А. А. Груба, Булевы функции, построенные по разрядным последовательностям линейных рекуррент,
Дискрет. матем., 2023, том 35, выпуск 1, 54–61

https://www.mathnet.ru/dm1751

Дискретная математика

том 35 выпуск 1 * 2023

УДК 519.716.322+519.113.6 DOI https://doi.org/10.4213/dm1751

Булевы функции, построенные по разрядным последовательностям линейных рекуррент

© 2023 г. А. А. Груба*

Изучается класс булевых функций, построенных по разрядным последовательностям линейных рекуррент над кольцом $\mathbb{Z}_{2^n}$. Для него исследуются: расстояния между функциями, мощность класса, нелинейность и веса функций. Показано, что этот класс состоит из функций, значительно удаленных от класса всех аффинных функций.

Ключевые слова: линейные рекуррентные последовательности, булевы функции, нелинейность булевых функций

1. Введение

Пусть n — натуральное число, $R = \mathbb{Z}_{2^n} = \{0, 1, \ldots, 2^n - 1\}$ — кольцо вычетов по модулю 2^n, $P = \mathbb{Z}_2 = \{0, 1\}$ — поле из двух элементов. Операции сложения в R и P будем обозначать одним символом $+$. Контекст будет однозначно определять, в какой алгебре производится операция. Пусть $F(x) \in P[x]$ — унитарный (со старшим коэффициентом, равным 1) неприводимый многочлен степени m над полем P. Всюду в дальнейшем будем считать, что $F(x)$ — реверсивный многочлен над полем P, т. е. $F(0) \neq 0$. Известно [1], что период $T(F)$ многочлена $F(x)$ равен $T(F) = (2^m - 1)/d$, где d — некоторый делитель числа $2^m - 1$. Согласно [2] существует только один такой унитарный многочлен $G(x) \in R[x]$, что многочлен $\overline{G}(x) \in P[x]$, полученный из $G(x)$ приведением всех его коэффициентов по модулю 2, равен $F(x)$ и период $T(G)$ многочлена $G(x)$ совпадает с периодом $T(F)$. Такой многочлен $G(x)$ называется отмеченным над кольцом R. Кроме того, как показано в [2], существует простой способ построения многочлена $G(x)$ по многочлену $F(x)$.

Обозначим через $L_R(G)$ множество всех линейных рекуррентных последовательностей (ЛРП) v над кольцом R с характеристическим многочленом $G(x)$, а через $L_R(G)^*$ — его подмножество, состоящее из всех ЛРП, содержащих в своем начальном векторе

$$(v(0), \ldots, v(m-1))$$

хотя бы один обратимый элемент кольца R.

*Место работы: ООО «Центр сертификационных исследований», e-mail: andreyka7kc@gmail.com

Зададим на множестве $L_P(F)$ всех ЛРП над полем P с характеристическим многочленом $F(x)$ бинарное отношение $\sim$, полагая, что $u \sim u'$ при $u, u' \in L_P(F)$ тогда и только тогда, когда существует такое $t \in \mathbb{N}_0$, что $u' = x^t u$, т. е. $u'(i) = u(i+t)$ для всех $i \geqslant 0$. В силу реверсивности многочлена $F(x)$ введенное бинарное отношение является отношением эквивалентности на $L_P(F)$ и $L_P(F)^*$. Выберем и зафиксируем ненулевые ЛРП $u_0, \ldots, u_{d-1} \in L_P(F)$ так, чтобы $u_k \nsim u_l$ для всех $0 \leqslant k < l \leqslant d-1$. В силу того, что $T(u_0) = \cdots = T(u_{d-1}) = T(F)$, векторы

$$(u_0(i), \ldots, u_0(i+m-1)), \ldots, (u_{d-1}(i), \ldots, u_{d-1}(i+m-1)), \quad i = 0, 1, \ldots, T(F)-1,$$

пробегают все ненулевые векторы из множества P^m по одному разу.

Каждый элемент $a \in R$ однозначно представляется в виде

$$a = a_0 + 2a_1 + \cdots + 2^{n-1}a_{n-1}, \tag{1}$$

где $a_i \in P$, $i = 0, 1, \ldots, n-1$. Рассмотрим отображения $\varkappa_i \colon R \to P$, $i = 0, \ldots, n-1$, действующие по правилу

$$\varkappa_i(a) = a_i,$$

где a_i определяются согласно равенству (1).

Выберем произвольные ЛРП $v_0, \ldots, v_{d-1} \in L_R(G)^*$ и построим булеву функцию $f \colon P^m \to P$ по следующему правилу:

$$\begin{gathered} f(0, \ldots, 0) = 0, \\ f(u_0(i), \ldots, u_0(i+m-1)) = \varkappa_{n-1}(v_0(i)), \\ \cdots \\ f(u_{d-1}(i), \ldots, u_{d-1}(i)) = \varkappa_{n-1}(v_{d-1}(i)), \end{gathered}$$

где $i = 0, 1, \ldots, T(F)-1$. В силу того, что ЛРП $u_0, \ldots, u_{d-1}$ считаются фиксированными, в дальнейшем будем использовать обозначение

$$f(\vec{x}) = f_{v_0, \ldots, v_{d-1}}(\vec{x}),$$

где $\vec{x} = (x_1, \ldots, x_m)$. Будем изучать класс булевых функций

$$D_m(F) = \{f_{v_0, \ldots, v_{d-1}} \mid v_0, \ldots, v_{d-1} \in L_R(G)^*\}.$$

Нас будут интересовать следующие вопросы:

(1) оценка расстояния Хэмминга $\rho(f, g)$ между функциями $f = f_{v_0, \ldots, v_{m-1}}$, $g = f_{v'_0, \ldots, v'_{m-1}} \in D_m(F)$,
(2) нахождение мощности класса $D_m(F)$,
(3) оценка нелинейности $\mathrm{nl}(f)$ для функции $f \in D_m(F)$,
(4) оценка веса $\|f\|$ для функции $f \in D_m(F)$,
(5) условие отсутствия в классе $D_m(F)$ аффинных булевых функций.

