J. KSIAM **Vol.6**, No.1, 109-119, 2002

THE ORPHAN STRUCTURE OF $BCH(3,m)$ CODE

Geum-sug Hwang

Abstract

If C is a code, an *orphan* is a coset without any parent. We investigate the structure of orphans of the code $BCH(3,m)$. All weight 5 cosets and all weight 3 *reduced* cosets are orphans, and all weight 1,2 and 4 are not orphans. We conjecture that all weight 3 *unreduced* cosets are not orphans. We prove this conjecture for $m = 4,\ 5$.

1. Introduction

An $[n,k]$ code C over F_q is a k-dimensional subspace of the n-tuple space $GF(q^n)$. An $[n,k]$ code C can be specified by k linearly independent vectors in C. A k by n matrix G over F_q whose rows forms a basis of C is called *generator matrix* of C and $C = \{x = uG \mid u = (u_1, u_2, \cdots, u_k),\ u_i \in F_q\}$ $(*1)$. Also C can be specified by $n-k$ linearly independent homogeneous equations. A $n-k$ by n matrix H such that $C = \{(x_1, x_2, \cdots, x_n) \mid Hx^t = 0,\ x_i \in F_q\}$ $(*2)$ is called *parity check matrix* for C. $(*1)$ and $(*2)$ together imply that G and H are related by $GH^t = 0$ and $HG^t = 0$. A *coset* of a code C is the set $a + C = \{a + x \mid x \in C\}$ for any vector a. Each vector b is in some coset and each coset contains q^k vectors. For a vector b, $s = Hb^t$ is the *syndrome* of b where s is a column vector of length $n-k$. Two vectors are in same coset if and only if $Ha^t = Hb^t$. Hence there are one to one correspondence between syndromes and cosets. A minimum weight vector in a coset is called a *coset leader* and the *coset weight* is the weight of a coset leader. The cosets of C are partially ordered by defining for two cosets C' and C'' of C, $C' \le C''$ provided there is a coset leader x' of C' and a coset leader x'' of C'' such that $x' \le x''$. Here for the vectors $x' = (x'_1, x'_2, \cdots, x'_n)$ and $x'' = (x''_1, x''_2, \cdots, x''_n)$, $x' \le x''$ means that $x''_i \ne 0$ whenever $x'_i \ne 0$. The coset C' is a *child* of C'', and C'' is a *parent* of C', provided $C' \le C''$ and there is no coset D with $C' < D < C''$. An *orphan* is a coset without any parent.

Key words and phrases. orphan, reduced coset, unreduced coset.
This research was supported by PUFS under grant PUFS-2000

Let $BCH(t,m)$ denote the binary Bose-Chaudhuri-Hocquenghem code of primitive length $n = 2^m - 1$ and design distance $\delta = 2t+1$. We investigate the orphan structure of the code $BCH(3,m)$ code. The $BCH(3,m)$ code, $m \geq 4$, is the null space of the 3 by n matrix H over $GF(2^m)$ given by

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

where α is a primitive element of $GF(2^m)$. The *syndrome* s of a received word $r = (r_0, r_1, \cdots, r_{n-1})$ is $s = Hr^t = (S_1, S_3, S_5),\ S_j \in GF(2^m)$. The cosets are the set $C(s) = \{r\ :\ Hr^t = s\}$. Given an arbitrary binary n-tuple $a = (a_0, a_1, \cdots, a_{n-1})$ of weight ω, the *locator polynomial* of a is the polynomial of degree ω defined by

$$\sigma(X) = \prod_{\{i: a_i \neq 0\}} (X + \alpha^i) = X^\omega + \sigma_1 X^{\omega-1} + \cdots + \sigma_\omega.$$

The roots of the locator polynomial of a indicate the coordinate positions which are 1 in a. There is a one to one correspondence between binary n-tuples and locator polynomials. A locator polynomial $\sigma(X) = \prod_{i=1}^{\omega}(X + A_i)$ of degree ω is called an *error locator polynomial* with syndrome s provided it is the locator polynomial of a coset leader of a coset $C(s),\ s = (S_1, S_3, S_5)$ of weight ω. This implies that $S_j = \sum_{i=1}^{\omega} A_i^j,\ j = 1,3,5$. We give the relation between the coefficients σ_i of the locator polynomial $\sigma(X)$ and the components S_j of its syndrome, namely $S_1 = \sigma_1,\ S_3 = \sigma_1 S_1^2 + \sigma_2 S_1 + \sigma_3$ and $S_5 = \sigma_1 S_1^4 + \sigma_2 S_3 + \sigma_3 S_1^2 + \sigma_4 S_1 + \sigma_5$.

We define the syndrome (T_1, T_3, T_5) to be *reduced* provided that $T_1 = 0$. A coset with reduced syndorme is called a *reduced coset* and a coset with $T_1 \neq 0$ is called an *unreduced coset*. The *transform* of $C(s),\ s = (S_1, S_3, S_5)$ is the reduced coset $C(t)$ with syndrome $t,\ t = (T_1, T_3, T_5) = (0, S_3 + S_1^3, S_5 + S_1^5)$. Note that two different cosets can have the same transform. Any coset $C(s)$ of weight 1 has syndrome $s = (S_1, S_1^3, S_1^5)$, and so its transform is the code $C(0)$. Hence if $t \neq 0$ then $C(s)$ has weight > 1. The *covering radius* of a code is the largest weight of orphan. The existence of orphans of weight less than covering radius complicates the determination of the covering radius of a code. Let's start with the following characterization of orphan given by R. A. Brualdi and V. S. Pless.

