorem. This is a key result in order to complete the determination of the coset distribution.

Lemma 3: Let $u \neq 0$, $u \in F = \mathrm{GF}(2^m)$. For $m \geq 10$ and for given $i = 0$ or 1 there exists an element $x \in F \setminus \{0, 1\}$ such that

$$\mathrm{Tr}\left(\frac{u}{x(x+1)}\right) = i$$

and

$$\mathrm{Tr}\left(\frac{u}{x(x+1)^3}\right) = \mathrm{Tr}\left(\frac{u}{x^3(x+1)}\right) = 0.$$

Proof: Let T be the number of elements in $F' = F \setminus \{0, 1\}$, obeying the conditions in the theorem. Further, let $e(f) = (-1)^{Tr(f)}$. Then standard methods give

$$\begin{aligned} 8T = &\sum_{x \in F'} \left(1 + e\left(\frac{u}{x(x+1)^3}\right)\right)\left(1 + e\left(\frac{u}{x^3(x+1)}\right)\right) \\ &\times \left(1 + (-1)^i e\left(\frac{u}{x(x+1)}\right)\right) \\ = &\sum_{x \in F'} 1 + \sum_{x \in F'} e\left(\frac{u}{x(x+1)^3}\right) + \sum_{x \in F'} e\left(\frac{u}{x^3(x+1)}\right) \\ &+ \sum_{x \in F'} e\left(\frac{u}{x^3(x+1)^3}\right) + \sum_{x \in F'} (-1)^i e\left(\frac{u}{x(x+1)}\right) \\ &+ \sum_{x \in F'} (-1)^i e\left(\frac{ux}{(x+1)^3}\right) + \sum_{x \in F'} (-1)^i e\left(\frac{u(x+1)}{x^3}\right) \\ &+ \sum_{x \in F'} (-1)^i e\left(\frac{u(x^4 + x^2 + 1)}{x^3(x+1)^3}\right). \end{aligned}$$

In order to apply the bound of Lemma 2, we have to check that all functions $a(x)/b(x)$ which appear in the sums above satisfy the condition of the lemma. We take, for example, the function $ux/(x+1)^3$. We have to show that there is no rational $h(x) \in \overline{F}(x)$ such that

$$\frac{ux}{(x+1)^3} = h(x)^2 + h(x). \tag{9}$$

Suppose, on the contrary, that there is a rational function $h(x) = a(x)/b(x)$ which satisfies (9). We can assume without loss of generality that gcd $(a(x), b(x)) = 1$. We obtain

$$uxb(x)^2 = (x+1)^3 a(x)(a(x) + b(x)).$$

This is a polynomial equality. So, the left-hand side of this equality is divisible by $(x+1)^3$. This means that $b(x)$ is divisible at least by $(x+1)^2$. But then, the right hand side of this equality is divisible by $(x+1)^4$, which is impossible, since $a(x)$ cannot be divisible by $x+1$ when $b(x)$ is divisible by $x+1$. We therefore conclude that the equality (9) is impossible. Hence we can apply Lemma 2 to this sum. The other functions in all the sums above are treated in the same way.

Using the bounds for the exponential sums given in the lemma above implies that all the last seven sums are upper bounded by $c\sqrt{2^m} + 1$, where c takes the values $4, 4, 6, 2, 2, 2$, and 6, respectively, starting from the first sum after $\sum 1$. It follows therefore that $8T \geq 2^m - 2 - 26\sqrt{2^m} - 7$ and so T is strictly positive for $m \geq 10$. □

Theorem 3: Let $m \geq 10$ and let D be a coset such that $S_1 \neq 0$ which does not obey both the conditions $M = S_3^2 + S_1^3 S_3 + S_5 S_1 + S_1^6 = 0$ and $Tr\left(\left(S_3 + S_1^3\right)/S_1^3\right) = 1$. Then D is a coset of weight at most 4.

