LETTER

Local Weight Distribution of the (256, 93) Third-Order Binary Reed-Muller Code

Kenji YASUNAGA[†a)], **Toru FUJIWARA**[†b)], ***Members, and*** **Tadao KASAMI**[††], ***Fellow, Honorary Member***

SUMMARY Local weight distribution is the weight distribution of minimal codewords in a linear code. We give the local weight distribution of the $(256, 93)$ third-order binary Reed-Muller code. For the computation, a coset partitioning algorithm is modified by using a binary shift invariance property. This reduces the time complexity by about 1/256 for the code. A necessary and sufficient condition for minimality in Reed-Muller codes is also presented.

key words: *local weight distribution, minimal codeword, Reed-Muller code, binary shift*

1. Introduction

The studies of minimal codewords in a linear code are crucial for the performance analysis of the code under maximum-likelihood (ML) decoding. The weight distribution of minimal codewords, called *local weight distribution*, is also important for ML decoding performance analysis of the code. For example, the local weight distribution gives a tighter upper bound on error probability for soft decision decoding over AWGN channel than the usual union bound [6]. The Séguin lower bound can be improved by using local weight distributions for several codes [13]. The number of minimal codewords in codes determines the complexity of gradient-like decoding of the code [9].

The local weight distributions have been determined for some codes [2], [3], [11], [14]. The local weight distributions of the first-order and second-order binary Reed-Muller codes are completely determined [2]. In [14], the *coset partitioning algorithm* for computing the local weight distributions was proposed and applied to some extended primitive BCH codes and the $(128, 64)$ third-order binary Reed-Muller codes. The local weight distribution of the $(256, 93)$ third-order binary Reed-Muller code was not computed in [14] due to its large complexity but a clue was presented. In this letter, we consider use *binary shifts* to reduce the complexity of the coset partitioning algorithm for Reed-Muller codes following the way presented in [14], and compute the distribution of the $(256, 93)$ third-order Reed-Muller code. The complexity is reduced to 1/256 for this code by this modification. We also give a necessary and sufficient condition for minimality of codewords in terms of Boolean polynomial for codes of length power of two, including binary Reed-Muller codes. This condition is a generalization of the fact that is used in the method in [4] and has not been stated explicitly. One may be able to use it for studying minimal codewords in Reed-Muller codes or codes whose length is a power of two.

2. Review of Coset Partitioning Algorithm

Let C be an (n, k) linear code over the finite field $\mathbf{F}_q$. A support set of a vector $\boldsymbol{v}$, which is the set of indices of nonzero elements in $\boldsymbol{v}$, is defined as $\mathrm{Supp}(\boldsymbol{v}) = \{i : v_i \neq 0\}$. If $\mathrm{Supp}(\boldsymbol{v}) \subset \mathrm{Supp}(\boldsymbol{v}')$ (respectively, $\subseteq$), we write $\boldsymbol{v} \prec \boldsymbol{v}'$ (respectively, $\preceq$). A codeword $\boldsymbol{v} (\neq \mathbf{0})$ is called *minimal* in C if $\boldsymbol{v}' \preceq \boldsymbol{v}$ implies $\boldsymbol{v}' = c\boldsymbol{v}$, where $\boldsymbol{v}' \in C \setminus \{\mathbf{0}, \boldsymbol{v}\}$ and c is a nonzero constant in $\mathbf{F}_q$. In some papers, a minimal codeword is called a *zero neighbor* [1], [14]. Henceforth we only consider the case $q = 2$, i.e. C is a binary code. The local weight distribution of C is defined as the $(n + 1)$-tuple $(L_0(C), L_1(C), \ldots, L_n(C))$, where $L_w(C)$ is the number of minimal codewords with weight w in C.

We review a coset partitioning algorithm for computing local weight distribution proposed in [14]. This algorithm works effectively for codes which have large automorphism group. For a detail description of time/space complexity and effectiveness of this algorithm, see [14].