Theorem 1.1 *Let C' be a coset of C with weight ω. Then C' is an orphan if and only if the vectors of C' with weights ω and $\omega + 1$ cover all coordinate positions.*

Proof We first note that each parent of C' is of the form $e_i + C'$ for some unit vector $e_i,\ 1 \leq i \leq n$. If the vectors of weight w and $w+1$ of C' cover all coordinate positions, then the weight of $e_i + C'$ is either $w-1$ or w and hence $e_i + C'$ cannot be a parent of C'. Now suppose that C' is an orphan. If there is a coordinate position j which is not coverd by any vector of weight w or $w+1$ of C', then $e_j + C'$ contains a vector of weight $w+1$ but contains no vectors of weight w, and it follows that $e_j + C'$ is a parent of C'.

Let a coset C' of a code C of distance d have weight ω, $\omega < \lfloor (d-1)/2 \rfloor$. If there are two vectors u, v in C' of weight ω or $\omega+1$, then the vector $u+v$ is a codeword and its weight is less than d, contradicting the distance of C is d. Hence such a coset C' cannot be an orphan by theorem 1.1.

Since the distance of $BCH(3,m)$ is 7, all cosets of weight 1 and 2 are not orphans. Since the maximal coset weight of $BCH(3,m)$ is 5, it is trivial that all cosets of weight 5 are orphans. Hence it remains only to investigate cosets of weight 3 and 4. We note that a coset of weight 3 has a unique coset leader. We now use the notation $\sigma_k(X)$ to denote a locator polynomial of degree k.

Lemma 1.2 *Let $\sigma_{2k-1}(X) = \prod_{i=1}^{2k-1}(X + A_i)$, $k \geq 1$, be the locator polynomial of a vector of a reduced coset $C(t)$. If $L\sigma_{2k-1}(L) \neq 0$ for some $L \in GF(2^m)$, then $(X+L)\sigma_{2k-1}(X+L)$ is a locator polynomial of degree $2k$ with syndrome t. Conversely, if $\sigma_{2k}(X)$ is any even degree locator polynomial with syndrome t and L is one of its roots, then $\sigma_{2k}(X+L)/X$ is a locator polynomial of degree $2k-1$ with syndrome t.*

Proof Since $\sigma_{2k-1}(X)$ is a locator polynomial, its roots A_i, $i = 1, \cdots, 2k-1$ are distinct nonzero elements of $GF(2^m)$. It follows from the condition $L\sigma_{2k-1}(L) \neq 0$ that L and $A_i + L$ are also distinct and nonzero so that $\sigma_{2k}(X) = (X+L)\sigma_{2k-1}(X+L)$ is also locator polynomial. To show that $\sigma_{2k}(X)$ has syndrome t it suffices to show that $L^j + \sum_{i=1}^{2k-1}(A_i + L)^j = \sum_{i=1}^{2k-1} A_i^j$, $j = 1,3,5$. Since $\sum_{i=1}^{2k-1} A_i = 0$, we also have $\sum A_i^2 = 0$ and $\sum A_i^4 = 0$. Hence $L + \sum(A_i + L) = \sum A_i = 0$ and $L^j + \sum(A_i+L)^j = \sum A_i^j$ by expanding $(A_i+L)^j$, $j = 3,5$.

Conversely suppose that L is one of the roots of an even degree locator polynomial $\sigma_{2k}(X)$. Let $A_1, \cdots, A_{2k}$ be the roots of $\sigma_{2k}(X)$ and assume $L = A_1$. Since all A_i, $i = 1, \cdots, 2k$ are nonzero and distinct, $L + A_i = A_1 + A_i$ are also distinct and nonzero. Hence $\sigma_{2k}(X+L)/X$ is a locator polynomial of degree $2k-1$. Since $L^j + \sum_{i=2}^{2k}(A_i)^j = 0$, $j = 1,2,4$

$$\begin{aligned}\sum_{i=2}^{2k}(A_i+L)^j &= \sum(A_i)^j + L(\sum(A_i)^{j-1}) + L^{j-1}(\sum A_i) + L^j \\ &= \sum(A_i)^j + LL^{j-1} + L^{j-1}L \\ &= \sum(A_i)^j,\ j = 1,3,5.\end{aligned}$$

Thus $\sigma_{2k}(X+L)/X$ also has syndrome t.

Henceforth we denote a binary n- tuple A of weight ω with 1's in positions $i_1, i_2, \cdots, i_\omega$ by $A = \{A_1, A_2, \cdots, A_\omega\} = \{\alpha^{i_1}, \alpha^{i_2}, \cdots, \alpha^{i_\omega}\}$.

Corollary 1.3 *Any weight* 4 *vector of weight* 3 *reduced coset* $C(t)$ *has the form* $\{L, A_1 + L, A_2 + L, A_3 + L\}$ *for some* $L \in GF(2^m)$, $L \neq 0$, A_i, $i = 1, 2, 3$ *where* $\{A_1, A_2, A_3\}$ *is the unique coset leader of* $C(t)$.

