Math-Net.Ru

Общероссийский математический портал

Г. И. Ивченко, Ю. И. Медведев, В. А. Миронова, Многочлены Кравчука и их применения в задачах криптографии и теории кодирования, *Матем. вопр. криптогр.*, 2015, том 6, выпуск 1, 33–56

DOI: <https://doi.org/10.4213/mvk150>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.197.217.227

26 апреля 2023 г., 10:21:30

УДК: 519.212.2+519.114

Многочлены Кравчука и их применения в задачах криптографии и теории кодирования

Г. И. Ивченко¹, Ю. И. Медведев², В. А. Миронова³

^{1,3} МИЭМ НИУ Высшая школа экономики, Москва

² Академия криптографии Российской Федерации, Москва

Получено 20.IV.2012

Приводится обзор основных свойств многочленов Кравчука, доказан ряд новых результатов для них, представляющих интерес для теории и приложений. Исследуются аналитические, теоретико-числовые свойства и асимптотическое поведение многочленов Кравчука при различных соотношениях между параметрами, анализируются их стохастические свойства при рандомизации параметров, рассматриваются применения многочленов Кравчука в анализе криптографических свойств булевых функций и в задачах теории кодирования.

Ключевые слова: многочлены Кравчука, случайные многочлены Кравчука, булевы функции, коды Хемминга, асимптотические соотношения

Krawtchouk polynomials and their applications in cryptography and coding theory

G. I. Ivchenko¹, Yu. I. Medvedev², V. A. Mironova³

^{1,3}NRU Higher School of Economics, Moscow

²Academy of Cryptography of the Russian Federation, Moscow

Abstract. Basic properties of the Krawtchouk polynomials are reviewed, some new results which are of interest for the theory and applications are obtained. We study analytic, number-theoretic properties and asymptotic behaviour of the Krawtchouk polynomials under different relations between their parameters along with the probabilistic properties of polynomials with random parameters. Applications of the Krawtchouk polynomials to the cryptographic properties of Boolean functions and coding theory are discussed.

Key words: Krawtchouk polynomials, random Krawtchouk polynomials, Boolean functions, Hamming codes, asymptotic formulas

Citation: *Mathematical Aspects of Cryptography*, 2015, vol. 6, no. 1, pp. 33–56 (Russian).

1. Введение. Генезис и представления многочленов Кравчука

Многочлены Кравчука действительного переменного x обычно определяются следующим образом:

$$P_k(x; n) = \sum_j (-1)^j \binom{x}{j} \binom{n-x}{k-j}, \quad (1.1)$$

где n, k — целые положительные числа и $\binom{x}{j} = \frac{x(x-1)\dots(x-j+1)}{j!}$, $j = 0, 1, \dots$

В дальнейшем, мы, как правило, будем считать, что переменная x принимает целые неотрицательные значения m , и для многочленов Кравчука использовать обозначение $P_k(m; n)$. Наряду с многочленами $P_k(m; n)$ иногда целесообразно использовать *нормированные* (или *симметрические*) многочлены Кравчука

$$S_k(m; n) = \binom{n}{m} P_k(m; n) = S_m(k; n). \quad (1.2)$$

Существуют и другие, более общие определения многочленов Кравчука. Так, в монографии Г. Сегё [8] многочленом Кравчука называется многочлен

$$K_k(m; n) = \binom{n}{k}^{-1/2} (pq)^{-\frac{k}{2}} \sum_j (-1)^{k-j} \binom{m}{j} \binom{n-m}{k-j} p^{k-j} q^j, \quad (1.3)$$

где p, q — положительные действительные числа.

Отметим также, что если в (1.3) положить $p = q = \frac{1}{2}$, то

$$K_k(m; n) = \binom{n}{k}^{-1/2} \sum_j (-1)^{k-j} \binom{m}{j} \binom{n-m}{k-j} = \binom{n}{k}^{-1/2} (-1)^k P_k(m; n). \quad (1.4)$$

Многочлены $P_k(m; n)$ были введены в 30-х годах прошлого столетия украинским математиком М. Ф. Кравчуком в [1] и являются частным случаем обширного класса ортогональных многочленов. Многочлены Кравчука широко используются в различных задачах математического анализа и теории вероятностей. В настоящее время к ним проявляется большой интерес в теории кодирования, криптографии и защите информации. Они используются при решении ряда теоретико-вероятностных и комбинаторных задач на группах и других алгебраических структурах, при анализе булевых функций и их

спектральных характеристик. Хотя теория этих многочленов далеко продвинута, для решения новых задач известные их свойства зачастую оказываются недостаточными, и целью данной работы является дать, во-первых, систематический обзор уже накопленных в этой области результатов, и, во-вторых, исследовать ряд новых свойств многочленов Кравчука, расширяющих сферу их приложений.

Изучению многочленов Кравчука посвящено значительное число работ. Вот далеко не полный их список: монографии Г. Сегё [8], Ф. Дж. Мак-Вильямс и Н. Дж. Слоэна [9], В. М. Сидельникова [10], Г. Бэйтмена и А. Эрдейи [11], В. Гузика и Р. Станицы [12], Ф. Дельсарта [6], а также статьи Ф. Дельсарта [13], Ван Тилборга [14], В. И. Левенштейна [15], Ф. Фаинсильвера и Р. Шотта [16], Р. Савицкого [17], В. И. Хохлова [18], [19].

2. Соотношения ортогональности

Система многочленов, определяемых соотношением (1.3), ортогональна относительно биномиального распределения $Bi(n, p)$ случайной величины X . Именно (см. [8]):

$$\mathbf{E} K_{\alpha}(X; n) K_{\beta}(X; n) = \sum_{m=0}^n b(m; n, p) K_{\alpha}(m; n) K_{\beta}(m; n) = \delta_{\alpha, \beta}, \quad (2.1)$$

где $b(m; n, p) = \binom{n}{m} p^m q^{n-m}$, $q = 1 - p$, и $\delta_{\alpha, \beta}$ — символ Кронекера. В частности, если $p = q = \frac{1}{2}$, то соотношение ортогональности принимает вид (см. (1.4))

$$\mathbf{E} P_{\alpha}(X; n) P_{\beta}(X; n) = \sum_{m=0}^n b\left(m; n, \frac{1}{2}\right) P_{\alpha}(m; n) P_{\beta}(m; n) = \binom{n}{\alpha} \delta_{\alpha, \beta}. \quad (2.2)$$

Другое соотношение ортогональности для многочленов Кравчука имеет вид (см. [8])

$$\sum_{m=0}^n P_k(m; n) P_m(r; n) = 2^n \delta_{k, r}.$$

Отметим еще одну связь многочленов Кравчука с биномиальным распределением.

Пусть $p = (1 - \delta)/2$. Непосредственно проверяется, что

$$b(m; n, p) = \binom{n}{m} 2^{-n} \sum_{k=0}^n P_k(m; n) \delta^k. \quad (2.3)$$

Это представление полезно при малых значениях параметра δ .

