ПОЛИНОМЫ ШАПИРО
И КОДЫ РИДА-МАЛЛЕРА*

В. Н. Малозёмов — malv@math.spbu.ru

И. С. Стояноска — irena.stoyanoska@gmail.com

26 ноября 2011 г.

В этом докладе мы анализируем связь между полиномами Шапиро и кодами Рида-Маллера, отмеченную в работе [1].

1°. Полиномы Шапиро определяются рекуррентно:

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

и при $m = 0, 1, \ldots$

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

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

В частности,

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

Ясно, что полиномы $P_m(x)$ и $Q_m(x)$ имеют степень $2^m - 1$.

ЛЕММА 1. *Справедливы формулы*

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

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

*Семинар по дискретному гармоническому анализу и геометрическому моделированию «DHA & CAGD»: http://www.dha.spb.ru/

Доказательство. Формула (3) при $m = 0, 1, 2$ и формула (4) при $m = 1, 2$ проверяются непосредственно. Сделаем индукционный переход от m к $m+1$, считая, что $m \geqslant 2$.

Перепишем соотношения (1) и (2), заменив в них m на $m-1$ и x на x^2. Приняв во внимание, что $(x^2)^{2^{m-1}} = x^{2^m}$, получим

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

Теперь заменим в (1) и (2) m на $m-1$ и x на $-x^2$. С учётом равенства $(-x^2)^{2^{m-1}} = x^{2^m}$, верного при $m \geqslant 2$, придём к соотношениям

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

На основании индукционного предположения и формул (1), (5), (6) получаем

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

Соотношение (3) установлено.

Аналогично проверяется соотношение (4). □

2°. Обозначим $n = 2^m$. По построению первые n коэффициентов полинома $P_{m+1}(x)$ совпадают с коэффициентами полинома $P_m(x)$. Отсюда следует, что коэффициенты полиномов Шапиро не зависят от m.

Пусть

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

ЛЕММА 2. *Для коэффициентов $\{a_k\}$ справедливо рекуррентное соотношение:*

$$a_0 = 1$$

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

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

Доказательство. Согласно (3) при $m \geqslant 1$ имеем

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

Отсюда очевидным образом следует требуемое. □

В таблице приведены результаты последовательного вычисления коэффициентов полиномов Шапиро по формулам (7).

Таблица

m	Коэффициенты полинома $P_m(x)$							
0	1							
1	1	1						
2	1	1	1	-1				
3	1	1	1	-1	1	1	-1	1

3°. Для коэффициентов a_k полинома $P_m(x)$ можно указать явную формулу. Для этого с индексом k свяжем его двоичный код:

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

ТЕОРЕМА 1. *При $k \in 0 : 2^m - 1$, $m \geqslant 2$, справедлива формула*

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

Доказательство. При $m = 2$, когда $k = (k_1, k_0)_2$, формула (8) проверяется непосредственно. Сделаем индукционный переход от m к $m + 1$.

Пусть $k \in 0 : 2^{m+1} - 1$. Представим k в виде $k = 2k' + \sigma$, где $k' \in 0 : 2^m - 1$ и $\sigma \in \{0, 1\}$. Запишем $k' = (k'_{m-1}, \ldots, k'_0)_2$. Тогда

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

то есть $k_\alpha = k'_{\alpha-1}$ при $\alpha \in 1 : m$ и $k_0 = \sigma$.

Согласно (7)

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

Воспользуемся индукционным предположением, согласно которому

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

Получим

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

Теорема доказана. $\square$

Введём функцию

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

Величина $\phi(k)$ при фиксированном k показывает, сколько раз в двоичном коде индекса k встречается блок $\begin{bmatrix}1 & 1\end{bmatrix}$. С помощью функции $\phi(k)$ формулу (8) можно переписать в виде

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

4°. Отметим одно фундаментальное свойство полиномов Шапиро.