Proof Let $\sigma_3(X) = \prod_{i=1}^{3}(X + A_i)$ be the error locator polynomial of $C(t)$. For any nonzero $L \in GF(2^m)$, if $L \neq A_i$, $i = 1, 2, 3$ then $L\sigma_3(L) \neq 0$. Hence $(X + L)\sigma_3(X + L)$ is locator polynomial of degree 4 with syndrome t by Lemma 1.2. This implies that $\{L, A_1+L, A_2+L, A_3+L\}$ is a weight 4 vector of $C(t)$. Since the distance of $BCH(3, m)$ is 7, any two distinct locator polynomials of degree 4 with syndrome t have no common root. From the converse part of Lemma 1.2 and uniqueness of the coset leader of $C(t)$, any weight 4 vector of $C(t)$ has this form.

Theorem 1.4 *The weight* $\tilde{\omega}$ *of a reduced coset* $C(t)$ *is either zero or an odd integer* ≥ 3.

Proof Because any coset of weight 1 has syndrome $s = (S_1, S_1^3, S_1^5)$, $S_1 \neq 0$, $\tilde{w}$ cannot be one. Assume that $\tilde{w}$ is positive and even, say $\tilde{w} = 2k$. Let $\sigma_{2k}(X)$ be an error locator polynomial with syndrome t, and let L be a root of $\sigma_{2k}(X)$. Define $\sigma_{2k-1}(X) = \sigma_{2k}(X + L)/X$. Then $\sigma_{2k-1}(X)$ is a locator polynomial with syndrome t by Lemma 1.2, contradicting $\tilde{w}$ is the weight of $C(t)$.

We get the relation between error locator polynomial of coset $C(s)$ and that of its transform $C(t)$ from the next theorem which is in [2]T. Berger and V. A. Van Der Horst. Henceforth we denote a binary n-tuple A of weight ω with 1's in positions $i_1, i_2, \cdots, i_\omega$ by $A = \{A_1, A_2, \cdots, A_\omega\} = \{\alpha^{i_1}, \alpha^{i_2}, \cdots, \alpha^{i_\omega}\}$. Two vectors are *disjoint* provided their locator polynomials have no common roots.

Theorem 1.5 *Let* $C(s)$, $s = (S_1, S_3, S_5)$ *be a coset of weight* $\omega > 1$. *Then an error locator polynomial* $\sigma(X)$ *with syndrome* s *can be obtained from an error locator polynomial* $\tilde{\sigma}(X)$ *of its transform by*

$$\sigma(X) = \begin{cases} \tilde{\sigma}(X), & if\ S_1 = 0 \\ \tilde{\sigma}(X)/(X + S_1), & if\ S_1 \neq 0,\ \omega\ \text{even} \\ \tilde{\sigma}(X + S_1), & if\ S_1 \neq 0,\ \omega\ \text{odd.} \end{cases}$$

Proof If $S_1 = 0$, then $t = s$ and $\sigma(X) = \tilde{\sigma}(X)$, so we need only consider $S_1 \neq 0$.

Case 1 : ω is even. By Theorem 1.4, $\tilde{\omega}$ equals either $\omega - 1$ or $\omega + 1$. Assume that $\tilde{\omega} = \omega - 1$. Then $\tilde{\sigma}(S_1)$ cannot equal zero because that implies $\tilde{\sigma}(X)/(X + S_1)$ is a locator polynomial of degree $\tilde{\omega} - 1 = \omega - 2$ with syndrome s, thereby contracting $C(s)$

has weight w. Thus $\tilde{\sigma}(X+S_1)$ has distinct nonzero roots and is a locator polynomial. Therefore $\tilde{\sigma}(X+S_1)$ has weight $\tilde{w}=w-1$ with syndrome s because we have

$$\begin{aligned}\sum_{i=1}^{\tilde{w}}(A_i+S_1)^j &= \sum(A_i)^j + S_1(\sum(A_i)^{j-1}) + S_1^{j-1}(\sum A_i) + \sum S_1^j \\ &= T_j + S_1^j,\ j=1,3,5\end{aligned}$$

since $(\sum A_i)^{j-1} = \sum A_i = 0$ where $A_i,\ i=1,\cdots,\tilde{w}$ are roots of $\tilde{\sigma}(X)$. This contradicts that $C(s)$ has weight w, so $\tilde{w}=w+1$. It follows that $\sigma(S_1)\neq 0$. Otherwise, $\sigma(X)/(X+S_1)$ is a locator polynomial with syndrome t and degree $w-1$, which would contradict that $C(t)$ has weight $\tilde{w}=w+1$. Since we now know that $\sigma(S_1)\neq 0$ and $\tilde{w}=w+1,\ \tilde{\sigma}(X)=(X+S_1)\sigma(X)$ is an locator polynomial with syndrome t, or $\sigma(X)=\tilde{\sigma}(X)/(X+S_1)$.

Case 2 : w is odd. By Theorem 1.4, $\tilde{w}=w$ and $\tilde{\sigma}(X+S_1)$ is a locator polynomial with syndrome s and the degree $\tilde{w}$ of $\tilde{\sigma}(X+S_1)$ equals w. Thus $\tilde{\sigma}(X+S_1)$ is an error locator polynomial with syndrome s.