3. Рекуррентные соотношения и другие свойства

1) Три последовательных многочлена Кравчука $P_{k-1}(m; n)$, $P_k(m; n)$ и $P_{k+1}(m; n)$ связаны рекуррентным соотношением (см. [9])

$$(k+1)P_{k+1}(m; n) = (n-2m)P_k(m; n) - (n-k+1)P_{k-1}(m; n) \quad (3.1)$$

с начальными значениями $P_0(m; n) = 1$, $P_1(m; n) = n - 2m$. Аналогично:

$$(n-m)P_k(m+1; n) = (n-2k)P_k(m; n) - mP_k(m-1; n) \quad (3.2)$$

с начальными значениями $P_k(0; n) = \binom{n}{k}$, $P_k(1; n) = (1 - \frac{2k}{n}) \binom{n}{k}$,

$$(n-m)P_k(m+1; n) = (n-2k)P_k(m; n) - mP_k(m-1; n) \quad (3.3)$$

с начальными значениями $P_k(m; 0) = 1$, $P_k(m; 1) = 1 - m$, $m = 0, 1$.

2) В [9] показано, что любой многочлен $R(x)$ степени t с действительными коэффициентами можно представить в виде линейной комбинации

$$R(x) = \sum_{k=0}^t a_k P_k(x; n),$$

называемой *разложением $R(x)$ по Кравчуку*. Числа a_k называются *коэффициентами Кравчука*, они вычисляются по формулам

$$a_k = 2^{-n} \sum_{l=0}^k R(l) P_l(k; n), \quad k = 0, 1, \dots, t.$$

3) Многочлены Кравчука удовлетворяют *соотношению Кристоффеля–Дарбу* (см. [9])

$$\begin{aligned} & \frac{P_{k+1}(x; n)P_k(y; n) - P_k(x; n)P_{k+1}(y; n)}{xy} = \\ & = \frac{2}{k+1} \binom{n}{k} \sum_{i=0}^k P_i(x; n)P_i(y; n) \binom{n}{i}^{-1}, \quad x \neq y, \end{aligned} \quad (3.4)$$

а для их производной по x справедливо представление

$$P'_k(x; n) = -2 \sum_{i=0}^{[(k-1)/2]} \frac{P_{k-2i-1}(x; n)}{2i+1}. \quad (3.5)$$

4) *Свойства корней* (см. [9]). Многочлен $P_k(x; n)$ имеет k различных действительных корней $0 < x_1 < \dots < x_k < n$, симметричных относительно центра $n/2$, т.е. $x_i + x_{k+1-i} = n$, $i = 1, \dots, k$, при этом $x_{i+1} - x_i > 2$ для всех n и $k < n/2$. Корни $y_1, \dots, y_{k-1}$ многочлена $P_{k-1}(y; n)$ перемежаются с корнями многочлена $P_k(x, n)$:

$$0 < x_1 < y_1 < x_2 < y_2 < \dots < x_{k-1} < y_{k-1} < x_k < n,$$

т.е. в каждом интервале (x_i, x_{i+1}) лежит ровно один корень y_i , $i = 1, 2, \dots, k-1$.

Имеют место следующие соотношения для корней (см. [14]):

$$\begin{aligned} \sum_{i=1}^k x_i &= \frac{k n}{2}, \\ \sum_{1 \leq i < j \leq k} x_i x_j &= \frac{k(k-1)}{24} (3n(n-1) + 2(k-2)), \\ \sum_{1 \leq i < j \leq k} (x_j - x_i)^2 &= \frac{k^2(k-1)}{12} (3n - 2k + 4). \end{aligned}$$

В теории кодирования особое значение имеет наименьший корень многочлена $P_k(x; n)$, для которого имеет место представление

$$x_1 = x_{1,n}(k) = \frac{n}{2} - \max \left(\sum_{i=0}^{k-2} a_i a_{i+1} \sqrt{(i+1)(n-i)} \right), \quad (3.6)$$

где максимум берется по всем действительным числам a_i , удовлетворяющим равенству $\sum_{i=0}^{k-1} a_i^2 = 1$. При $k \leq [n/2]$ справедливы оценки

$$\frac{n}{2} - \sqrt{(k-1)(n-k+2)} \leq x_{1,n}(k) \leq \frac{n}{2} - \sqrt{k(n-k)} + k^{1/6} \sqrt{n-k}.$$

Кроме того, если $n, k \rightarrow \infty$ так, что $k/n \rightarrow \lambda$, то

$$\frac{x_{1,n}(k)}{n} \rightarrow \xi = \frac{1}{2} - \sqrt{\lambda(1-\lambda)}.$$

При $n \rightarrow \infty$ и фиксированном k корни $x_i = x_{i,n}(k)$ аппроксимируются соответствующими корнями многочленов Эрмита:

$$x_{i,n}(k) = \frac{n}{2} + \frac{\sqrt{n-k-1}}{2} h_i(k) (1 + o(1)), \quad i = 1, 2, \dots, k, \quad (3.7)$$

где $h_1(k) < \dots < h_k(k)$ — нули многочленов Чебышева–Эрмита

$$H_k(x) = (-1)^k e^{\frac{x^2}{2}} \frac{d^k}{dx^k} e^{-\frac{x^2}{2}}. \quad (3.8)$$

В задачах теории кодирования важную роль играют целые корни многочлена $P_k(x, n)$. Обозначим их число $N(k)$. Для n четных и k нечетных целое число $n/2$ всегда является корнем $P_k(x, n)$, который называется *тривиальным*. Вопрос о существовании нетривиальных целых корней в общем случае остается открытым. Известно (см. [20]), что такие корни существуют для бесконечно многих значений n при

$$k = 2, 3, \frac{n-3}{2}, \frac{n-4}{2}, \frac{n-5}{2}, \frac{n-6}{2}, \frac{n-8}{2},$$

и при $t = n - 2k = 3, 4, 5, 6, 8$. Для ряда значений $n < 8400$ и соответствующих k известны частные значения нетривиальных целых корней, например (третья компонента является значением k):

$$(n, k, r) = (36, 5, 14), (67, 23, 31), (132, 19, 62), (576, 84, 286), (8361, 798, 4178).$$

В общем же случае можно лишь утверждать, что $N(k) \leq \min(k, n - 2k)$ (в [20] получен и ряд других границ для этой величины).

4. Производящие функции многочленов Кравчука и соотношения между ними

Основным аналитическим аппаратом для изучения свойств многочленов Кравчука является аппарат производящих функций.

