The relations between binary Reed-Muller codes and cyclic codes

Toshiko Koyama and Yuko Homma

(Received May 15, 2004)

Abstract. First we introduce a different representation of binary Reed-Muller codes. In consequence, we describe clearly the relations between binary Reed-Muller codes and binary cyclic codes, and prove them easily and directly.

1 Introduction

Though the shortened generalized Reed-Muller code is defined as a cyclic code (cf. [1]), there are no systematic and detailed explanations about the relations between binary Reed-Muller codes and binary cyclic codes so far as we know. So that, we introduce a different representation of Reed-Muller codes, and using this representation, describe the relations between them clearly. Consequently we can prove them easily and explicitly.

2 Reed-Muller codes

Let F_{2^m} be a finite field of order 2^m and let α be a primitive element of F_{2^m}. F_{2^m} is an m-dimensional vector space over prime field F_2 with a basis $\{1,\alpha,\alpha^2,\cdots,\alpha^{m-1}\}$. According to the list of the elements of F_{2^m} i.e. $F_{2^m}=\{\alpha^0=1,\alpha^1,\alpha^2,\cdots,\alpha^{2^m-2},\alpha^\infty=0\}$, we represent the characteristic function of an affine subspace U of F_{2^m} as $(c_0,c_1,\cdots,c_{2^m-2},c_\infty)$, i.e. if $\alpha^i\in U$ then $c_i=1$, otherwise $c_i=0$.

Definition 2.1 Let $0\le r\le m$. The linear code of length $n=2^m$ which is generated by all the characteristic functions of $(m-s)$-dimensional affine subspaces of F_{2^m} with $0\le s\le r$, is called the r th order binary Reed-Muller code and denoted by $R(r,m)$.

Theorem 4.5.9 in [1] shows us that $R(r,m)$ defined above is clearly equivalent to what is defined by Definition 4.5.6 in [1].

For $\xi_i\in F_2$ with $1\le i\le m$, $\sum_{i=1}^{m}\xi_i\,\alpha^{i-1}$ represents an element of F_{2^m}. Let U be the solution space of the following system of s linear equations $\xi_{i_1}=1$, $\xi_{i_2}=1,\cdots,\xi_{i_s}=1$ with $1\le i_1<i_2<\cdots<i_s\le m$. U is an $(m-s)$-dimensional affine subspace of F_{2^m}. The solution of void system stands for the whole space F_{2^m}. The set of the characteristic functions of the solution spaces of the systems of s linear equations with $0\le s\le r$ mentioned above is a basis for $R(r,m)$ (cf. [1]). Hence, the dimension of $R(r,m)$ is $1+\binom{m}{1}+\cdots+\binom{m}{r}$. Note that the minimum distance of $R(r,m)$ is 2^{m-r} and the dual of $R(r,m)$ is $R(m-r-1,m)$.

3 The relations between binary Reed-Muller codes and cyclic codes

Let C be a binary cyclic code of length n. If we identify code word $(c_0, c_1 \cdots, c_{n-1}) \in C$ with $c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} \in F_2[x]/(x^n - 1)$, C is an ideal in $F_2[x]/(x^n - 1)$ and for some polynomial $g(x)$ which is a divisor of $x^n - 1$, $C = (g(x))$. We call $g(x)$ a generator polynomial of the cyclic code C. Let β be a primitive n th root of unity. And suppose that $f(x) \in C$ if and only if $f(\beta^{i_j}) = 0$ for $j = 1,2,\cdots,k$. Then we call $\{ \beta^{i_1}, \cdots, \beta^{i_k} \}$ a defining set for C.

Proposition 3.1 $R(r,m)$ is equivalent to an extended cyclic code.

Proof. Let $(c_0, c_1, \cdots, c_{2^m-2}, c_\infty)$ be the characteristic function of an $(m-s)$-dimensional affine subspace U with $0 \le s \le r$. By the linear mapping $x \mapsto \alpha x$ for $x \in F_{2^m}$, U is mapped to αU. The characteristic function of αU, $(c_{2^m-2}, c_0, \cdots, c_\infty) \in R(r,m)$ and this is the cyclic shift on the first $2^m - 1$ positions of $(c_0, \cdots, c_{2^m-2}, c_\infty)$. Since all code words of $R(r,m)$ have even weight, $R(r,m)$ is equivalent to an extended cyclic code. □

Definition 3.2 Let U be an affine subspace of F_{2^m}. We define $\sum_i(U) = \sum_{x \in U} x^i$.

Definition 3.3 Let i be an integer. We denote the number of 1's in the binary expansion of i by $w(i)$.

We quote Lemma 6.6.12 in [1] as follows.

Lemma 3.4 Let U be a k-dimensional affine subspace of F_{2^m}. If $w(i) < k$ then $\sum_i(U) = 0$.

Proposition 3.5 Let α be a primitive element of F_{2^m}, and let $\{\alpha^i \mid 0 < i \le 2^m - 2, w(i) < l\}$ be a defining set for a cyclic code C of length $n = 2^m - 1$. $\overline{C}$ (extended code of C) is equivalent to $(m-l)$ th order Reed-Muller code $R(m-l,m)$. And the cyclic code with defining set $\{\alpha^i \mid 0 \le i \le 2^m - 2, w(i) < l\}$ is equivalent to shortened $R(m-l,m)$.