Corollary 1.6 *No orphan has weight 4.*

Proof Let $\sigma(X)$ be an error locator polynomial of weight 4 coset $C(s)$ with coset leader $\{A_1,A_2,A_3,A_4\}$ with syndrome $s=(S_1,S_3,S_5),\ S_1\neq 0$. By Theorem 1.5, an error locator polynomial $\tilde{\sigma}(X)$ of the transform $C(t)$ of $C(s)$ is $\tilde{\sigma}(X)=\sigma(X)(X+S_1)$. This means that $\{S_1,A_1,A_2,A_3,A_4\}$ is a coset leader of $C(t)$, and $C(t)$ is a parent of $C(s)$. Thus a coset of weight 4 is not orphan.

Theorem 1.7 *All reduced cosets of weight* 3 *are orphans. Furthermore, such cosets have exactly* $(n-3)/4$ *weight* 4 *vectors.*

Proof Let $C(t)$ be a reduced coset of weight 3 with coset leader $A=\{A_1,A_2,A_3\}$. For any nonzero $L\in GF(2^m),\ L\neq A_i,\ i=1,2,3,\ \bar{L}=\{L,L+A_1,L+A_2,L+A_3\}$ is a weight 4 vector in $C(t)$. Since distance is 7, A and $\bar{L}$ are disjoint. Hence A and weight 4 vectors of $C(t)$ cover all coordinate positions. Therefor, any two distinct weight 4 vectors are also disjoint, so there are exactly $(n-3)/4$ weight 4 vectors of $C(t)$.

We define the trace mapping from $GF(2^m)$ to $GF(2)$ by

$$Tr(A) = A + A^2 + \cdots + A^{2m-1},\ A\in GF(2^m).$$

The following lemma shows the properties of trace mappings which can be found in [8]F. J. MacWilliams and N. J. A. Solane.

Lemma 1.8 *The followings hold:*

(i) Exactly half of the elements A in $GF(2^m)$ have $Tr(A) = 0$ and exactly half have $Tr(A) = 1$.
(ii) $Tr(A + B) = Tr(A) + Tr(B),\ A, B \in GF(2^m)$.
(iii) $Tr(A^{2^i}) = Tr(A),\ i = 1, \cdots, m - 1$.

We next obtain sufficient conditions for a weight 3 coset not to be an orphan by using the trace mapping. [4]E. R. Berlekamp, H. Rumssey and G. Solomon characterized quadratic equations over fields of characteristic two which have roots and we record their result in the next lemma.

Lemma 1.9 *The quadratic equation, $X^2 + AX + B = 0,\ A, B \in GF(2^m),\ A \neq 0$, has solutions in $GF(2^m)$ if and only if $Tr(B/A^2) = 0$.*

Lemma 1.10 *Any reduced coset with syndrome $(0, 0, T_5),\ T_5 \neq 0$ has weight 5.*

Proof Let $C(t)$ has syndrome $t,\ t = (0, 0, T_5)$. Since $T_1 = 0$, $C(t)$ has weight 3 or 5 by Theorem 1.4. Assume that $C(t)$ has weight 3 and let $\tilde{\sigma}(X) = X^3 + \sigma_1 X^2 + \sigma_2 X + \sigma_3$ be the error locator polynomial of $C(t)$. we have $\sigma_1 = T_1 = 0$ and $\sigma_3 = T_3 = 0$. Then $\tilde{\sigma}(X)$ has zero as its root which contradicts that $\tilde{\sigma}(X)$ is a locator polynomial. Hence $C(t)$ has weight 5.

Lemma 1.11 *Assume m is odd. Any reduced coset $C(t)$ with syndrome $t = (0, T_3, 0),\ T_3 \neq 0$ has weight 5.*

Proof Since $T_1 = 0$, C(t) has weight 3 or 5 by Theorem 1.4. Assume that $C(t)$ has weight 3 with coset leader $\{A_1, A_2, A_3\}$. Since $A_1 + A_2 + A_3 = 0,\ 0 = T_5 = T_3(A_1A_2 + A_2A_3 + A_1A_3) = T_3(A_1^2 + A_2^2 + A_1A_2)$. Since $T_3 \neq 0,\ A_1^2A_2^2 + A_1A_2 = 0$ and so A_2 is a root of $X^2 + A_1X + A_1^2 = 0$. By Lemma 1.8, $Tr(A_1^2/A_2^2) = Tr(1) = 0$, contradicting to that m is odd. Hence $C(t)$ has weight 5.