1) Из представления (1.1) легко находится вид производящей функции по параметру k :

$$P(z; m, n) = \sum_k P_k(m; n) z^k = (1 - z)^m (1 + z)^{n-m}. \quad (4.1)$$

Некоторые авторы определяют многочлены Кравчука именно через эту производящую функцию. Используя обозначение $[z^n] f(z) = \text{coef}_{z^n} f(z)$, можно записать, что

$$P_k(m; n) = \left[z^k \right] (1 - z)^m (1 + z)^{n-m}. \quad (4.2)$$

2) Аналогично, из (1.6) находится производящая функция по параметру m (производящая функция для симметрических многочленов Кравчука):

$$Q(t; k, n) = \sum_m \binom{n}{m} P_k(m; n) t^m = \binom{n}{k} (1 - t)^k (1 + t)^{n-k}.$$

3) Так же легко находятся двойные производящие функции:

$$\begin{aligned} R(z; t; n) &= \sum_{k,m} \binom{n}{m} P_k(m; n) z^k t^m = \sum_m P(z; m, n) \binom{n}{m} t^m = \\ &= (1 + z + t(1 - z))^n = (1 + t + z(1 - t))^n, \\ S(z; x; m, n) &= \sum_{k,l} P_k(m; n+l) z^k x^l = P(z; m, n) \frac{1}{1-x-xz} \text{ при } |x(1+z)| < 1. \end{aligned}$$

Заменой параметров

$$p = \frac{1-z}{2}, \quad q = \frac{1+z}{2}, \quad p_1 = \frac{1-t}{2}, \quad q_1 = \frac{1+t}{2}$$

функции $R(z; t; n)$ можно придать вид

$$R(z; t; n) = 2^n (q + tp)^n = 2^n (q_1 + zp_1)^n.$$

При действительных значениях z и t ее можно рассматривать (с точностью до множителя) как производящую функцию биномиального закона распределения с соответствующими параметрами. Это обстоятельство позволяет использовать свойства биномиального закона распределения при анализе свойств многочленов Кравчука и наоборот.

4) Непосредственно из формулы (4.1) вытекают следующие рекуррентные соотношения для функции $P(z; m, n)$ и ее производной:

$$\begin{aligned} P(z; m, n) &= (1 - z)^r P(z; m - r, n - r), \quad r = \pm 1, \pm 2, \dots, \\ P(z; m, n) &= (1 + z)^r P(z; m, n - r), \quad r = \pm 1, \pm 2, \dots, \\ P'(z; m, n) &= (n - m)P(z; m, n - 1) - mP(z; m - 1, n - 1). \end{aligned}$$

5. Интегральные представления многочленов Кравчука

В [5] показано, что при четном m

$$P_k(m; n) = (-1)^{\frac{m}{2}} \frac{2^{n+1}}{\pi} \int_0^{\pi/2} \cos[(n - 2k)x] \sin^m x \cos^{n-m} x \, dx, \quad (5.1)$$

а при нечетном m

$$P_k(m; n) = (-1)^{\frac{m-1}{2}} \frac{2^{n+1}}{\pi} \int_0^{\pi/2} \sin[(n - 2k)x] \sin^m x \cos^{n-m} x \, dx. \quad (5.2)$$

6. Соотношения для многочленов Кравчука при различных значениях параметров

Свойства симметрии. Из (4.1) следует цепочка соотношений

$$\begin{aligned} P_k(m; n) &= \binom{n}{k} \binom{n}{m}^{-1} P_m(k; n) = (-1)^m P_{n-k}(m; n) = \\ &= (-1)^k P_k(n-m; n) = (-1)^{n-k-m} P_{n-k}(n-m; n). \end{aligned} \quad (6.1)$$

Отсюда следует, что многочлены Кравчука являются симметрическими функциями по параметрам m и k относительно точки $n/2$ (с учетом четности n и k). Эти соотношения симметрии позволяют проводить анализ свойств многочленов лишь по одному из параметров, переформулируя их затем для других параметров.

Теорема 1. 1) При четных n и $k = n/2$ имеет место представление:

$$P_k(m; n) = \begin{cases} 0 & \text{при нечетном } m, \\ (-1)^{\frac{m}{2}} \frac{2^n}{\pi} B\left(\frac{m+1}{2}, \frac{n-m+1}{2}\right) & \text{при четном } m, \end{cases} \quad (6.2)$$

где $B(a, b)$ — бета-функция.

2) Имеют место следующие оценки:

$$|P_k(m; n)| \leq \frac{2^n}{\pi} B\left(\frac{m+1}{2}, \frac{n-m+1}{2}\right), \quad (6.3)$$

$$|P_k(0; n)| = |P_k(n; n)| \leq \frac{2^n}{\pi} B\left(\frac{1}{2}, \frac{n+1}{2}\right) \leq 2^n \sqrt{\frac{2}{n}} \left(1 - \frac{1}{n+1}\right) \quad (6.4)$$

и равномерно по k

$$|P_k(m; n)| = \begin{cases} O(2^n n^{-(m+1)/2}), & n \rightarrow \infty, m = \text{const}, \\ O(n^{-(n+1)/2} m^{m/2} (n-m)^{(n-m)/2}), & n, m, n-m \rightarrow \infty. \end{cases} \quad (6.5)$$

Эти соотношения следуют из представлений (5.1), (5.2), известных свойств бета-функции и асимптотических оценок и неравенств для гамма-функции.

7. Линейные соотношения для сумм многочленов Кравчука

Из производящей функции (4.1) при $z = \pm 1$ непосредственно следуют соотношения

$$\sum_{k=0}^n P_k(m; n) = 2^n \delta_{m,0}, \quad (7.1)$$

$$\sum_{k=0}^n (-1)^k P_k(m; n) = 2^m \delta_{n-m,0}. \quad (7.2)$$

Теорема 2. *Справедливы следующие формулы:*

$$\sum_{k=0}^n (k)_r P_k(m; n) = (-1)^m r! \binom{n-m}{n-r} 2^{n-r} I(r \geq m), \quad (7.3)$$

$$\sum_{k=0}^n (-1)^k (k)_r P_k(m; n) = (-1)^{n-m} r! \binom{m}{n-r} 2^{n-r} I(r \geq n-m), \quad (7.4)$$

где $(k)_r = k(k-1) \dots (k-r+1)$,

$$\sum_{k=0}^n \binom{n-k}{n-l} P_k(m; n) = \binom{n-m}{l}, \quad l = 1, 2, \dots, k, \quad (7.5)$$

$$\sum_{l=0}^m \binom{m}{l} \binom{n-m}{j-l} P_k(l; j) = \binom{n-k}{j-k} P_k(m; n), \quad j = k, k+1, \dots, n. \quad (7.6)$$

Формулы (7.3) и (7.4) получаются дифференцированием производящей функции (4.1) в точках $z = \pm 1$, формулы (7.5) и (7.6) проверяются непосредственно.