Proof: We will show that we can find a polynomial $\sigma(X)$ of degree 4 with four zeros (not necessarily distinct) in $\mathrm{GF}(2^m)$ with the required syndrome. We will show that we can select the coefficient σ_2 of X^2 in the polynomial $\sigma(X)$ in (4) such that it has all zeros in $\mathrm{GF}(2^m)$. This implies that (1) holds and therefore that the coset has weight at most 4. If some of the zeros of $\sigma(X)$ are 0 or repeated this leads to a coset of weight less than 4.

Set x to be an element of $\mathrm{GF}(2^m) \setminus \{0, 1\}$, such that

$$\mathrm{Tr}\left(\frac{M/S_1^6}{x(x+1)}\right) = \mathrm{Tr}\left(\frac{S_3 + S_1^3}{S_1^3}\right)$$

and

$$\mathrm{Tr}\left(\frac{M/S_1^6}{x^3(x+1)}\right) = \mathrm{Tr}\left(\frac{M/S_1^6}{x(x+1)^3}\right) = 0.$$

This can be done by Lemma 3.

Set σ_2 to be a solution in $\mathrm{GF}(2^m)$ of the quadratic equation

$$\left(\frac{\sigma_2}{S_1^2}\right)^2 + \left(\frac{\sigma_2}{S_1^2}\right) + k = 0$$

where

$$k = \frac{M/S_1^6}{x(x+1)} + \frac{S_3 + S_1^3}{S_1^3} + x^2(x^2 + 1).$$

This can be done since $\mathrm{Tr}(k) = 0$, by the choice of x in the previous step. Then set

$$\begin{aligned}\sigma_1 &= S_1\\ \sigma_3 &= S_3 + S_1^3 + \sigma_2 S_1\\ \sigma_4 &= \frac{S_5 + S_3 S_1^2 + \sigma_2(S_3 + S_1^3)}{S_1}\end{aligned}$$

and

$$\begin{aligned}a &= S_1 x\\ b &= \frac{\sigma_3 + a\sigma_2 + a^2(a + S_1)}{S_1}\\ d &= \frac{\sigma_3 + (a + S_1)\sigma_2 + a(a + S_1)^2}{S_1}\end{aligned}$$

and

$$\sigma(X) = (X^2 + aX + b)(X^2 + (a + S_1)X + d).$$

Note that since $x \notin \{0, 1\}$ and $S_1 \neq 0$, we cannot have $a = 0$ nor $a = S_1$. Further, observe that

$$\begin{aligned}\mathrm{Tr}(b/a^2) &= \mathrm{Tr}\left(\frac{\sigma_3 + a\sigma_2 + a^2(a + S_1)}{a^2 S_1}\right)\\ &= \mathrm{Tr}\left(\frac{S_3 + S_1^3 + (a + S_1)\sigma_2 + a^2(a + S_1)}{a^2 S_1}\right)\\ &= \mathrm{Tr}\left(\frac{S_3 + S_1^3}{a^2 S_1} + \frac{\sigma_2}{aS_1} + \frac{\sigma_2}{a^2} + \frac{a}{S_1} + 1\right)\\ &= \mathrm{Tr}\left(\frac{S_3 + S_1^3}{a^2 S_1} + \frac{\sigma_2^2}{a^2 S_1^2} + \frac{\sigma_2}{a^2} + \frac{a}{S_1} + 1\right).\end{aligned}$$

Since $a = S_1 x$, then we obtain

$$\begin{aligned}\mathrm{Tr}(b/a^2) &= \mathrm{Tr}\left(\frac{S_3 + S_1^3 + \sigma_2^2/S_1 + \sigma_2 S_1}{x^2 S_1^3} + x + 1\right)\\ &= \mathrm{Tr}\left(\frac{(S_3 + S_1^3)/S_1^3 + k}{x^2} + x + 1\right)\\ &= \mathrm{Tr}\left(\frac{M/S_1^6}{x^3(x+1)} + x^2 + 1 + x + 1\right)\\ &= \mathrm{Tr}\left(\frac{M/S_1^6}{x^3(x+1)}\right)\\ &= 0.\end{aligned}$$