2. Main Theorems

Theorem 2.1 *Let $C(t),\ t = (0, T_3, T_5)$ be a reduced coset of weight 3 and $C(s),\ s = (S_1, S_3, S_5)$ be a unreduced coset whose transform is $C(t)$. If $Tr(T_3/S_1^3) = 0$, then $C(s)$ is not an orphan.*

Proof Let $A = \{A_1, A_2, A_3\}$ be the coset leader of $C(s)$. Then $\{A_1 + S_1, A_2 + A_1, A_3 + S_1\}$ is the coset leader of $C(t)$ by Theorem 1.5. Note that $C(s)$ is not an orphan if and only if there exists a nonzero $L \in GF(2^m)$ such that $A' = \{A_1, A_2, A_3, L\}$ is a coset leader of weight 4 coset. Since, by Lemma 1.9 $Tr(T_3/S_1^3) = 0$ if and only if $X^2 + S_1X + T_3/S_1 = 0$ has a solution, there exists a $L \in GF(2^m)$ such that $LS_1(L + S_1) + T_3 = 0$. If $L = 0$ then $T_3 = 0$, and so $C(t)$ has weight 5 by Lemma 1.10. Hence $L \neq 0$. We now show that $L \neq A_i,\ i = 1, 2, 3$. Assume that $L = A_1$. Then $A_1S_1(A_1 + S_1) = T_3 = (A_1 + S_1)^3 + (A_2 + S_1)^3 + (A_3 + S_1)^3 = (A_1 + S_1)(A_2 + S_1)(A_3 + S_1) = (A_1S_1 + A_1A_2)(A_1 + S_1)$ implies $A_2A_3 = 0$, contradicting A has weight 3. Thus $A' = \{A_1, A_2, A_3, L\}$ is a weight 4 vector of some coset $C(s')$, where $s' = (S_1 + L, S_3 + L^3, S_5 + L^5)$. Then the transform $C(t')$ of $C(s')$, has syndrome $(0, T_3 + LS_1(L + S_1), T_5 + LS_1(L^3 + S_1^3))$. Since $T_3 + LS_1(L + S_1) = 0$, the coset weight of $C(t'),\ t' = (0, 0, T_5 + LS_1(L^3 + S_1^3))$ is 5 by Lemma 1.10. Hence $C(s')$ has weight 4 by Theorem 1.5. Thus the weight 4 vector A' is a coset leader of $C(s')$, and hence $C(s')$ is a parent of $C(s)$. Therefore $C(s)$ is not an orphan.

Theorem 2.2 *Assume m is odd. Let $C(t),\ t = (0, T_3, T_5)$ be a reduced coset of weight 3. There exists $(n - 7)/2$ weight 3 unreduced cosets whose transform is $C(t)$, and they are not orphans. Furthermore, there are at least $n(n - 1)(n - 7)/12$ weight 3 cosets which are not orphans.*

Proof Let $A = \{A_1, A_2, A_3\}$ be the coset leader of $C(t)$. By Theorem 1.5 and the uniqueness of the coset leader of $C(t)$, for any nonzero $L \in GF(2^m)$ with $L \neq A_i$, the coset $C(l), l = (L, T_3 + L^3, T_5 + L^5)$ has weight 3 with coset leader $\{A_1 + L, A_2 + L, A_3 + L\}$ and $C(t)$ is a transform of $C(l)$. Hence we want to count L such that $Tr(T_3/L^3) = 0$, $L \neq 0, A_1, A_2, A_3$. Since m is odd, $n = 2^m - 1$ is not divisible by 3. This means α^3 is a primitive element whenever α is a primitive element of $GF(2^m)$. Thus, for the given T_3, $\{T_3/L^3 \mid L \in GF(2^m),\ L \neq 0\}$ is the set of all nonzero elements of $GF(2^m)$. By (i) in Lemma 1.8, there are exactly $(n - 1)/2$ nonzero L such that $Tr(T_3/L^3) = 0$. But,

$$\begin{aligned} Tr(T_3/L^3) &= Tr((A_1^3 + A_2^3 + A_3^3)/A_1^3) = Tr(A_1A_2A_3/A_1^3) \\ &= Tr((A_3^2 + A_1A_3)/A_1^2) = Tr((A_3/A_1)^2 + Tr(A_3/A_1) \\ &= Tr(A_3/A_1) + Tr(A_3/A_1) = 0, \end{aligned}$$

using $A_1 + A_2 + A_3 = 0$ and (ii), (iii) in Lemma 1.8. We conclude that if $L = A_i,\ i = 1, 2, 3$ then $Tr(T_3/L^3) = 0$, but coset $C(l)$, $l = (L, T_3 + L^3, T_5 + L^5)$ does not have weight 3. Therefore there are $(n + 1)/2 - 4 = (n - 7)/2$ weitght 3 unreduced cosets whose transform is $C(t)$ and they are not orphans by Theorem 2.1. We now count the number of weight 3 reduced cosets with syndrome $(0, T_3, *)$ for some fixed $T_3 \in GF(2^m)$ and arbitrary $* \in GF(2^m)$. This is equivalent to counting the number of coset leaders of these cosets since each coset has only one coset leader. Let $C(t)$ be a weight 3 reduced coset with syndrome $(0, T_3, *)$ and let $\{A_1, A_2, A_3\}$ be the coset leader of $C(t)$. Then, by Lemma 1.9, $T_3 = A_1^3 + A_2^3 + A_3^3 = A_1^3 + A_2^3 + (A_1 + A_2)^3 = A_1A_2(A_1 + A_2)$ (or $A_2A_3(A_2 + A_3)$). Therefore

$$\begin{gathered} \{A_1, A_2, A_3\} \text{ is the coset leader of a coset } C(t),\ t = (0, T_3, *) \\ \text{if and only if } A_i \text{ is a root of } X^2 + A_jX + T_3/A_j = 0,\ i \neq j\ i, j = 1, 2, 3 \\ \text{if and only if } Tr(T_3/A_1^3) = Tr(T_3/A_2^3) = Tr(T_3/A_3^3) = 0. \end{gathered}$$

We have already noted that there are $(n - 1)/2$ nonzero $L \in GF(2^m)$ such that $Tr(T_3/L^3) = 0$, so there are $1/3((n - 1)/2)$ weight 3 reduced cosets with syndrome

$(0, T_3, *)$ for each nonzero $T_3 \in GF(2^m)$. Therefore we have at least $n(1/3((n-1)/2)((n-7)/2) = n(n-1)(n-7)/12$ weight 3 unreduced cosets which are not orphans.