Замечание. Другие линейные соотношения для многочленов Кравчука можно находить по следующей схеме: умножить левую и правую части равенства (4.1) на $(1-z)^{\pm j}$ (или на $(1+z)^{\pm j}$), $j = 1, 2, \dots$, и затем разложить соответствующую функцию по степеням z . Например,

$$\begin{aligned} [z^r] (1-z)^{-j} P(z; m, n) &= \sum_{k=0}^r \binom{j+k-1}{k} P_{r-k}(m; n) = \\ &= [z^r] (1-z)^{m-j} (1+z)^{n-m} = P_r(m-j; n-j), \quad r \geq 0, \quad j \geq 1. \end{aligned}$$

В частности, при $j = 1$ получаем формулу для неполной суммы:

$$\sum_{k=0}^r P_k(m; n) = P_r(m-1; n-1). \quad (7.7)$$

Левая часть этого соотношения носит название многочлена Ллойда (см. [9], с. 177).

8. Теоретико-числовые свойства многочленов Кравчука

1) Формулу (1.1) можно записать в виде разности двух комбинаторных сумм:

$$P_k(m; n) = \sum_j \binom{m}{2j} \binom{n-m}{k-2j} - \sum_j \binom{m}{2j+1} \binom{n-m}{k-2j-1},$$

откуда следует представление

$$\begin{aligned} P_k(m; n) \binom{n}{k}^{-1} &= \mathbf{P}\{\eta \equiv 0 \pmod{2}\} - \mathbf{P}\{\eta \equiv 1 \pmod{2}\} = \\ &= 2 \left(\mathbf{P}\{\eta \equiv 0 \pmod{2}\} - \frac{1}{2} \right), \end{aligned} \quad (8.1)$$

где η — случайная величина, имеющая гипергеометрическое распределение:

$$\mathbf{P}\{\eta = j\} = \frac{\binom{m}{j} \binom{n-m}{k-j}}{\binom{n}{k}}, \quad 0 \leq j \leq \min(k, m).$$

2) Суммы вида

$$L_r(m; n) = \sum_{k \equiv 0 \pmod{r}} P_k(m; n), \quad r = 2, 3, \dots \quad (8.2)$$

можно находить на основании следующего утверждения.

Лемма. Пусть $A(z) = \sum_k a_k z^k$ — производящая функция последовательности $\{a_0, a_1, \dots\}$, $r \geq 2$ — некоторое целое число. Тогда производящая функция последовательности $\{a_0, a_r, a_{2r}, \dots\}$ есть

$$A_r(z) = \frac{1}{r} \sum_{s=0}^{r-1} A\left(ze^{2\pi i \frac{s}{r}}\right).$$

Утверждение леммы вытекает из соотношения

$$\sum_{s=0}^{r-1} e^{2\pi i \frac{ks}{r}} = \begin{cases} r & \text{при } k, \text{ кратном } r, \\ 0 & \text{в противном случае.} \end{cases}$$

Применяя эту лемму к многочленам Кравчука, получаем (см. (4.1))

$$L_r(m; n) = \frac{1}{r} \sum_{s=0}^{r-1} \left(1 - e^{2\pi i \frac{s}{r}}\right)^m \left(1 + e^{2\pi i \frac{s}{r}}\right)^{n-m}.$$

Отсюда приходим к формуле

$$L_r(m; n) = 2^n (-i)^m \frac{1}{r} \sum_{s=0}^{r-1} e^{\pi i \frac{ns}{r}} \left(\sin \pi \frac{s}{r}\right)^m \left(\cos \pi \frac{s}{r}\right)^{n-m}. \quad (8.3)$$

В частности, если n кратно r , то

$$L_r(m; n) = 2^n (-i)^m \frac{1}{r} \sum_{s=0}^{r-1} \left(\sin \pi \frac{s}{r}\right)^m \left(\cos \pi \frac{s}{r}\right)^{n-m}.$$

Отсюда в качестве следствий получаем следующее утверждение.

Утверждение 1. Имеют место равенства:

$$L_r(2j+1; n) = 0, \quad j = 0, 1, \dots,$$

$$L_2(m; n) = 2^{n-1} (\delta_{m,0} + \delta_{m,n}), \quad (8.4)$$

$$\sum_{k \equiv 1 \pmod{2}} P_k(m; n) = 2^{n-1} (\delta_{m,0} - \delta_{m,n}), \quad (8.5)$$

а также равенства:

при четном $m > 0$

$$L_3(m; n) = 2^{-n} \delta_{m,0} + (-1)^n 3^{m/2} \cdot \begin{cases} 2, & \text{если } n \text{ кратно } 3, \\ -1 & \text{в противном случае,} \end{cases} \quad (8.6)$$

при нечетном $m > 0$

$$L_3(m; n) = \begin{cases} 0, & \text{если } n \text{ кратно } 3, \\ (-1)^{n+(m-1)/2} 3^{(m+1)/2} & \text{в противном случае.} \end{cases} \quad (8.7)$$

9. Квадратичные соотношения

1) С использованием производящей функции (4.1) находим:

$$\sum_{k=0}^n P_k(l; n) P_k(m; n) = [z^0] P(z; l, n) P\left(\frac{1}{z}; m, n\right) = (-1)^m P_n(l + m; 2n), \quad (9.1)$$

$$\begin{aligned} \sum_{k=0}^n (-1)^k P_k(l; n) P_k(m; n) &= [z^0] P(z; l, n) P\left(-\frac{1}{z}; m, n\right) = \\ &= (-1)^{n-m} P_n(n + l - m; 2n). \end{aligned} \quad (9.2)$$

2) Пусть $j = 0, \pm 1, \dots$, тогда

$$\sum_{k=0}^n P_k(m; n) P_{k-j}(m; n) = [z^j] P(z; m, n) P\left(\frac{1}{z}; m, n\right) = (-1)^m P_{n+j}(2m; 2n), \quad (9.3)$$

$$\begin{aligned} \sum_{k=0}^n (-1)^k P_k(m; n) P_{k-j}(m; n) &= [z^j] P(z; m, n) P\left(-\frac{1}{z}; m, n\right) = \\ &= (-1)^{n-m+(n+j)/2} \binom{n}{(n+j)/2} I(n+j \equiv 0 \pmod{2}). \end{aligned} \quad (9.4)$$

В частности, с учетом (6.2) получаем соотношения

$$\sum_{k=0}^n P_k^2(m; n) = (-1)^m P_n(2m; 2n) = \frac{2^{2n}}{\pi} B\left(m + \frac{1}{2}, n - m + \frac{1}{2}\right), \quad (9.5)$$

$$\sum_{k=0}^n (-1)^k P_k^2(m; n) = (-1)^{m+n/2} \binom{n}{n/2} I(n \equiv 0 \pmod{2}). \quad (9.6)$$

3) Как показано в [3], формула для суммы квадратов лишь по четным значениям индекса k имеет вид

$$\sum_{k \geq 0} P_{2k}^2(m; n) = \frac{2^{2n-1}}{\pi} B\left(m + \frac{1}{2}, n - m + \frac{1}{2}\right) + \frac{(-1)^{m+n/2}}{2} \binom{n}{n/2} I(n \equiv 0 \pmod{2}). \quad (9.7)$$

(При нечетных значениях n эта сумма равна половине полной суммы.)