For a permutation π and a set of vectors D, let $\pi[D] = \{\pi\boldsymbol{v} : \boldsymbol{v} \in D\}$. The automorphism group of a code C is the set of all permutations by which C is permuted into C, and denoted by $\mathrm{Aut}(C)$, i.e., $\mathrm{Aut}(C) = \{\pi : \pi[C] = C\}$. Minimality of codewords is invariant under the automorphism group of the code. Let $\pi \in \mathrm{Aut}(C)$ and $\boldsymbol{v} \in C$. If $\boldsymbol{v}$ is a minimal codeword, then $\pi\boldsymbol{v}$ is also a minimal codeword [14].

For a binary (n, k) linear code C and its linear subcode with dimension k', let C/C' denote the set of cosets of C' in C, that is, $C/C' = \{\boldsymbol{v} + C' : \boldsymbol{v} \in C\}$. For a coset $\boldsymbol{v} + C' \in C/C'$, the codeword $\boldsymbol{v}$ is called a *representative* codeword of the coset. Let $Z_w(D)$ be the set of minimal codewords of C in a coset D with weight w. We call the $(n + 1)$-tuple $(|Z_0(D)|, |Z_1(D)|, \ldots, |Z_n(D)|)$ for a coset D the *local weight subdistribution* for D. Then the local weight distribution of C is given as the sum of the local weight subdistributions for the cosets in C/C';

$$L_w(C) = \sum_{D \in C/C'} |Z_w(D)|.$$

Manuscript received October 30, 2006.
Final manuscript received December 11, 2006.

[†] The authors are with Graduate School of Information Science and Technology, Osaka University, Suita-shi, 565-0871 Japan.

[††] The author is with Nara Institute of Science and Technology, Ikoma-shi, 630-0192 Japan.

a) E-mail: k-yasunaga@ist.osaka-u.ac.jp
b) E-mail: fujiwara@ist.osaka-u.ac.jp

DOI: 10.1093/ietfec/e90–a.3.698

Cosets in C/C' are closed under $\mathrm{Aut}(C) \cap \mathrm{Aut}(C')$. For any $\pi \in \mathrm{Aut}(C) \cap \mathrm{Aut}(C')$ and $D \in C/C'$, $\pi[D] \in C/C'$ [14]. We call $D_1, D_2 \in C/C'$ are equivalent if there exists $\pi \in \mathrm{Aut}(C) \cap \mathrm{Aut}(C')$ such that $\pi[D_1] = D_2$. If we partition the set of cosets C/C' into equivalence classes and know the number of equivalent cosets for each class, the local weight distribution of C is determined by the local weight subdistributions for representative cosets;

$$L_w(C) = \sum_{D \in RC_\Pi(C/C')} e_\Pi(D) \cdot |Z_w(D)|, \qquad (1)$$

where $RC_\Pi(C/C')$ is the set of representative cosets obtained by partitioning C/C' into equivalence classes with the set of permutations $\Pi \subseteq \mathrm{Aut}(C) \cap \mathrm{Aut}(C')$, and $e_\Pi(D)$ is the number of equivalent cosets to D when using Π for partitioning cosets.

Based on the above definitions and properties, the coset partitioning algorithm is formulated as follows:

Coset partitioning algorithm for computing LWD [14]:

1) Choose a subcode C' for which $RC_\Pi(C/C')$ and $e_\Pi(D)$ for $D \in RC_\Pi(C/C')$ are known, or easily computable.
2) Compute the local weight subdistributions for $D \in RC_\Pi(C/C')$.
3) Compute the local weight distribution of C from (1).

The coset partitioning algorithm can be applied to computing the local weight subdistributions for cosets. For a coset $\boldsymbol{v} + C'$ and a linear subcode C'' of C', $\boldsymbol{v} + C'$ can be seen as the set of cosets $(\boldsymbol{v} + C')/C''$. If one partition $(\boldsymbol{v} + C')/C''$ into equivalence classes, the time complexity for computing the local weight subdistribution for $\boldsymbol{v} + C'$ will be reduced. To do this, we should find a subset of $\{\rho : \rho\boldsymbol{v} \in \boldsymbol{v} + C',\ \rho \in \mathrm{Aut}(C) \cap \mathrm{Aut}(C') \cap \mathrm{Aut}(C'')\}$ because of the following theorem.