Theorem 2.3 *Assume m is an even. There are at least $n\beta(\beta-1) + (n/8)(n-2\beta)(n-2\beta-5)$ weight 3 unreduced cosets which are not orphans where β is the number of nonzero elements $\alpha^j \in GF(2^m)$ such that the trace of α^j is zero and $j \equiv 0\ (mod\ 3)$.*

Proof Let $C(t)$, $t = (0, T_3, T_5)$ be a weight 3 reduced coset with coset leader $A = \{A_1, A_2, A_3\}$. Since m is even, $n = 2^m - 1$ is divisible by 3. So $\{\ T_3/L^3 \mid L \in GF(2^m),\ L \neq 0\}$ is not the set of all nonzero elements of $GF(2^m)$. To count the number of nonzero L such that $Tr(T_3/L^3) = 0$, define β to be the cardinality of Ψ where $\Psi = \{\alpha^j \in GF(2^m) \mid \alpha^j \neq 0,\ Tr(\alpha^j) = 0,\ j \equiv 0\ (mod\ 3)\}$. Let $T_3 = \alpha^j$ for some j. We separate the remainder of the proof into two cases according to whether j is divisible by 3 or not.

Case 1 : Let $T_3 = \alpha^3 k$, for some k. Then if $T_3/L^3 = R$ for some $R \in \Psi$, then $T_3/(L\alpha^{n/3})^3 = T_3/(L\alpha^{2n/3})^3 = R$ and $L \in GF(2^m)$. Hence, by the same argument in Theorem 2.2, there exist 3β nonzero L such that $Tr(T_3/L^3) = 0$, and we have $3\beta - 3$ weight 3 unreduced cosets whose transform is $C(t)$ and by Theorem 2.1 they are not orphans. Also we have β weight 3 reduced cosets with syndrome $(0, T_3, *)$ for some fixed $T_3 \in GF(2^m)$, and there are $n/3$ nonzero elements of $GF(2^m)$, $T_3 = \alpha^{3k}$ for some k. This means that there are at least $(n/3)(\beta)(3\beta - 3) = n\beta(\beta - 1)$ weight 3 cosets which are not orphans.

Case 2 : Let $T_3 = \alpha^k,\ k = 1, 2\ (mod\ 3)$. Exactly half of the elements in $GF(2^m)$ have trace zero, so we have $(n-1)/2 - \beta = 1/2(n - 1 - 2\beta)$ nonzero $R = \alpha^j$ such that $Tr(R) = 0,\ j$ is not divisible by 3. Note if $j \equiv 1\ (mod\ 3)$, then $2j \equiv 2\ (mod\ 3)$. Thus, there are $(n-1-2\beta)/4R$ such that $Tr(R) = 0,\ j \equiv 1$ or $2\ (mod\ 3)$ respectively. Since there exists $L \in GF(2^m)$ such that $T_3/L^3 = R \in \Psi$ if and only if $k \equiv j\ (mod\ 3)$, there are weight 3 unreduced cosets whose transform is $C(t)$ and $((n-1-2\beta)/4) - 3$ weight 3 reduced cosets with syndrome $(0, T_3, *)$ for some fixed nonzero $T_3 \in GF(2^m)$. Therefore we have at least $2[(n/3)((n-1-2\beta)/4)((3(n-1-2\beta)-12)/4)] = (n/8)(n-1-2\beta)(n-5-2\beta)$ weight 3 unreduced cosets which are not orphans.

From Case 1 and Case 2, there are at least $n\beta(\beta-1) + (n/8)(n-2\beta-1)(n-2\beta-5)$ weight 3 unreduced cosets which are not orphans.

Theorem 2.4 *Assume that m is odd. Let $C(t),\ t = (0, T_3, T_5)$ be a reduced coset of weight 3 and $C(s),\ s = (S_1, S_3, S_5)$ be an unreduced coset whose transform is $C(t)$. If $Tr(T_5/S_1^5) = 0$, then C(s) is not an orphan.*

Proof Let $\{A_1, A_2, A_3\}$ be the coset leader of $C(t)$. Then $\{A_1+S_1, A_2+S_1, A_3+S_1\}$ is the coset leader of $C(s)$. Since $Tr(T_5/S_1^5) = 0$, by Lemma 1.9, $X^2 + S_1^2 X + T_5/S_1 = 0$ has roots $P,\ Q \in GF(2^m)$ such that $P + Q = S_1^2$ and $PQ = T_5/S_1$. Therefore $X^4 + S_1^3 X + T_5/S_1 = (X^2 + S_1 X + P)(X^2 + S_1 X + Q)$ $(*3)$ for $P,\ Q \in GF(2^m)$. Since