4) Обозначим

$$S(m, k, l, n) = \sum_{j=0}^n \binom{l}{s} \binom{n-k}{l-s} P_j(m; n), \quad (9.8)$$

где $s = (k + l - j)/2$ (в этой сумме слагаемые с нецелыми значениями s равны нулю).

Утверждение 2. *Имеют место формулы линейаризации:*

$$P_k(m; n) P_l(m; n) = \binom{n}{k} S(m, k, l, n), \quad (9.9)$$

$$P_m(k; n) P_l(m; n) = \binom{n}{m} S(m, k, l, n), \quad (9.10)$$

$$P_k(m; n) P_m(l; n) = \frac{\binom{n}{k} \binom{n}{m}}{\binom{n}{l}} S(m, k, l, n). \quad (9.11)$$

Доказательство следует из представлений $P_k(m; n) = \sum_{\bar{x}: \|\bar{x}\|=k} (-1)^{(\bar{u}, \bar{x})}$, где $(\bar{u}, \bar{x}) = \sum_{i=1}^n u_i x_i \pmod{2}$ — скалярное произведение векторов пространства $V_n = \{0, 1\}^n$,

$$P_k(m; n) P_l(m; n) = \sum_{U_{k,l}} (-1)^{(\bar{u}, (\bar{x} \oplus \bar{y}))}, \quad U_{k,l} = \{\bar{x}, \bar{y} \in V_n: \|\bar{x}\| = k, \|\bar{y}\| = l\},$$

и стандартных комбинаторных рассуждений ($\|\bar{x}\| = \sum_{i=1}^n x_i$ — вес вектора $\bar{x}$).

10. Асимптотические свойства

Асимптотическое поведение многочленов $P_k(m; n)$ при $n \rightarrow \infty$ можно исследовать, используя их связь с гипергеометрическим распределением (см. (8.1)), которую мы запишем в виде

$$P_k(m; n) \binom{n}{k}^{-1} = 2 \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} \frac{\binom{m}{2j} \binom{n-m}{k-2j}}{\binom{n}{k}} - 1. \quad (10.1)$$

Варианты этого поведения описываются следующей теоремой.

Теорема 3. 1) Пусть $n \rightarrow \infty$, а величины k и m ограничены. Тогда

$$P_k(m; n) = \binom{n}{k} \left(1 - \frac{2km}{n} + O\left(\frac{1}{n^2}\right) \right). \quad (10.2)$$

2) Пусть $n \rightarrow \infty$, а k и $n - m$ ограничены. Тогда

$$P_k(m; n) = \binom{n}{k} \left(1 - \frac{2k(n-m)}{n} + O\left(\frac{1}{n^2}\right) \right). \quad (10.3)$$

3) Пусть $n, m \rightarrow \infty$, $m/n \rightarrow p$, $0 < p < 1$, а k ограничено. Тогда

$$P_k(m; n) = \binom{n}{k} (1-2p)^k \left(1 - \frac{2k(k-1)p(1-p)(1-2p)^{k-2}}{n(1+(1-2p)^k)} + O\left(\frac{1}{n^2}\right) \right). \quad (10.4)$$

4) Пусть $n, k \rightarrow \infty$, $m/n \rightarrow 0$, $km/n \rightarrow \lambda > 0$. Тогда

$$P_k(m; n) = \binom{n}{k} e^{-2\lambda} \left(1 + O\left(\frac{1}{n}\right) \right). \quad (10.5)$$

Доказательство. 1) В первом случае асимптотика суммы в (10.1) определяется первым слагаемым, что приводит к формуле (10.2).

2) В этом случае асимптотика суммы в (10.1) определяется ее последним слагаемым, и результат имеет вид (10.3).

3) В этом случае, как известно, гипергеометрическое распределение сходится к биномиальному распределению с параметрами (k, p) , и учет скорости сходимости, как нетрудно проверить, приводит к представлению (10.4).

4) Соотношение (10.5) является следствием того факта, что в рассматриваемых условиях гипергеометрическое распределение сходится к распределению Пуассона с параметром λ с указанной скоростью сходимости.

Известен также следующий результат (см. [8]). Пусть $n \rightarrow \infty$, $m = \frac{n}{2} + a\sqrt{\frac{n}{4}}$, a — фиксированное число, а k ограничено. Тогда

$$n^{-k/2}P_k(m; n) = (-1)^k \frac{1}{k!} H_k(a) + o(1), \quad (10.6)$$

где $H_k(x)$ — многочлены Чебышева–Эрмита (см. (3.8)).

Наконец, отметим асимптотическое соотношение

$$P_n(2m; 2n) = (-1)^m \frac{2^{2n}}{\pi} \cdot \begin{cases} \frac{\Gamma(m+1/2)}{n^{m+1/2}} (1 + o(1)), & n \rightarrow \infty, m = \text{const}, \\ \sqrt{\frac{\pi}{2}} \frac{m^m (n-m)^{n-m}}{n^{n+1/2}} (1 + o(1)), & n, m, n-m \rightarrow \infty, \end{cases} \quad (10.7)$$

которое следует из представления (9.5) и асимптотики для бета-функции.

11. Рандомизированные многочлены Кравчука

1) *Рандомизация. Логбиномиальное распределение.* Пусть параметр m в $P_k(m; n)$ является случайной величиной η с биномиальным распределением $Bi(n, p)$, $0 \leq p \leq 1$. Распределение случайной величины $\xi = a^\eta$, $a > 0$, мы будем называть *логбиномиальным распределением с параметрами a, n, p* , поскольку ее логарифм по основанию a имеет биномиальное распределение $Bi(n, p)$. При анализе булевых функций (см. п. 5 ниже) обычно этот параметр является весом $\|\bar{x}\|$ случайного булева вектора $\bar{x} = (x_1, \dots, x_n)$ с независимыми в совокупности компонентами с распределением

$$\mathbf{P}\{x_i = 1\} = p = \frac{1 - \delta}{2}, \quad \mathbf{P}\{x_i = 0\} = q = \frac{1 + \delta}{2}, \quad (11.1)$$

$$-1 \leq \delta \leq 1, \quad i = 1, \dots, n.$$

В таком случае

$$\mathbf{P}\{\|\bar{x}\| = m\} = \binom{n}{m} p^m q^{n-m},$$

и многочлены Кравчука $P_k(\eta; n)$, как и любые функционалы от них, становятся случайными величинами. Так, случайная производящая функция $P(z; \eta, n)$ (см. (4.1)) будет иметь распределение

$$\mathbf{P}\{P(z; \eta, n) = P(z; m, n)\} = \binom{n}{m} p^m q^{n-m}, \quad m = 0, 1, \dots, n.$$

Отсюда непосредственно вытекает следующее утверждение.