Similarly we obtain

$$\begin{aligned}\mathrm{Tr}\left(\frac{d}{(a + S_1)^2}\right) &= \mathrm{Tr}\left(\frac{\sigma_3 + (a + S_1)\sigma_2 + a(a + S_1)^2}{(a + S_1)^2 S_1}\right)\\ &= \mathrm{Tr}\left(\frac{S_3 + S_1^3 + a\sigma_2 + a(a + S_1)^2}{(a + S_1)^2 S_1}\right).\end{aligned}$$

Note that this is the same formula as for $\mathrm{Tr}(b/a^2)$ with $a + S_1$ replaced by a or equivalently x replaced by $x + 1$. Therefore we have

$$\mathrm{Tr}\left(\frac{d}{(a + S_1)^2}\right) = \mathrm{Tr}\left(\frac{M/S_1^6}{x(x+1)^3}\right) = 0.$$

Then note that $\sigma(X)$ factors into linear factors and

$$\sigma(X) = X^4 + S_1 X^3 + (a(a + S_1) + b + d)X^2 + (ad + (a + S_1)b)X + bd$$

and routine calculations show that

$$\sigma(X) = X^4 + \sigma_1 X^3 + \sigma_2 X^2 + \sigma_3 X + \sigma_4.$$

For each i let T_i be the sum of the ith powers of the roots of $\sigma(X)$ (repeating roots according to their multiplicity in such sums). Then it remains to show that $T_i = S_i$ for $i = 1, 3, 5$. The Newton identities give us

$$\begin{aligned}T_1 &= \sigma_1\\ T_3 &= \sigma_1 T_1^2 + \sigma_2 T_1 + \sigma_3\\ T_5 &= \sigma_1 T_1^4 + \sigma_2 T_3 + \sigma_3 T_1^2 + \sigma_4 T_1\end{aligned}$$

and since $\sigma_1 = S_1$, we have $T_1 = S_1$. Then

$$\begin{aligned}T_3 &= \sigma_1 S_1^2 + \sigma_2 S_1 + \sigma_3\\ &= S_3\end{aligned}$$

by the definitions of σ_1 and σ_3. Further,

$$\begin{aligned}T_5 &= \sigma_1 S_1^4 + \sigma_2 S_3 + \sigma_3 S_1^2 + \sigma_4 S_1\\ &= S_5\end{aligned}$$

by the definitions of σ_1, σ_3 and σ_4. We conclude that the zeros of $\sigma(X)$ obey the syndrome equations in (1). Note that if some of the zeros of $\sigma(X)$ are 0 or equal, it means that the coset has a coset leader of weight less than 4. In any case, the coset D has weight at most 4. □

Proof of Theorem 1: The theorem was shown to be true for $8 \leq m \leq 12$ by a computer search due to van der Horst and Berger [8]. From Remark 1 following Theorem 2 we know that the number of cosets of weight $w = 5$ with $S_1 \neq 0$ is at least $n(n+1)/2$. Further, from Remark 2 following Lemma 1 we know that the number of cosets of weight $w = 5$ with $S_1 = 0$ equals $(5n^2 + 13n)/6$, which implies that $K_5 \geq \frac{4}{3}n(n+2)$.

According to Theorem 3 all cosets with $S_1 \neq 0$ other than those in Theorem 2 have weight at most 4. It follows therefore that $K_5 = \frac{4}{3}n(n+2)$ and therefore, since the total number of cosets is $(n+1)^3$, that $K_4 = \frac{1}{6}n(5n^2 + 10n - 3)$.

