SHAPIRO POLYNOMIALS AND REED-MULLER CODES*

V. N. Malozemov — malv@math.spbu.ru

I. S. Stojanoska — irena.stoyanoska@gmail.com

26 November 2011

In this paper we investigate the relationship bethween the Shapiro polynomials and the Reed-Muller codes given in the paper [1].

1°. The Shapiro polynomials are defined recursively by

$$P_0(x) \equiv 1, \quad Q_0(x) \equiv 1$$

and when $m = 0, 1, \ldots$,

$$P_{m+1} = P_m(x) + x^{2^m} Q_m(x), \tag{1}$$

$$Q_{m+1} = P_m(x) - x^{2^m} Q_m(x). \tag{2}$$

For example,

$$\begin{aligned} P_1(x) &= 1 + x, & Q_1(x) &= 1 - x, \\ P_2(x) &= 1 + x + x^2 - x^3, & Q_2(x) &= 1 + x - x^2 + x^3, \\ P_3(x) &= 1 + x + x^2 - x^3 + & Q_3(x) &= 1 + x + x^2 - x^3 - \\ &\quad + x^4 + x^5 - x^6 + x^7, & &\quad - x^4 - x^5 + x^6 - x^7. \end{aligned}$$

It is clear that the degree of polynomials $P_m(x)$ and $Q_m(x)$ is $2^m - 1$.

LEMMA 1. *The following formulas hold*

$$P_{m+1}(x) = P_m(x^2) + x\,P_m(-x^2), \quad m = 0, 1, \ldots; \tag{3}$$

$$Q_{m+1}(x) = Q_m(x^2) + x\,Q_m(-x^2), \quad m = 1, 2, \ldots. \tag{4}$$

*Seminar on Discrete Harmonic Analysis and Computer Aided Geometric Design (DHA & CAGD): `http://www.dha.spb.ru/`

P r o o f. The formula (3) for $m = 0, 1, 2$ and formula (4) for $m = 1, 2$ can be checked directly. We now make the induction step from m to $m + 1$, for $m \geq 2$.

We rewrite the relations (1) and (2), replacing m by $m-1$ and x by x^2. Taking into account that $(x^2)^{2^{m-1}} = x^{2^m}$, we have

$$\begin{aligned} P_m(x^2) &= P_{m-1}(x^2) + x^{2^m} Q_{m-1}(x^2), \\ Q_m(x^2) &= P_{m-1}(x^2) - x^{2^m} Q_{m-1}(x^2). \end{aligned} \tag{5}$$

Now we replace m by $m - 1$ and x by $-x^2$ in (1) and (2). Given the equality $(-x^2)^{2^{m-1}} = x^{2^m}$, which is true for $m \geq 2$, we get the relations

$$\begin{aligned} P_m(-x^2) &= P_{m-1}(-x^2) + x^{2^m} Q_{m-1}(-x^2), \\ Q_m(-x^2) &= P_{m-1}(-x^2) - x^{2^m} Q_{m-1}(-x^2). \end{aligned} \tag{6}$$

Using the induction hypothesis and the formulas (1), (5), (6) we get

$$\begin{aligned} P_{m+1}(x) = P_m(x) + x^{2^m} Q_m(x) &= P_{m-1}(x^2) + x P_{m-1}(-x^2) + \\ &+ x^{2^m}[Q_{m-1}(x^2) + x\, Q_{m-1}(-x^2)] = P_{m-1}(x^2) + x^{2^m} Q_{m-1}(x^2) + \\ &+ x[P_{m-1}(-x^2) + x^{2^m} Q_{m-1}(-x^2)] = P_m(x^2) + x P_m(-x^2). \end{aligned}$$

The relation (3) is thus established.

The formula (4) is verified in a similar manner. □

2°. Set $n = 2^m$. By definition, the first n coefficients of the polynomial $P_{m+1}(x)$ are identical with those of $P_m(x)$. It follows then that these coefficients do not depend on m.

Let

$$P_m(x) = \sum_{k=0}^{n-1} a_k\, x^k.$$

LEMMA 2. *The following recursive relations of the coefficients $\{a_k\}$ hold:*

$$a_0 = 1$$

and for $k \in 0 : 2^{m-1} - 1,\ m = 1, 2, \ldots$

$$a_{2k} = a_k, \quad a_{2k+1} = (-1)^k a_k. \tag{7}$$

P r o o f. According to (3), for $m \geq 1$ we have

$$\begin{aligned} P_m(x) &= P_{m-1}(x^2) + x P_{m-1}(-x^2) = \\ &= \sum_{k=0}^{2^{m-1}-1} a_k\, x^{2k} + \sum_{k=0}^{2^{m-1}-1} (-1)^k a_k\, x^{2k+1}. \end{aligned}$$

The needed relations immediately follow from this formula. □

The following table shows the results of the sequential computation of the Shapiro polynomials' coefficients, by formula (7).