Теорема 4. Пусть случайная величина η имеет распределение $Bi(n, p)$, а действительное число z удовлетворяет условию $|z| < 1$. Тогда случайная величина $\xi = a^\eta = P(z; \eta, n) (1+z)^{-n}$ имеет логбиномиальное распределение с параметрами $a = (1-z)(1+z)^{-1}$, n, p .

Моменты этой величины считаются просто:

$$\mathbf{E}(a^\eta)^r = \sum_{m=0}^n a^{rm} \binom{n}{m} p^m q^{n-m} = (pa^r + q)^n, \quad r = 1, 2, \dots$$

2) Моменты $P_k(\eta; n)$. а) Из представления (4.1) и (11.1) имеем:

$$\begin{aligned} \mathbf{E} P_k(\eta; n) &= [z^k] \sum_{m=0}^n \binom{n}{m} (p(1-z))^m (q(1+z))^{n-m} = \\ &= [z^k] (p(1-z) + q(1+z))^n = [z^k] (1 + \delta z)^n = \binom{n}{k} \delta^k. \end{aligned} \quad (11.2)$$

Для равновероятного случая ($\delta = 0$) отсюда получаем, что $\mathbf{E} P_k(\eta; n) = 0$ для всех $k = 1, 2, \dots, n$.

Замечание. Если параметр k в $P_k(m; n)$ случаен: $k = \eta$ с биномиальным распределением $Bi(n, p)$, то в силу соотношения

$$\binom{n}{k}^{-1} P_k(m; n) = \binom{n}{m}^{-1} P_m(k; n)$$

(см. (6.1)) справедливы формулы

$$\mathbf{E} \binom{ln}{\eta}^{-1} P_\eta(m, n) = \delta^m, \quad m = 0, 1, \dots, n.$$

Формула (11.2) и приведенные в разделах 6 и 7 соотношения позволяют легко находить моменты из других случайных величин, связанных с $P_k(\eta; n)$. Например,

$$\mathbf{E} P_k(n - \eta; n) = \binom{n}{k} (-\delta)^k,$$

$$\mathbf{E} P_k(\eta - 1; n) = \sum_{j=0}^k \binom{n+1}{j} \delta^j,$$

$$\mathbf{E} (\eta P_k(\eta; n)) = \frac{n}{2} \binom{n-1}{k} \delta^{k-1} (1-\delta) \left(\delta - \frac{k}{n-k} \right), \quad k = 1, \dots, n-1,$$

$$\mathbf{E}(\eta P_n(\eta; n)) = \mathbf{E}(\eta(-1)^\eta) = n\delta^{n-1} \frac{\delta-1}{\delta+1}.$$

б) При вычислении вторых моментов, воспользовавшись формулой (9.9), получим

$$\mathbf{E} P_k(\eta; n) P_l(\eta; n) = \binom{n}{k} \mathbf{E} S(\eta, k, l, n) = \binom{n}{k} \sum_{j=0}^n \binom{l}{s} \binom{n-k}{l-s} \binom{n}{j} \delta^j. \quad (11.3)$$

В частности,

$$\mathbf{E} P_k^2(\eta; n) = \binom{n}{k} \sum_{j=0}^n \binom{k}{s} \binom{n-k}{k-s} \binom{n}{j} \delta^j. \quad (11.4)$$

3) *Случайное блуждание.* Пусть $\xi_1, \xi_2, \dots$ — независимые случайные величины с распределением

$$\mathbf{P}\{\xi_i = 1\} = \mathbf{P}\{\xi_i = -1\} = \frac{1}{2}, \quad i = 1, 2, \dots,$$

задающие случайное блуждание $\{X_n = \xi_1 + \dots + \xi_n, \quad n = 1, 2, \dots\}$ на целочисленной решетке, и $Y_n = (n - X_n)/2$ — число отрицательных приращений среди первых n скачков (так как величина $n - X_n$ всегда четная, то Y_n — целочисленная случайная величина). Тогда справедлива следующая цепочка соотношений (см. также (4.1)):

$$\begin{aligned} \prod_{i=1}^n (1 + z \xi_i) &= \sum_{k=0}^n z^k s_k(\xi_1, \dots, \xi_n) = \\ &= (1 - z)^{Y_n} (1 + z)^{n - Y_n} = P(z; Y_n, n) = \sum_{k=0}^n z^k P_k(Y_n; n), \end{aligned} \quad (11.5)$$

где

$$s_k(x_1, \dots, x_k) = \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} x_{i_1} x_{i_2} \cdots x_{i_k}, \quad k \geq 1, \quad s_0 = 1$$

— элементарные симметрические функции.

Таким образом, в этой конструкции естественно появляются многочлены Кравчука со случайным параметром Y_n , имеющим биномиальное распределение $Bi(n, 1/2)$. Такие многочлены $P_k(Y_n; n)$ мы будем называть *биномиальными многочленами Кравчука*. Напомним, что для них выполняется соотношение ортогональности (2.2).

Утверждение 3. *Имеет место представление*

$$P_k(\mu; n) = s_k(\xi_1, \dots, \xi_n), \quad (11.6)$$

где μ — случайная величина, равная числу отрицательных значений среди аргументов $\xi_1, \dots, \xi_n$.

Это утверждение вытекает из (11.5).

4) *Многомерные многочлены Кравчука* (см. [16], [18]). Пусть теперь $\xi_1, \xi_2, \dots$ — независимые одинаково распределенные случайные величины с произвольным дискретным распределением

$$\mathbf{P} \{ \xi_i = a_j \} = p_j, \quad j = 1, \dots, N, \quad p_1 + \dots + p_N = 1,$$

и $\mathbf{E} \xi_i = \mu$, $\mathbf{D} \xi_i = \sigma^2$.

По аналогии с (11.5) рассмотрим функцию

$$G_n(z) = \prod_{i=1}^n (1 + z(\xi_i - \mu)) = \prod_{j=1}^N (1 + z(a_j - \mu))^{\nu_j}, \quad (11.7)$$

где $\nu_j = \sum_{i=1}^n I(\xi_i = a_j)$, $j = 1, \dots, N$. Вектор $\nu(n) = (\nu_1, \dots, \nu_N)$ имеет полиномиальное распределение с параметрами $n = \nu_1 + \dots + \nu_N$ и $p = (p_1, \dots, p_N)$. Разложим функцию $G_n(z)$ по степеням z :

$$G_n(z) = \sum_{r=0}^n z^r K_r(\nu(n)), \quad K_r(\nu(n)) = \sum_{k_1 + \dots + k_N = r} \prod_{j=1}^N \binom{\nu_j}{k_j} (a_j - \mu)^{k_j}. \quad (11.8)$$

Ее коэффициенты назовем *многомерными многочленами Кравчука*. Для этих многочленов аналогом (2.2) является соотношение

$$\mathbf{E} K_r(\nu(n)) K_s(\nu(n)) = \delta_{r,s} \sigma^{2r} \binom{n}{r},$$

которое вытекает из непосредственно проверяемых равенств

$$\mathbf{E} G_n(z) G_n(v) = \left(1 + z v \sigma^2 \right)^n = \sum_{r,s} z^r v^s \mathbf{E} K_r(\nu(n)) K_s(\nu(n)).$$

5) *Многочлены Кравчука и булевы функции*.