$P+Q+=S_1^2$, $Tr(P/S_1^2)+Tr(Q/S_1^2)=Tr(1)=1$. Thus only one of $Tr(P/S_1^2)$ and $Tr(Q/S_1^2)$, say $Tr(P/S_1^2)$, equals to zero. By Lemma 1.9, there exists $L \in GF(2^m)$ such that L is a root of $X^2+S_1X+P=0$. From (*3), L is a root of $X^4+S_1^3X+T_5/S_1=0$, and so $S_1L^4+S_1^4L=S_1^5+L^5+(S_1+L)^5=T_5$. Hence $\{S_1,L,S_1+L\}$ is coset leader of weight 3 reduced coset $C(p)$ with syndrome $(0,P,T_5)$ where $P=S_1L(S_1+L)$. By Lemma 1.10, a coset $C(p')=C(t)+C(p)$ with syndrome $(0,T_3+P,0)$ has weight 5. Now $\bar{A}=\{A_1,A_2,A_3,S_1,L,S_1+L\}$ is a vector of $C(p')$ has a vector of weight less than 5, contradicting to that $C(p')$ has weight 5. This $\bar{A}$ is a vector in $C(p')$ of weight 6. Thus $\{A_1+S_1,A_2+S_1,A_3+S_1,L,L+S_1\}$ is a weight 5 vector in $C(p')$ and is a coset leader. Since any descendent of coset leader is also coset leader of some coset, $\{A_1+S_1,A_2+S_1,A_3+S_1,L\}$ is a coset leader of some coset which is a parent of $C(s)$. Therefore $C(s)$ is not an orphan.

We have shown that many weight 3 unreduced cosets are not orphans. We conjecture that all weight 3 unreduced cosets are not orphans. We prove that this conjecture for $m=4$ and 5.

Lemma 2.5 *Let $C(s)$, $s=(S_1,S_3,S_5)$ be a weight 3 unreduced coset. For each weight 4 vector $A=\{A_1,A_2,A_3,A_4\}$ of $C(s)$ with $A_i \neq S_1$, $i=1,\cdots,4$, we have $\bar{A}=\{A_1+S_1,A_2+S_1,A_3+S_1,A_4+S_1\}$ is also a weight 4 vector of $C(s)$.*

Proof Since the A_i are distinct nonzero elements different from S_1, the elements A_i+S_1 are nonzero and distinct. We calculate $\sum_{i=1}^4(A_i+S_1)^j=\sum_{i=1}^4 A_i^j+S_1(\sum(A_i)^{j-1})+S_1^{j-1}(\sum A_i)+\sum S_1^j=\sum A_i^j$, since $\sum A_i^{j-1}=S_1^{j-1}$, $j=1,3,5$.

Corollary 2.6 *Any weight 4 coset $C(s)$ has at least two coset leaders.*

Lemma 2.7 *A locator polynomial of a weight 4 vector of the weight 3 unreduced coset $C(s)$ and a locator polynomial of weight 4 vector of the transform $C(t)$ of $C(s)$ have at most one common root.*

Proof Let $Q=\{Q_1,Q_2,Q_3,Q_4\}$ and $P=\{P_1,P_2,P_3,P_4\}$ be weight 4 vectors in $C(s)$ and $C(t)$ respectively. Without loss of generality, assume that $Q_1=P_1$ and $Q_2=P_2$. We claim that $\{Q_3,Q_4,P_3,P_4\} \in C(s')$, $s'=(S_1,S_1^3,S_1^5)$, a coset of weight 1. This follows since $Q_3^j+Q_4^j=S_j+Q_1^j+Q_2^j=S_j+P_1^j+P_2^j=S_j+T_j+P_3^j+P_4^j=S_1^j+P_3^j+P_4^j$, $j=1,3,5$. Therefore $\{S_1,Q_3,Q_4,P_3P_4\}$ is a codeword, contradicting the fact that the minimum distance of $BCH(3,m)$ is 7.

Lemma 2.8 *Suppose that the locator polynomial $\sigma(X)$ of weight 4 vector of weight 3 unreduced coset $C(s)$ has one common root with the locator polynomial $\tilde{\sigma}(X)$ of weight 4 vector of its transform $C(t)$. If S_1 is neither a root of $\sigma(X)$ nor $\tilde{\sigma}(X)$, then $\tilde{\sigma}(X)$ cannot have a common root with $\sigma(X+S_1)$, where $\sigma(X+S_1)$ is also a locator polynomial of weight 4 vector of $C(s)$.*