Theorem 1 ([14]). *For $E_1, E_2 \in (\boldsymbol{v} + C')/C''$, the local weight subdistribution for E_1 and that for E_2 are the same if there exists $\pi \in \{\rho : \rho\boldsymbol{v} \in \boldsymbol{v} + C', \rho \in \mathrm{Aut}(C) \cap \mathrm{Aut}(C')\}$ such that $\pi[E_1] = E_2$.*

If one considers use the coset partitioning algorithm for computing the local weight distribution of C and the local weight subdistributions for its representative cosets $\boldsymbol{v}_i + C'(1 \le i \le |RC_\Pi(C/C')|)$, then there needs a subset of $\{\rho : \rho\boldsymbol{v} \in \boldsymbol{v}_i + C',\ \rho \in \mathrm{Aut}(C) \cap \mathrm{Aut}(C') \cap \mathrm{Aut}(C'')\}$ for every i.

3. A Necessary and Sufficient Condition for Minimality in Reed-Muller Codes

We give a necessary and sufficient condition for minimality of codewords in terms of Boolean polynomial for codes of length 2^m, including binary Reed-Muller codes. This condition is a generalization of the fact that is used in Theorem 7 in [4].

Any binary vector of length 2^m can be expressed in terms of Boolean polynomial of m variables. Let P_m be the set of Boolean polynomials with m variables $x_1, x_2, \ldots, x_m$. For a nonnegative integer i less than 2^m, let $(b_{i1}, b_{i2}, \ldots, b_{im})$ be the standard binary expression of i such that $i = \sum_{j=1}^{m} b_{ij} 2^{m-j}$. For $f(x_1, x_2, \ldots, x_m) \in P_m$, define a vector $\boldsymbol{v}(f) = (v_0, v_1, \ldots, v_{2^m-1})$ where $v_i = f(b_{i1}, b_{i2}, \ldots, b_{im})$. A vector $\boldsymbol{v}(f)$ is the vector representation of Boolean polynomial f. Any binary vector $\boldsymbol{u}$ of length 2^m have a Boolean polynomial f such that $\boldsymbol{u} = \boldsymbol{v}(f)$. We use both vector and polynomial for representing codewords of length 2^m.

We give a necessary and sufficient condition for non-minimality in a code of length 2^m.

Lemma 1. *For $f, g \in P_m$, if $f \preceq g$ then $gf = f$. Otherwise, $gf \prec f$.*

Theorem 2. *For a code C of length 2^m, $f \in C$ is not minimal in C if and only if there exists $g \in P_m$ such that $gf \in C \setminus \{0, f\}$.*

Proof. (If part) From Lemma 1, $gf \neq f$ means $gf \prec f$. The existence of $gf \in C$ such that $gf \prec f$ leads the non-minimality of f.
(Only if part) Non-minimality of f implies the existence of $f' \in C \setminus \{0\}$ such that $f' \prec f$. Then f' is g because $f'f = f' \neq f$ from Lemma 1. □

The r-th order binary Reed-Muller code of length 2^m, denoted by $RM(r, m)$, is the set of vectors obtained by all Boolean polynomials of degree at most r. A necessary and sufficient condition for minimality in Reed-Muller codes is given straightforwardly from Theorem 2.

Corollary 1. *A Boolean polynomial $f \in RM(r, m)$ is minimal in $RM(r, m)$ if and only if, for any $g \in RM(r, m)$, $gf \notin RM(r, m) \setminus \{0, f\}$.*

Theorem 7 in [3] says about the number of minimal codewords in certain representative cosets of $RM(3, m)/RM(2, m)$. In the proof of this theorem, a necessary condition for minimality in Reed-Muller code in the case g of Corollary 1 is confined to x_i is used implicitly. Therefore, Corollary 1 is a generalization of the fact used in this proof.