Утверждение 4. Пусть координаты вектора $\bar{x} = (x_1, \dots, x_n)$ — независимые в совокупности и одинаково распределенные бернуллиевские случайные величины с распределением

$$\mathbf{P} \{ x_i = 1 \} = p = \frac{1 - \delta}{2}, \quad -1 \leq \delta \leq 1,$$

и $f(\bullet)$ — булева функция от n переменных. Тогда случайная величина $f(\bar{x})$ имеет распределение

$$\mathbf{P}\{f(\bar{x}) = 1\} = \frac{1}{2^n} \sum_{k=0}^n \sum_{m=0}^n f_m P_k(m, n) \delta^k. \quad (11.9)$$

где f_m — вес булевой функции $f(\bar{x})$ на векторах веса m , $m = 0, 1, \dots, n$.

Утверждение непосредственно проверяется с использованием формулы полной вероятности и соотношения (2.3).

В частности, если $f(\bar{x})$ есть элементарная симметрическая функция: $f(\bar{x}) = s_m(\bar{x}) \bmod 2$, то

$$\begin{aligned} \mathbf{P}\{f(\bar{x}) = 1\} &= \frac{1}{2^n} \sum_{k=0}^n \binom{n}{m} P_k(m; n) \delta^k = \\ &= 2^{-n} \binom{n}{m} (1 + \delta)^{n-m} (1 - \delta)^m = 2^{-n} \binom{n}{m} P_{n,m}(\delta), \end{aligned}$$

где $P_{n,m}(\delta)$ — производящая функция многочленов Кравчука в точке δ (см. (4.1)).

Многочлены Кравчука играют ключевую роль при анализе спектральных свойств симметрических булевых функций (см. [2, 5]). Именно, если

$$f(\bar{x}), \bar{x} = (x_1, x_2, \dots, x_n) \in V_n = \{0, 1\}^n$$

есть симметрическая булева функция от n переменных, и $f(\bar{x}) = a_k$, если $\|\bar{x}\| = k$, $k = 0, 1, \dots, n$, то ее спектральные коэффициенты w_m^f (значения спектра Уолша на векторах $\bar{x}$ веса m) можно записать в виде линейной комбинации многочленов Кравчука:

$$w_m^f = \sum_{k=0}^n a_k P_k(m; n), \quad m = 0, 1, \dots, n, \quad (11.10)$$

и наоборот,

$$a_k = 2^{-n} \sum_{m=0}^n w_m^f P_m(k; n), \quad k = 0, 1, \dots, n. \quad (11.11)$$

При этом многочлены Кравчука могут быть представлены в виде

$$P_k(m; n) = \sum_{\bar{x}: \|\bar{x}\|=k} (-1)^{(\bar{u}, \bar{x})}, \quad (11.12)$$

где $(\bar{u}, \bar{x}) = \sum_{i=1}^n u_i x_i \pmod{2}$ — скалярное произведение векторов пространства V_n . Формула (11.12) может служить в качестве одного из определений многочленов Кравчука (см. [4], с. 53).

12. Многочлены Кравчука и задачи теории кодирования

Многочлены Кравчука играют большую роль в теории кодирования. Особое значение они имеют при решении таких важных проблем, как оценка оптимальной мощности кодов и схем отношений в пространстве Хэмминга, обладающих теми или иными свойствами. Важнейшей проблемой теории кодирования, является проблема отыскания и построения наибольшего по объему кода заданной длины n с заданным минимальным расстоянием d между кодовыми словами.

1) Пусть $A(n, d)$ — максимальное число кодовых слов в произвольном двоичном коде (линейном или нелинейном) длины n с минимальным расстоянием между словами d . Известна классическая задача о нахождении верхних и нижних оценок для этого числа, которой посвящено огромное количество работ (см. [10]). Практически наилучшей верхней оценкой этого числа является граница Мак-Элайеса–Радемича–Рамсея–Велча при конечных значениях n . При больших значениях параметра n такой оценкой считается оценка Варшамова–Гилберта. В остальных случаях указанная оценка определяется через многочлены Кравчука. В частности (см. [9], с.545),

$$A(n, d) \leq \binom{n}{k} \frac{(n - k - (k + 1)Q_{k,n})}{-2a(k + 1)Q_{k,n}},$$

где $Q_{k,n} = P_{k+1}(a, n)/P_k(a, n)$ — отношение двух соседних многочленов Кравчука, a и k — параметры, лежащие в границах $x_{1,n}(k+1) < a < x_{1,n}(k)$, $a < d$, а $x_{1,n}(k)$ — минимальный корень $P_k(x; n)$.

Кроме того, если $n, k \rightarrow \infty$ так, что $k/n \rightarrow \lambda$, $0 < \lambda < 1$, то (см. (3.7))

$$A(n, d) \leq \binom{n}{k} \frac{(n + 1)^2}{2(k + 1)(n\xi)^{k+1}},$$

где $\xi = \frac{1}{2} - \sqrt{\lambda(1 - \lambda)}$.

2) Напомним, что *совершенный код* — это такое множество S векторов пространства V_n , что все шары радиуса r с центрами в точках множества S покрывают все пространство V_n без перекрытий (этот код исправляет все ошибки веса (числа искаженных компонент кодового слова) не более r , и не

может исправить ни одной ошибки веса, большего r). *Кратное совершенное s -покрытие радиуса r* — это такое множество $C \subseteq V_n$, где все шары радиуса r с центрами в точках множества C покрывают каждую точку пространства V_n ровно s раз. Вопрос о существовании таких кодов (покрытий) решается через свойства целых корней многочленов Кравчука.

Именно (см. [20]), если многочлен $P_k(x; n)$ имеет хотя бы один не целый корень, то не существует совершенного кода радиуса k в пространстве V_{n+1} . Пусть N — минимальное целое, удовлетворяющее неравенству

$$\sum_{m=0}^k \binom{n}{m} \leq s \sum_{m=0}^N \binom{n}{m}.$$

Тогда, если $P_k(m; n)$ имеет меньше N целых корней, то не существует s -покрытия радиуса k в V_{n+1} .