Proof Let $A = \{A_1, A_2, A_3\}$ be a coset leader of $C(t)$, and let $P = \{P_1, P_2, P_3, P_4\}$ and $Q = \{Q_1, Q_2, Q_3, Q_4\}$ be weight 4 vectors of $C(t)$ abd $C(s)$ respectively. Suppose that the locator polynomial $\tilde{\sigma}(X)$ of P has one common root with the locator polynomial $\sigma(X)$ of Q, say $P_1 = Q_1$. We can say that P is of the form $P_{i+1} = P_1 + A_i,\ i = 1, 2, 3$ since $\{P_1, P_1 + A_1, P_1 + A_2, P_3 + A_3\}$ is a weight 4 vector of $C(t)$ and any two distinct weight 4 vectors are disjoint. By Lemma 2.5 and $Q_i \neq 0,\ \bar{Q} = \{Q_1 + S_1, Q_2 + S_1, Q_3 + S_1, Q_4 + S_1\}$ is a weight 4 vector of $C(s)$ and $\sigma(X + S_1)$ is the locator polynomial of $\bar{Q}$. So suppose that P and $\bar{Q}$ have a common nonzero position. If $P_1 = Q_i + S_1$ for some i, then $Q_1 + Q_i = S_1$, since $P_1 = Q_1$. This contradicts the fact that the weight of Q is 4. Without loss of generality, assume that $P_2 = Q_2 + S_1$. Then $Q_2 + S_1 = P_2 = P_1 + A_1 = Q_1 + A_1,\ Q_1 + Q_2 + S_1 = Q_3 + Q_4 = A_1$. So we have $Q_3 = Q_4 + A_1$. Hence $\{Q_4, Q_4 + A_1, Q_4 + A_2, Q_4 + A_3\} = \{Q_4, Q_3, Q_4 + A_2, Q_4 + A_3\}$ is weight 4 vector in $C(t)$ which has two common nonzero positions with Q, contradicting Lemma 2.7. Hence P cannot have a common nonzero position with Q.

Theorem 2.9 *No weight* 3 *unreduced coset is an orphan for* $m = 4$ *and* 5.

Proof Let $C(s)$ be weight 3 coset and let $C(t)$ be its transform with coset leader $A = \{A_1, A_2, A_3\}$. Then $\{S_1, A_1, A_2, A_3\}$ is a weight 4 vector of $C(s)$ since $S_1 \neq 0,\ A_i$. We claim that this is the only weight 4 vector of $C(s)$. To get a contradiction, assume that $Q = \{Q_1, Q_2, Q_3, Q_4\},\ Q_i \neq S_1,\ A_j\ i = 1, \cdots, 4;\ j = 1, 2, 3$ is another weight 4 vector of $C(s)$. Then $\bar{Q} = \{Q_1 + S_1, Q_2 + S_1, Q_3 + S_1, Q_4 + S_1\}$ is also weight 4 vector of $C(s)$ by Lemma 2.5. Define $P(i) = \{Q_i, Q_i + A_1, Q_i + A_2, Q_i + A_3\}$ and $\bar{P}(i) = \{Q_i + S_1, Q_i + S_1 + A_1, Q_i + S_1 + A_2, Q_i + S_1 + A_3\}$ for $i = 1, \cdots, 4$. Then $P(i)$ and $\bar{P}(i)$ are weight 4 vectors of $C(t)$. It is sufficient to show that these 8 weight 4 vectors are distinct since $C(t)$ has only $(n-3)/4 < 8,\ (m = 4, 5)$ weight 4 vectors by Theorem 1.7. If $P(i) = P(j),\ i \neq j$ then we have $Q_i = Q_j + A_k$ for some k, so the locator polynomial of $P(j)$ has two common roots with locator polynomial of Q, contradicting Lemma 2.7. Thus we have $P(i) \neq P(j)$, and $\bar{P}(i) \neq \bar{P}(j)$ for $i \neq j$. If $P(i) = \bar{P}(i)$ then $A_i = S_1$, contradicting $C(s)$ has weight 3. Now assume that $P(i) = \bar{P}(j),\ i \neq j$, say $i = 1,\ j = 2$. Then $Q_1 = Q_2 + S_1 + A_k$ for some k. This implies $Q_3 = Q_4 + A_k$, so the locator polynomial of $P(4)$ has two common roots with Q contradicting Lemma 2.7. Thus all these weight 4 vectors are distinct, contradicting Theorem 1.7. Hence $C(s)$ has only one weight 4 vector and so is not an orphan by Theorem 1.1.

REFERENCES

[1] E. F. Assmus, Jr. and H. F. Mattson, Jr.[1976], Some three-error correcting BCH codes haxe covering radius 5,IEEE Trans. Inform. Theory, vol IT-22, 348-349.

[2] T. Berger and J. A. Van der Horst1976], Complete decoding of triple-error correcting binary BCH codes. IEEE Trans. Inform. Theory, vol IT-22, 138-147.

[3] E. R. Berkamp1968], Algebrac coding Theory, McGraw-Hill, New York.
[4] E. R. Berkamp, H. Rumsy and G. Solomon1967], On the solution of algebrac equations over finite fields, information and Control, 10, 553-564.
[5] T. Helleseth[1973], All binary 3-error correcting BCH codes oh length - 1 have coverimg radius 5, IEEE Trans. Inform. Theory, vol It-19, 344-356.
[6] T. Helleseth[1985], On the covering radius of cyclic linear codes and arithmetic codes, Discrete Appl. Math., 11, 157-173.
[7] F. J. MacWilliams and N. j. A. sloane[1977], The theory of Error-Correcting Codes, New York: North Holland.
[8] A. Tieta"va"inen[1987], On the covering radius of long binary BCH codes. Discrete Appl. Math., 16, 75-77.

Division of Information and Management Science,
College of Information and Science,
Pusan University of Foreign Studies,
55-1, Uam-Dong, Nam-Gu, Busan

email: gshwang@ taejo.pufs.ac.kr
Classification number C020705