III. The Coset Distribution of Extended BCH Codes of Length $n = 2^m$ With Minimum Distance $d = 8$

In this section we determine the coset distribution of the extended codes of the triple-error-correcting BCH codes. Denote by B the extended binary primitive BCH code of length $N = 2^m$ with minimum distance 8. The parity-check matrix H^{ext} of B is defined by

$$H^{\mathrm{ext}} = \begin{bmatrix} 1 & 1 & 1 & 1 & \dots & 1\\ 0 & 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1}\\ 0 & 1 & \alpha^3 & \alpha^6 & \dots & \alpha^{3(n-1)}\\ 0 & 1 & \alpha^5 & \alpha^{10} & \dots & \alpha^{5(n-1)}\end{bmatrix}$$

where α is an element of order $n = 2^m - 1$ in GF(2^m). Note that the syndrome in this case is a 4-tuple (S_0, S_1, S_3, S_5).

Denote by Γ_i the number of cosets of B of weight i. Since B is an extended binary $[N = 2^m, k = N - 3m - 1]$-code with covering radius at most 6, we have immediately that

$$\sum_{i=0}^{6} \Gamma_i = 2N^3 \quad \text{and} \quad \sum_{i=0}^{3} \Gamma_{2i} = \sum_{i=1}^{3} \Gamma_{2i-1}.$$

Using that $\Gamma_0 = 1$ and that clearly $\Gamma_i = \binom{N}{i}$ for $i = 1, 2, 3$, we deduce that

$$\Gamma_4 + \Gamma_6 = N^3 - 1 - \binom{N}{2}$$

and

$$\Gamma_5 = N^3 - \binom{N}{1} - \binom{N}{3} = \frac{1}{6}N(N-1)(5N+8).$$

Hence, to find the complete coset distribution we have to find the number Γ_6 or Γ_4. From the previous sections we know the coset

TABLE I
COSET DISTRIBUTION OF BCH CODES

m	K_0	K_1	K_2	K_3	K_4	K_5
5	1	31	465	4495	13020	14756
6	1	63	1953	39711	160524	59892
7	1	127	8001	333375	1717548	38100

TABLE II
COSET DISTRIBUTION OF EXTENDED BCH CODES

m	Γ_0	Γ_1	Γ_2	Γ_3	Γ_4	Γ_5	Γ_6
5	1	32	496	4960	17515	27776	14756
6	1	64	2016	41664	200235	220416	59892
7	1	128	8128	341376	2050923	1755648	38100

distribution for the code of length $n = 2^m - 1$. Further, we observe that

$$\Gamma_6 = K_5.$$

This can be seen since any coset of weight 6 of the code B of length $N = 2^m$ is reduced to a coset of weight 5 of the corresponding code of length $n = 2^m - 1$, and vice versa, when we do overall parity checking. In other words, more precisely, a coset with syndrome (S_1, S_3, S_5) has weight 5 in the binary triple-error-correcting BCH code of length $n = 2^m - 1$ if and only if $(S_0 = 0, S_1, S_3, S_5)$ is the syndrome of a coset of weight 6 in the extended code. Therefore, $\Gamma_6 = K_5$ and the coset distribution of the extended code follows directly from the coset distribution of the binary primitive triple-error-correcting BCH code and this gives the final result below.

Theorem 4: Let Γ_i denote the number of cosets with a coset leader of weight i in the extended triple-error-correcting binary primitive BCH code of length $N = 2^m$ where $m \geq 8$. Then the distribution of the cosets is given by

$$\begin{aligned}
\Gamma_0 &= 1 \\
\Gamma_1 &= \binom{N}{1} \\
\Gamma_2 &= \binom{N}{2} \\
\Gamma_3 &= \binom{N}{3} \\
\Gamma_4 &= \frac{1}{6}(N-1)(6N^2 - 5N - 2) \\
\Gamma_5 &= \frac{1}{6}N(N-1)(5N+8) \\
\Gamma_6 &= \frac{4}{3}(N-1)(N+1).
\end{aligned}$$

For completeness sake, the number of cosets with a coset leader of weight i in the triple-error-correcting binary primitive BCH code of length $n = 2^m - 1$ and in the extended code are given in the Tables I and II when $m = 5, 6$, and 7.