В настоящее время нет полного ответа на вопрос, когда существуют нецелые корни у многочленов Кравчука. Ряд частных решений этой проблемы имеется в [20].

С этой проблемой тесно связан вопрос о том, когда многочлен Кравчука вообще не имеет целых корней (эта задача также частично рассмотрена в [20]). Различные частные решения этого вопроса связаны с приведениями этих многочленов по модулю в стиле известной теоремы Лукача. Отметим также, что проблема наличия или отсутствия целых четных корней у $P_k(m; n)$ тесно связана с проблемой восстановления исходного графа по некоторой совокупности его подграфов (см. [21]).

3) *Линейные коды*. Пусть $L = L(n, k)$ — линейный двоичный код, слова которого составляют линейное подпространство размерности k , а дуальный (ортогональный) к нему код есть $L' = L'(n, n - k)$. Пусть $A_i = A_i(L)$ — число кодовых слов веса i в коде L . Вектор

$$A(L) = (A_0(L), A_1(L), \dots, A_n(L))$$

есть распределение весов (спектр расстояний) этого кода.

Преобразованием Мак-Вильямса спектра расстояний называется вектор

$$A'(L) = (A'_0(L), A'_1(L), \dots, A'_n(L)) \quad (12.1)$$

с компонентами

$$A'_k(L) = \sum_{m=0}^n A_m(L) P_k(m; n), \quad k = 0, 1, \dots, n,$$

где $P_k(m; n)$ — многочлены Кравчука (см. [9]), при этом

$$A'_k(L) = 2^{-n} \sum_{m=0}^n A'_m(L) P_k(m; n), \quad k = 0, 1, \dots, n.$$

Вектор (12.2) есть не что иное, как распределение весов дуального кода.

Отметим, что в классической модели случайного кода, когда кодовые слова выбираются равновероятно, *преобразование Мак-Вильямс (с точностью до множителя) есть не что иное, как математическое ожидание вектора, образованного многочленами Кравчука:*

$$A'_k(K) = \mathbf{E} P_k(\|x\|; n) |M|, \quad k = 0, 1, \dots, n.$$

Для линейного кода вводятся четыре параметра d, s, d', s' , где целые d и d' — минимальные веса кода L и дуального к нему кода L' соответственно, целые s и s' — числа различных весов кодов L и L' . Параметр s' называется внешним расстоянием, поскольку любой вектор y , не принадлежащий K , удален от кода K не более чем на s' .

Одна из основных задач теории кодирования — построение и изучение наиболее мощных кодов при тех или иных значениях параметров, а также нахождение соотношений между этими параметрами. Важное значение при решении этих вопросов имеют целые нули полиномов Ллойда:

$$Q_t(x; n) = \sum_{k=0}^t P_k(x; n) = P_t(x-1; n-1).$$

Имеет место следующее утверждение (граница Хэмминга и теорема Ллойда [13]): мощность кода K удовлетворяет неравенству

$$M \leq 2^n \left(\sum_{m=0}^t \binom{n}{m} \right)^{-1}, \quad t = [(d-1)/2],$$

при этом равенство достигается, если полином Ллойда имеет t различных целых нулей в множестве $\{1, 2, \dots, n\}$.

В заключение выражаем благодарность В. А. Копытцеву и В. Г. Михайлову за ценные замечания, способствовавшие улучшению изложения результатов данной работы.

Список литературы

1. *Krawtchouk M.* Sur une generalization des polynomes d'Hermite. *Comptes Rendus de l'Acad. Des Sci.* — 1929. — Т. 189. № 17. — P. 620–622.
2. *Canteaut A., Videau M.* Symmetric Boolean function // *IEEE Trans. Inf. Theory.* — 2005. — V. 51. № 8. — P. 2791–2811.
3. *Sarkar S., Maitra S.* Efficient search for symmetric Boolean functions under constraints on Walsh spectra values // *J. Comb. Math. and Comb. Comput.* — 2009. — V. 68. — P. 163–191.
4. *Mouffron M.* Balanced alternating and symmetric functions over finite sets // *Workshop on Boolean Functions: Cryptography and Applications (BFCA'08).* — 2008. — Copenhagen, Denmark. — P. 27–44.
5. *Ивченко Г. И., Медведев Ю. И., Миронова В. А.* Анализ спектра случайных симметрических булевых функций // *Математические вопросы криптографии.* — 2013. — Т. 4. № 1. — С. 59–76.
6. *Дельсарт Ф.* Алгебраический подход к схемам отношений теории кодирования. — М.: Мир, 1976, (пер. с англ.).
7. *Feinsilver Ph., Fitzgerald R.* The spectrum of symmetric Krawtchouk matrices. // *Linear algebra and its appl.* — 1996. — 235. — P. 121–139.
8. *Сегё Г.* Ортогональные многочлены. — М.: ФИЗМАТЛИТ, 1962.
9. *Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.* Теория кодов, исправляющих ошибки. — М.: Связь, 1979.
10. *Сидельников В. М.* Теория кодирования. — М.: ФИЗМАТЛИТ, 2008.
11. *Бэйтмен Г., Эрдейи А.* Высшие трансцендентные функции. — М.: Наука, 1965.
12. *Cusick Th. W., Stanica P.* Cryptographic Boolean Functions and Applications // *AP Elsevier, Amsterdam etc.* — 2009.
13. *Delsarte Ph.* Four fundamental parameters of a code and their combinatorial significance. // *Inf. and Control.* — 1973. — V. 23. № 5. — P. 407–438.
14. *Van Tilborg H. C. A.* Uniformly packed codes. Ph. D. Thesis, Eindhoven. — 1976.
15. *Levenshtein V. I.* Universal bounds for codes and designs // В кн. *Handbook of Coding theory.* — Amst., 1998. — P. 499–648.
16. *Feinsilver Ph., Schott R.* Krawtchouk polynomials and finite probability theory // *Probability Measures on Groups, X, Plenum.* — 1991. — P. 129–135.
17. *Savicky P.* On the bent Boolean functions that are symmetric // *European J. Comb.* — 1994. — V. 15. — P. 407–410.

18. *Хохлов В. И.* Многочлены, ортогональные относительно полиномиального распределения, и факториально-степенной формализм // Теория вероятн. и ее примен. — 2001. — Т. 46. Вып. 3. — С. 585–592.
19. *Хохлов В. И.* Многочлены Эрмита и многочлены Пуассона–Шарлье как классические пределы многочленов Кравчука // Обозр. прикл. и промышл. матем. — 2005. — Т. 16. Вып. 5. — С. 937–940.
20. *Krasikov I., Litsyn S.* On integral zeros of Krawtchouk polynomials // J. Comb. Theory, Ser. A. — 1996. — V. 74. — P. 132–138.
21. *Stanley R. P.* Reconstruction from vertex-switching // J. Comb. Theory, Ser. B. — 1985. — V. 38. — P. 132–138.