4. LWD Computation for the (256, 93) Reed-Muller Code

A clue for computing the local weight distribution of the (256, 93) Reed-Muller code, or $RM(3, 8)$, was presented in Sect. IV-B of [14]; The way is to use the coset partitioning algorithm described in Sect. 2 for computing the local weight subdistributions. However, we still have problem to find a permutation set having the property described in Theorem 6 of [14] (or Theorem 1 above). In this letter, we give one of such permutations, called *binary shift*, and use it for the computation. Thereby we determine the local weight distribution of the (256, 93) Reed-Muller code. Note that, as we will describe below, the local weight subdistributions for

4 out of 32 representative cosets in $RM(3,8)/RM(2,8)$ are determined with little computation as Borissov et al. shown in [3]. The property they used for the proof is generalized as a necessary and sufficient condition for minimality in Reed-Muller codes in Sect. 3.

To compute the local weight distribution of $RM(3,8)$ using the coset partitioning algorithm as described in Sect. 2, we choose $RM(2,8)$ and $RM(1,8)$ as C' and C'' respectively since $RM(1,8) \subset RM(2,8) \subset RM(3,8)$. The general affine group $GA(m)$ is an automorphism group of $RM(r,m)$ [10]. We choose $GA(8)$ as the permutation set Π, which is used for the coset partitioning algorithm above. $RC_{GA(8)}(RM(3,8)/RM(2,8))$ and $e_{GA(8)}(D)$ for $D \in RC_{GA(8)}(RM(3,8)/RM(2,8))$ are presented in [7], [12]. $RM(3,8)/RM(2,8)$ is classified into 32 equivalence classes. Thus we have to compute the local weight subdistributions for 32 representative cosets. To compute the local weight subdistributions for each representative coset $f + RM(2,8)$, we need to find a permutation set $\{\rho : \rho f \in f + RM(2,8),\ \rho \in GA(8)\}$ for each coset.

The general affine group $GA(m)$ is the set of permutations for m-variable polynomials $f(x_1, x_2, ..., x_m)$ that replace

$$f(x_1, ..., x_m) \text{ by } f\left(\sum a_{1j}x_j + b_j, ..., \sum a_{mj}x_j + b_m\right)$$

where $A = (a_{ij})$ is an invertible $m \times m$ binary matrix and $(b_1, ..., b_m)$ is a binary m-tuple. Affine permutation is called a *binary shift* when A is the identity matrix E. Let $BS(m)$ denote $GA(m)$ with $A = E$.

The set of binary shifts is suitable for the permutation set described in Theorem 1 because, for any coset $f + RM(2,8)$, a binary shift π satisfies $\pi f \in f + RM(2,8)$ clearly. Let $C_{BS}(\boldsymbol{v})$ be a set of codewords permuted by the binary shifts, that is, $C_{BS}(\boldsymbol{v}) = \{\pi\boldsymbol{v} : \pi \in BS(m)\}$.

Theorem 3 ([5], [8]). *Let f be an Boolean polynomial with degree r. For a coset $f + RM(r-1,m)$, $C_{BS}(f)$ is a linear subspace of $f + RM(r-1,m)$.*

Lemma 2 ([5], [8]). *Let f be an r-th order Boolean polynomial, and $\beta_i \in BS(m)$ be the permutation that only replaces x_i by $x_i + 1$. For a coset $f + RM(r-1,m)$, $\beta_i f$ for $1 \le i \le m$ are bases of $C_{BS}(f)$.*

Lemma 3. *For $f + RM(r-1,m) \in RM(r,m)/RM(r-1,m)$, let $f + f_1 + RM(r-1,m)$ be a coset in $(f + RM(r-1,m))/RM(r-2,m)$. The local weight subdistribution of $f + f_1 + RM(r-1,m)$ and that of $f + f_1 + g + RM(r-1,m)$ for any $g \in C_{BS}(f_1)$ are the same.*

From Lemma 3, each coset in $(f + RM(r-1,m))/RM(r-2,m)$ has $|C_{BS}(f)| = 2^{\dim(C_{BS}(f))}$ equivalent cosets. Therefore, for each coset $f + RM(r-1,m) \in RM(r,m)/RM(r-1,m)$, the number of cosets in $(f + RM(r-1,m))/RM(r-2,m)$ we have to compute their local weight subdistributions will be reduced by $1/|C_{BS}(f)|$.