Table

m	$P_m(x)$ polynomial's coefficients							
0	1							
1	1	1						
2	1	1	1	−1				
3	1	1	1	−1	1	1	−1	1

3°. An explicit formula for the coefficents a_k of the polynomial $P_m(x)$ can be derived. In order to do this, we associate with the index k its binary expansion

$$k = (k_{m-1}, k_{m-2}, \ldots, k_0)_2, \quad k_\alpha \in \{0, 1\}.$$

THEOREM 1. *For $k \in 0 : 2^m - 1$, $m \geq 2$, the following formula holds*

$$a_k = (-1)^{\sum_{\alpha=1}^{m-1} k_{\alpha-1} k_\alpha}. \tag{8}$$

Proof. For $m = 2$, when $k = (k_1, k_0)_2$, the formula (8) is verified directly. We proceed by induction from m to $m + 1$.

Let $k \in 0 : 2^{m+1} - 1$. We represent k in the form $k = 2k' + \sigma$, where $k' \in 0 : 2^m - 1$ and $\sigma \in \{0, 1\}$. We can write $k' = (k'_{m-1}, \ldots, k'_0)_2$. Then,

$$k = (k'_{m-1}, \ldots, k'_0, \sigma)_2,$$

that is, $k_\alpha = k'_{\alpha-1}$ for $\alpha \in 1 : m$ and $k_0 = \sigma$.

According to (7)

$$a_{2k'+\sigma} = (-1)^{k'\sigma} a_{k'} = (-1)^{k'_0 \sigma} a_{k'}.$$

We use the induction hypothesis, whereby

$$a_{k'} = (-1)^{\sum_{\alpha=1}^{m-1} k'_{\alpha-1} k'_\alpha}.$$

We find that

$$\begin{aligned} a_k = a_{2k'+\sigma} &= (-1)^{k'_0 \sigma} (-1)^{\sum_{\alpha=1}^{m-1} k'_{\alpha-1} k'_\alpha} = \\ &= (-1)^{k_1 k_0} (-1)^{\sum_{\alpha=1}^{m-1} k_\alpha k_{\alpha+1}} = (-1)^{\sum_{\alpha=1}^{m} k_{\alpha-1} k_\alpha}. \end{aligned}$$

The theorem is proved. □

We introduce the function

$$\phi(k) = \sum_{\alpha=1}^{m-1} k_{\alpha-1}k_\alpha = \\ = k_0k_1 + k_1k_2 + \ldots + k_{m-2}k_{m-1}, \quad k \in 0 : n-1.$$

The value of this function $\phi(k)$ for k fixed equals the number of times the block $\begin{bmatrix}1 & 1\end{bmatrix}$ appears in the binary expansion of the index k. We now can rewrite formula (8) as

$$a_k = (-1)^{\phi(k)}, \quad k \in 0 : n-1.$$

4°. Let us note one fundamental property of the Shapiro polynomials.

THEOREM 2. *For all $m = 0, 1, \ldots$ and all complex z, such that $|z| = 1$, the following equality holds*

$$|P_m(z)|^2 + |Q_m(z)|^2 = 2^{m+1}.$$

This equality can be easily proven by induction, using the formulas (1), (2) and the elementary property of the complex numbers

$$|z_1 + z_2|^2 + |z_1 - z_2|^2 = 2\big(|z_1|^2 + |z_2|^2\big).$$

5°. We now turn to Reed-Muller codes (see, for example, [2, p. 58–62]). Let r and m be fixed natural numbers, $r < m$, and let $n = 2^m$. We introduce a block encoding matrix of the form

$$G = \begin{bmatrix} G_0 \\ G_1 \\ \ldots \\ G_r \end{bmatrix}.$$

Here, G_0 is a row vector of size n, consisting of ones,

$$G_0 = \begin{bmatrix}1 & 1 & \ldots & 1\end{bmatrix} = [g_0];$$

$G_1 = G_1[1 : m, 0 : n-1]$ is a matrix, the columns of which consist of the coefficients of the numbers $0, 1, \ldots, n-1$, in their binary expansion starting with the most significant bit. For example, for $m = 4$

$$G_1 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} g_1 \\ g_2 \\ g_3 \\ g_4 \end{bmatrix}.$$

To form the rows of the rest of the blocks G_s, $s = 2, \dots, r$, we take all possible component-wise products of s rows of the matrix G_1. The combinations of s rows are taken in lexicographic order. For example, let $m = 4$

$$G_2 = \begin{bmatrix} g_1g_2 \\ g_1g_3 \\ g_1g_4 \\ g_2g_3 \\ g_2g_4 \\ g_3g_4 \end{bmatrix}, \quad G_3 = \begin{bmatrix} g_1g_2g_3 \\ g_1g_2g_4 \\ g_1g_3g_4 \\ g_2g_3g_4 \end{bmatrix}.$$

The size of the block G_s is $C_m^s \times 2^m$. The matrix G is of size

$$(1 + C_m^1 + C_m^2 + \dots C_m^r) \times 2^m.$$

We consider the rows of the matrix as elements in $\mathbb{Z}_2^n$, where bitwise addition modulo 2 and bitwise multiplication are introduced.