Proof. Let $f(x)$ be the irreducible divisor of $x^{2^m-1} - 1$ having α^i as a root. The set of conjugate roots of $f(x) = 0$ is $\{\alpha^i, \alpha^{2i}, \cdots, \alpha^{2^s i}\}$ where s is the minimal positive integer such that $(2^{s+1} - 1)i \equiv 0 \pmod{2^m - 1}$. Since $w(i) = w(2i) = \cdots = w(2^s i)$, $\{\alpha^i \mid 0 < i \le 2^m - 2, w(i) < l\}$ is the maximal defining set for C. Hence $g(x) = \prod_{0 < w(i) < l} (x - \alpha^i)$ is a generator polynomial of C. Let U be a k-dimensional affine subspace of F_{2^m} with $k \ge l$ and let $(c_0, c_1, \cdots, c_{2^m-2}, c_\infty)$ be the characteristic

function of U. Consider $c(x)=\sum_{j=0}^{2^m-2}c_jx^j$. For i with $0<w(i)<l$, $c(\alpha^i)=\sum_{\alpha^j\in U}(\alpha^i)^j=\sum_{\alpha^j\in U}(\alpha^j)^i$ $=\sum_i(U)=0$ by Lemma 3.4. That is, $g(x)$ divides $c(x)$. Hence $R(m-l,m)\subset\overline{C}$.

Let $i=\sum_{j=0}^{m-1}\xi_{i,j}2^j$ be the binary expansion of i. The number of i with $1\le w(i)<l$ is

$\binom{m}{1}+\cdots+\binom{m}{l}$. $\dim(\overline{g(x)})=\dim(g(x))=2^m-1-\deg(g(x))=2^m-1-\left\{\binom{m}{1}+\cdots+\binom{m}{l-1}\right\}$

$=1+\binom{m}{1}+\cdots+\binom{m}{m-l}=\dim R(m-l,m)$. Hence $\overline{C}$ is equivalent to $R(m-l,m)$. Next, $h(x)=(x-1)g(x)$ is a generator of the cyclic code with defining set $\{\alpha^i \mid 0\le i\le 2^m-2, w(i)<l\}$. Since $(h(x))$ consists of all code words of $(g(x))$ with even weight, $(h(x))$ is equivalent to shortened $R(m-l,m)$. □

Corollary 3.6 Let α be a primitive element of F_{2^m} and let $g(x)=\prod_{1\le w(i)<l}(x-\alpha^i)$, $h(x)=$ $\prod_{1\le w(i)<k}(x-\alpha^i)$, with $l+k=m+1$. Then the extended code $(\overline{g(x)})$ is equivalent to the dual of $(\overline{h(x)})$.

Proof. This follows from the fact that the dual of $R(m-l,m)$ is $R(m-k,m)$. □

Let $g(x)=\prod_{0<w(i)<l}(x-\alpha^i)$ and let $h(x)=(x^{2^m-1}-1)/g(x)=\prod_{l\le w(i)\le m}(x-\alpha^i)$. The dual of the cyclic code $(g(x))$ is $(h(x))$. On the extended codes of them, following proposition holds.

Proposition 3.7 The dual of $(\overline{g(x)})$ is $(\overline{h(x)/(x-1)})$.

Proof. The cyclic code $(h(x)/(x-1))$ is generated by two polynomials $h(x)$ and $1+x+x^2\cdots+x^{2^m-2}$. $(h(x))$ and $(g(x))$ are orthogonal and since $h(1)=0$, $(\overline{h(x)})$ and $(\overline{g(x)})$ are orthogonal. The vector $(1,1,\cdots,1)$ of length 2^m is orthogonal to any vector of $(\overline{g(x)})$. Hence $(\overline{g(x)})$ and $(\overline{h(x)/(x-1)})$ are orthogonal. Since $\dim(g(x))+\dim(h(x))=2^m-1$, $\dim(\overline{g(x)})+\dim(\overline{h(x)/(x-1)})=$ $\dim(g(x))+\dim(h(x)/(x-1))=\dim(g(x))+\dim(h(x))+1=2^m$. □

Corollary 3.8 $(\overline{h(x)/(x-1)})$ is equivalent to $R(l-1,m)$, and $(h(x))$ is equivalent to shortened $R(l-1,m)$.

Proof. This follows from Propositions 3.5 and 3.7. □

Corollary 3.9 Let C be a binary cyclic code of length 2^m-1 with a defining set $\{\alpha^1,\alpha^2,\cdots,\alpha^{2^l-1}\}$, where α is a primitive element of F_{2^m}. (This is so-called BCH code of designed distance 2^l.) The extended code $\overline{C}$ contains $R(m-l-1,m)$.

Proof. If $1\le i\le 2^l-1$, then $1\le w(i)\le l$. The result follows immediately. □

References

[1] J. H. van Lint, *Introduction to Coding Theory*, Graduate texts in Mathematics 86 (Third Edition), Springer, 1999.

[2] P. J. Cameron and J. H. van Lint, *Designs, Graphs, Codes and their Links*, London Mathematical Society Student Tests 22, Cambridge University Press, 1991.

[3] J. H. van Lint, *Coding Theory*, Springer Lecture Notes Vol. 201, Springer, 1971.

Toshiko Koyama
c/o Department of Information Sciences
Ochanomizu University
Tokyo 112-8610
Japan
E-mail: koyama@is.ocha.ac.jp

Yuko Homma
1-19-4, Yayoicho, Nakanoku
Tokyo 164-0013
Japan
E-mail: yhomma@n.kanagawa-u.ac.jp