Table 1 The dimension of $C_{BS}(f_i)$ for representative coset $f_i + RM(2,8) \in RM(3,8)/RM(2,8)$.

i	f_i	$\dim(C_{BS}(f_i))$
1	0	0
2	123	3
3	123+245	5
4	123+456	6
5	123+245+346	6
6	123+145+246+356+456	6
7	127+347+567	7
8	123+456+147	7
9	123+245+346+147	7
10	123+456+147+257	7
11	123+145+246+356+456+167	7
12	123+145+246+356+456+167+247	7
13	123+456+178	8
14	123+456+178+478	8
15	123+245+678+147	8
16	123+245+346+378	8
17	123+145+246+356+456+178	8
18	123+145+246+356+456+167+238	8
19	123+145+246+356+456+158+237 +678	8
20	123+145+246+356+456+278+347 +168	8
21	145+246+356+456+278+347+168 +237+147	8
22	123+234+345+456+567+678+128 +238+348+458+568+178	8
23	123+145+246+356+456+167+578	8
24	123+145+246+356+456+167+568	8
25	123+145+246+356+456+167+348	8
26	123+456+147+257+268+278+348	8
27	123+456+147+257+168+178+248 +358	8
28	127+347+567+258+368	8
29	123+456+147+368	8
30	123+456+147+368+578	8
31	123+456+147+368+478+568	8
32	123+456+147+168+258+348	8

For 32 representative coset $f_i + RM(2,8) \in RM(3,8)/RM(2,8)$ for $1 \le i \le 32$, we computed the dimension of $C_{BS}(f_i)$. The computation is just investigating the number of independent vectors in candidate bases, which are presented in Lemma 2. The 32 representative cosets and the dimension of $C_{BS}(f_i)$ is listed in Table 1. In this table, we follow the notations in [8], [12], and polynomial $x_{i_1}x_{i_2}x_{i_3}$ is represented as $i_1i_2i_3$ for convenience. For most cases, the dimension of $C_{BS}(f_i)$ is 8, and thus the time complexity for computing the local weight subdistribution for $f_i + RM(2,8)$ is reduced by 1/256. For the case that $i = 1, 2, 3$ ($f_1 = 0$, $f_2 = x_1x_2x_3$, $f_3 = x_1x_2x_3 + x_2x_4x_5$), above binary shift set method is not very effective for their small $\dim(C_{BS}(f_i))$. For many of $f_i + RM(2,8)$ including those with $i \le 3$, we can find permutations such that $\pi f_i \in f_i + RM(2,8)$ because of their simple forms of polynomials. In [4], Borissov and Manev gave another approach for determining the local weight subdistributions for four cosets, above three cosets and the coset $f_7 + RM(2,8) = x_1x_2x_7 + x_3x_4x_7 + x_5x_6x_7 + RM(2,8)$. From Theorem 7 in [4], there is no minimal codewords in $f_1 + RM(2,8)$, and the local weight subdistribution for $f_2 + RM(2,8)$ is determined immediately. For each $f_3 + RM(2,m)$ and $f_7 + RM(2,m)$,

Table 2 Local weight distribution of the $(256, 93)$ third-order binary Reed-Muller code.

w	L_w
32	777 240
48	2 698 577 280
56	304 296 714 240
64	74 957 481 580 800
68	707 415 842 488 320
72	28 055 013 884 190 720
76	764 244 915 168 215 040
80	20 661 780 862 988 697 600
84	414 411 510 493 363 568 640
88	6 266 129 424 660 312 883 200
92	71 773 299 826 457 585 909 760
96	627 671 368 441 418 233 282 560
100	4 208 996 769 021 096 823 357 440
104	21 729 928 024 588 603 285 831 680
108	86 666 048 822 136 825 068 912 640
112	267 785 773 787 841 625 294 110 720
116	642 456 218 534 940 726 012 149 760
120	1 198 819 482 820 829 207 341 301 760
124	1 741 767 435 501 050 021 239 848 960
128	1 971 038 877 022 035 145 182 412 800
132	1 735 627 864 909 747 949 509 017 600
136	1 184 951 930 170 762 649 130 762 240
140	620 824 077 435 771 999 611 781 120
144	242 710 219 348 184 804 622 336 000
148	65 293 324 137 047 881 521 561 600
152	8 982 921 659 842 430 396 006 400

the number of codewords which one should check minimality is only 2^{m+1}. Therefore the local weight subdistributions for these three cosets are determined with little computation. The local weight distribution of $RM(3, 8)$ is shown in Table 2.