ТЕОРЕМА 2. *При всех* $m = 0, 1, \ldots$ *и всех комплексных* z, *таких, что* $|z| = 1$, *справедливо равенство*

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

Это равенство легко доказывается по индукции с помощью формул (1), (2) и элементарного свойства комплексных чисел

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

5°. Обратимся к кодам Рида-Маллера (см., например, [2, с. 76–81]). Зафиксируем натуральные числа r и m, $r < m$, и положим $n = 2^m$. Введём блочную кодирующую матрицу вида

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

Здесь G_0 — вектор-строка размера n, состоящая из единиц,

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

$G_1 = G_1[1 : m, 0 : n-1]$ — матрица, в столбцах которой стоят коэффициенты двоичных разложений чисел $0, 1, \ldots, n-1$, начиная со старшего разряда. Например, при $m = 4$

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

Строки остальных блоков G_s, $s = 2, \dots, r$, формируются как всевозможные покомпонентные произведения s строк матрицы G_1, причём комбинации из s строк берутся в лексикографическом порядке. Например, при $m = 4$

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

Блок G_s имеет размер $C_m^s \times 2^m$. Размер матрицы G равен

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

Будем считать, что строки матрицы G являются элементами множества $\mathbb{Z}_2^n$, в котором введены операция поразрядного сложения по модулю 2 и операция поразрядного умножения.

Пусть i — информационное слово. Все его компоненты равны нулю или единице, а длина совпадает с количеством строк матрицы G. Кодовое слово Рида-Маллера определяется так:

$$c = iG. \tag{9}$$

Это значит, что кодовое слово c является линейной комбинацией строк матрицы G, коэффициентами которой служат компоненты информационного слова i. Линейная комбинация вычисляется по правилам, введённым в $\mathbb{Z}_2^n$.

Пусть, например $m = 3$, $r = 1$. В этом случае,

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

Возьмём информационное слово $i = \begin{bmatrix} 1 & 1 & 1 & 0 \end{bmatrix}$. В качестве кодового слова получим $c = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$.

Множество кодовых слов c вида (9) при различных i называется кодом Рида-Маллера и обозначается $RM(r, m)$.

6°. Более детально изучим свойства матрицы G_1. Возьмём индекс $j \in 0 : n - 1$, $j = (j_{m-1}, \dots, j_0)_2$. По определению

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

Напомним определение функций Радемахера

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

Согласно (10) при $k \in 1 : m$

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

Обозначим через $(-1)^{G_1}$ матрицу с элементами $(-1)^{G_1[k,j]}$. Тогда свойство (11) можно сформулировать так: *k-я строка матрицы $(-1)^{G_1}$ совпадает со значениями функции Радемахера r_k.*

Теперь введём матрицу $D = G_1^T G_1$. Строки матрицы D являются линейными комбинациями в $\mathbb{Z}_2^n$ строк матрицы G_1. Покажем, что

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

где H — матрица Адамара. [Напомним (см., например, [3, с. 54]), что матрица Адамара на индексах $l = (l_{m-1}, \ldots, l_0)_2, j = (j_{m-1}, \ldots, j_0)_2$ определяется так:

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

Действительно, согласно (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°. Рассмотрим в $RM(2,m)$ при $m \geqslant 3$ кодовое слово

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

Например, при $m = 3$ имеем $s = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \end{bmatrix}$. Введём вектор

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

и запишем соответствующую производящую функцию

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

Видим, что $p(x)$ — полином Шапиро при $m = 3$, $p(x) = P_3(x)$.

Аналогичный факт имеет место и в общем случае.

ТЕОРЕМА 3. *Для коэффициентов полинома Шапиро $P_m(x)$ при $m \geqslant 3$ справедлива формула*

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

где s_j — компоненты кодового слова s вида (12).

Доказательство. Согласно (10)

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

Остаётся учесть, что в силу (8)

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

Теорема доказана. □

ЛИТЕРАТУРА

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. Блейхут Р. *Теория и практика кодов, контролирующих ошибки.* М.: Мир, 1986. 576 с.

3. Малозёмов В. Н., Машарский С. М. *Основы дискретного гармонического анализа.* Часть вторая. СПб.: НИИММ СПбГУ, 2003. 100 с.