Let i be the information word. All its components are equal to zero or one, and its length equals the number of rows of matrix G. The Reed-Muller codeword is defined as

$$c = i\,G. \tag{9}$$

This means, that the codeword c is a linear combination of the rows of matrix G. The coefficients of this linear combination are the components of the information word i (equal to zero or one). The linear combination is evaluated by the rules introduced in $\mathbb{Z}_2^n$.

For example, let $m = 3$, $r = 1$. In that case,

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

Let the information word be $i = \begin{bmatrix} 1 & 1 & 1 & 0 \end{bmatrix}$. We obtain the corresponding codeword $c = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$.

The set of codewords c of the form (9) for different i is called the Reed-Muller code and is denoted as $RM(r, m)$.

6°. We now study the properties of the matrix G_1 in more detail. Let $j \in 0 : n-1$, $j = (j_{m-1}, \dots, j_0)_2$. By definition,

$$G_1[k, j] = j_{m-k}, \quad k \in 1 : m. \tag{10}$$

Recall the definition of the Rademacher functions

$$r_k(j) = (-1)^{j_{m-k}}, \quad j \in 0 : n-1, \quad k \in 1 : m.$$

According to (10) for $k \in 1 : m$

$$(-1)^{G_1[k,j]} = r_k(j), \quad j \in 0 : n-1. \tag{11}$$

We denote by $(-1)^{G_1}$ a matrix with elements $(-1)^{G_1[k,j]}$. Then the property (11) can be formulated as: *the k-th row of the matrix $(-1)^{G_1}$ coincides with the values of the Rademacher functions r_k.*

Now we introduce the matrix $D = G_1^\top G_1$. The rows of matrix D are linear combinations in $\mathbb{Z}_2^n$ of the rows of matrix G_1. We show that

$$(-1)^D = H,$$

where H is Hadamard matrix. [Recall (see, for example, [3, p. 54]) that Hadamard matrix on the indexes $l = (l_{m-1}, \dots, l_0)_2, j = (j_{m-1}, \dots, j_0)_2$ is defined as

$$H[l,j] = (-1)^{\sum_{\alpha=0}^{m-1} l_\alpha j_\alpha}, \quad l, j \in 0 : n-1.]$$

According to (10)

$$\begin{aligned}(-1)^{D[l,j]} &= (-1)^{\left\langle \sum_{k=1}^{m} G_1[k,l] G_1[k,j] \right\rangle_2} = \\ &= (-1)^{\sum_{k=1}^{m} l_{m-k} j_{m-k}} = (-1)^{\sum_{\alpha=0}^{m-1} l_\alpha j_\alpha} = H[l,j].\end{aligned}$$

7°. Consider the following codeword in $RM(2,m)$ for $m \geq 3$

$$s = \sum_{k=1}^{m-1} g_k g_{k+1} = [s_0\, s_1 \dots s_{n-1}]. \tag{12}$$

For example, for $m = 3$ we have $s = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \end{bmatrix}$. We introduce the vector

$$(-1)^s = \begin{bmatrix} 1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 \end{bmatrix}$$

and write the corresponding generating function

$$p(x) = 1 + x + x^2 - x^3 + x^4 + x^5 - x^6 + x^7.$$

It is clear, that $p(x)$ is the Shapiro polynomial for $m = 3$, $p(x) = P_3(x)$.

A similar fact holds in general case.

THEOREM 3. *The following formula holds for the coefficients of the Shapiro polynomials $P_m(x)$ for $m \geq 3$*

$$a_j = (-1)^{s_j}, \quad j \in 0 : n-1,$$

where s_j are the components of the codeword s in the form (12).

P r o o f. According to (10)

$$s_j = \left\langle \sum_{k=1}^{m-1} G_1[k,j] G_1[k+1,j] \right\rangle_2 = \left\langle \sum_{k=1}^{m-1} j_{m-k} j_{m-k-1} \right\rangle_2 =$$
$$= \left\langle \sum_{\alpha=1}^{m-1} j_{\alpha-1} j_\alpha \right\rangle_2 .$$

Finally, taking into account (8), we obtain

$$(-1)^{s_j} = (-1)^{\sum_{\alpha=1}^{m-1} j_{\alpha-1} j_\alpha} = a_j.$$

The theorem is proved. □

REFERENCES

1. An M., Byrnes J., Moran W. , Saffari B. , Shapiro H. S. and Tolimieri R. *PONS, Reed-Muller codes, and group algebras.* NATO Advanced Study Institute: Computational Noncommutative Algebra and Applications. Tuscany, Italy. July 2003. P. 155–197

2. Blahut R. E. *Theory and practice of error control codes*, Addison-Wesley Pub. Co., 1983. 500 p.

3. Malozemov V. N., Masharskiy S. M. *Foundations of Discrete Harmonic Analysis.* Part 2. SPb.: NIIMM SPbSU, 2003. 100 p.