IV. CONCLUSION

We have determined the distribution of cosets in the binary primitive triple-error-correcting BCH codes of length $n = 2^m - 1$. This solves the conjecture from 1976 by van der Horst and Berger. As an easy consequence this also gives the coset distribution of the extended codes of length $N = 2^m$ and minimum distance $d = 8$.

ACKNOWLEDGMENT

The authors would like to thank the anynomous reviewers for their very detailed and careful comments that considerably improved the presentation of this paper.

REFERENCES

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

[2] E. R. Berlekamp, *Algebraic Coding Theory*. New York: McGraw-Hill, 1968.

[3] ——, "The weight enumerators for certain subcodes of the second-order Reed-Muller codes," *Inf. Contr.*, vol. 17, pp. 485–500, 1970.

[4] ——, "Weight enumeration theorems," in *Proc. Sixth Allerton Conf. Circuit and Systems Theory*, Urbana, IL, 1968, pp. 161–170.

[5] P. Charpin, T. Helleseth, and V. A. Zinoviev, "On cosets of weight 4 of binary BCH codes with minimal distance 8 and exponential sums," *Prob. Inf. Trans.*, vol. 41, no. 4, pp. 301–320, 2005.

[6] P. Charpin and V. A. Zinoviev, "On coset weight distributions of the 3-error-correcting BCH-codes," *SIAM J. Discr. Math.*, vol. 10, no. 1, pp. 128–145, Feb. 1997.

[7] T. Helleseth, "All binary 3-error-correcting BCH codes of length $\mathbf{2^m - 1}$ have covering radius 5," *IEEE Trans. Inf. Theory*, vol. IT-24, pp. 257–258, Mar. 1978.

[8] J. A. van der Horst and T. Berger, "Complete decoding of triple-error-correcting binary BCH codes," *IEEE Trans. Inf. Theory*, vol. IT-22, pp. 138–147, Mar. 1976.

[9] T. Kasami, "Weight distributions of Bose-Chaudhuri-Hocquenghen codes," in *Combinatorial Mathematics and Its Applications*, R. Bose and T. Dowling, Eds. Chapel Hill, NC: University of North Carolina Press, 1969, ch. 20.

[10] F. J. MacWilliams and N. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1996.

[11] C. Moreno and O. Moreno, "Exponential sums and Goppa codes: I," in *Proc. Amer. Math. Soc.*, vol. 111, 1991, pp. 523–531.

On Quasi-Cyclic Interleavers for Parallel Turbo Codes

Joseph J. Boutros, *Member, IEEE* and Gilles Zémor, *Member, IEEE*

***Abstract*—In this correspondence, we present an interleaving scheme that yields quasi-cyclic turbo codes. We prove that randomly chosen members of this family yield with probability almost 1 turbo codes with asymptotically optimum minimum distance, i.e., growing as a logarithm of the interleaver size. These interleavers are also very practical in terms of memory requirements and their decoding error probabilities for small block lengths compare favorably with previous interleaving schemes.**

***Index Terms*—Convolutional codes, iterative decoding, minimum distance, quasi-cyclic codes, turbo codes.**

I. INTRODUCTION

It is now well known that the behavior of turbo codes, although very powerful under high noise, exhibits an error floor phenomenon that can be explained by poor minimum distance properties. More specifically, it can be shown that for randomly chosen interleavers, the expected minimum distance of a classical two-level turbo code remains constant [21], [19], i.e., does not grow with block length. Can the error floor behavior of turbo codes be improved by designing the interleaver in a way that differs from pure random choice?

Manuscript received January 31, 2005; revised December 20, 2005. The material in this correspondence was presented in part at the 2004 IEEE International Symposium on Information Theory, Chicago, IL, June/July 2004.

The authors are with École Nationale Supérieure des Télécommunications, 75634 Paris 13, France (e-mail: boutros@enst.fr; zemor@enst.fr).

Communicated by M. P. Fossorier, Associate Editor for Coding Techniques.
Digital Object Identifier 10.1109/TIT.2006.871061