Since $RM(3, 8)$ is a transitive invariant code and has codewords with weight only multiples of four, the local weight distributions of the punctured $(255, 93)$ Reed-Muller code $RM(3, 8)_{\mathrm{p}}$ and its even weight subcode $RM(3, 8)_{\mathrm{p(e)}}$ are obtained by using Theorems 9, 11, and 12 in [14]. From these theorems, we have that

$$L_w(RM(3,8)_{\mathrm{p}}) = \begin{cases} \dfrac{w+1}{256} L_{w+1}(RM(3,8)), & \text{for odd } w, \\[2ex] \left(1 - \dfrac{w}{256}\right) L_w(RM(3,8)), & \text{for even } w, \end{cases}$$

$$L_w(RM(3,8)_{\mathrm{p(e)}}) = L_w(RM(3,8)_{\mathrm{p}}), \ \text{for even } w.$$

5. Conclusions

The local weight distribution of the $(256, 93)$ third-order binary Reed-Muller code was computed by the modified coset partitioning algorithm. We applied the coset partitioning technique to compute the local weight subdistributions for each representative cosets. Binary shifts in the general affine group is useful for partitioning subcosets into equivalence classes. The time complexity was reduced by 1/256 or more for almost all representative cosets.

References

[1] E. Agrell, "Voronoi regions for binary linear block codes," IEEE Trans. Inf. Theory, vol.42, no.1, pp.310–316, Jan. 1996.

[2] A. Ashikhmin and A. Barg, "Minimal vectors in linear codes," IEEE Trans. Inf. Theory, vol.44, no.5, pp.2010–2017, Sept. 1998.

[3] Y. Borissov, N. Manev, and S. Nikova, "On the non-minimal codewords in binary Reed-Muller codes," Discrete Appl. Math., vol.128, no.1, pp.65–74, May 2003.

[4] Y. Borissov and N. Manev, "Minimal codewords in linear codes," Serdica Math. J., vol.30, no.2-3, pp.303–324, 2004.

[5] Y. Desaki, T. Fujiwara, and T. Kasami, "The weight distributions of extended binary primitive BCH codes of length 128," IEEE Trans. Inf. Theory, vol.43, no.4, pp.1364–1371, July 1997.

[6] G.D. Forney, Jr., "Geometrically uniform codes," IEEE Trans. Inf. Theory, vol.37, no.5, pp.1241–1260, Sept. 1991.

[7] X. Hou, "$GL(m, 2)$ acting on $R(r, m)/R(r-1, m)$," Discr. Math., vol.149, pp.99–122, 1996.

[8] X. Hou, "Classification of $R(3, 8)/R(2, 8)$," unpublished.

[9] T.-Y. Hwang, "Decoding linear block codes for minimizing word error rate," IEEE Trans. Inf. Theory, vol.IT-25, pp.733–737, Nov. 1979.

[10] F.J. MacWilliams and N.J.A. Sloane, The Theory of Error-correcting Codes, North-Holland, 1977.

[11] M. Mohri, Y. Honda, and M. Morii, "A method for computing the local weight distribution of binary cyclic codes," IEICE Trans. Fundamentals (Japanese Edition), vol.J86-A, no.1, pp.60–74, Jan. 2003.

[12] T. Sugita, T. Kasami, and T. Fujiwara, "The weight distribution of the third-order Reed-Muller codes of length 512," IEEE Trans. Inf. Theory, vol.42, no.5, pp.1622–1625, Sept. 1996.

[13] T. Yasuda, K. Yasunaga, and T. Fujiwara, "Improvement of the Séguin lower bound using the local weight distribution," Proc. SITA2005, pp.435–438, Nov. 2005.

[14] K. Yasunaga and T. Fujiwara, "Determination of the local weight distribution of binary linear block codes," IEEE Trans. Inf. Theory, vol.52, no.10, pp.4444–4454, Oct. 2006.