Отметим, что ранее при $d = 1$ данный класс функций изучался в [3–5]. Рассмотрение произвольного значения d приводит к обобщениям результатов этих работ. С другой стороны, вычислительные эксперименты с классом $D_m(F)$ показывают наличие в случае $d > 1$ неизвестных ранее булевых функций, имеющих более предпочтительные параметры (например, нелинейность и степень функции) для решения прикладных задач. Кроме того, в случае $d > 1$ удается построить класс сбалансированных булевых функций, который не удалось получить в [3–5].

2. Расстояние Хэмминга между функциями

Теорема 1. *Пусть* $v_0, \dots, v_{d-1}, v'_0, \dots, v'_{d-1} \in L_R(G)^*$ *и* $\bar{v}_k \neq \bar{v}'_k$ *для всех* $k = 0, 1, \dots, d-1$. *Тогда для функций* $f = f_{v_0,\dots,v_{d-1}}$, $g = f_{v'_0,\dots,v'_{d-1}}$ *выполняется соотношение*

$$|\rho(f,g) - 2^{m-1}| \leqslant \left(\frac{2}{\pi}\ln 2^{n-1} + 1\right)^2 (d2^{n-1} - 1)2^{\frac{m}{2}-1}.$$

Доказательство. Пусть $f = f_{v_0,\dots,v_{d-1}}$, $g = f_{v'_0,\dots,v'_{d-1}}$. Рассмотрим коэффициент кросс-корреляции:

$$C(f,g) = \sum_{\vec{x}\in P^m} (-1)^{f(\vec{x})+g(\vec{x})}.$$

Так как

$$C(f,g) = |\{\vec{x}\colon f(\vec{x}) = g(\vec{x})\}| - |\{\vec{x}\colon f(\vec{x}) \neq g(\vec{x})\}| = 2^m - 2\rho(f,g),$$

то

$$|\rho(f,g) - 2^{m-1}| = \frac{|C(f,g)|}{2}. \tag{2}$$

Оценим $C(f,g)$. Имеем

$$C(f,g) = 1 + \sum_{k=0}^{d-1}\sum_{i=0}^{T(F)-1} (-1)^{\varkappa_{n-1}(v_k(i))+\varkappa_{n-1}(v'_k(i))}$$
$$= 1 + \sum_{k=0}^{d-1}\sum_{i=0}^{T(F)-1} (-1)^{\varkappa_{n-1}(v_k(i))}(-1)^{\varkappa_{n-1}(v'_k(i))}.$$

Отображение $\mu\colon R \to \mathbb{C}^*$, действующее по правилу

$$\mu(a) = (-1)^{\varkappa_{n-1}(a)}, \quad a \in R,$$

разложим (см. [6], [7]) по базису характеров группы $(R, +)$:

$$\mu(x) = \sum_{j=0}^{2^n-1} \nu_j \chi_j(x), \quad x \in R, \tag{3}$$

где

$$\chi_j(x) = e^{2\pi i \frac{jx}{2^n}}, \quad x \in R,$$

а ν_j, $j = 0, \dots, 2^n - 1$, — однозначно определенные комплексные числа, которые вычисляются по формуле

$$\nu_j = \frac{1}{2^n}\sum_{b\in R} \mu(b)\chi_j(b).$$

Согласно [8] $\nu_j = 0$ при всех четных значениях j и

$$\sum_{j=0}^{2^n-1} |\nu_j| \leqslant \frac{2}{\pi}\ln 2^{n-1} + 1. \tag{4}$$

С использованием равенства (3) получим

$$C(f,g) = 1 + \sum_{k=0}^{d-1} \sum_{i=0}^{T(F)-1} \sum_{j=0}^{2^n-1} \nu_j \chi_j(v_k(i)) \sum_{s=0}^{2^n-1} \nu_s \chi_s(v'_k(i)),$$

а значит,

$$C(f,g) = 1 + \sum_{k=0}^{d-1} \sum_{j,s=0}^{2^n-1} \nu_j \nu_s \sum_{i=0}^{T(F)-1} \chi(jv_k(i) + sv'_k(i)), \tag{5}$$

где $\chi = \chi_1$. Как было указано выше, достаточно рассмотреть суммирование только по нечетным значениям j и s. В этом случае последовательность $\omega_{j,s}$, элементы которой задаются равенством

$$\omega_{j,s}(i) = jv_k(i) + sv'_k(i), \quad i \geqslant 0,$$

является ЛРП из $L_R(G)$, причем последовательность $\overline{\omega}_{j,s}$, полученная из ЛРП $\omega_{j,s}$ заменой каждого ее элемента на остаток при делении на 2, является ЛРП с элементами

$$\overline{\omega}_{j,s}(i) = \overline{v}_k(i) + \overline{v}'_k(i), \quad i \geqslant 0.$$

В силу соотношения $\overline{v}_k \neq \overline{v}'_k$, $k = 0, \ldots, d-1$, будет выполняться включение $\omega_{j,s} \in L_R(G)^*$. Как показано в [9],

$$\left| \sum_{i=0}^{T(F)-1} \chi(\omega_{j,s}(i)) + \frac{1}{d} \right| \leqslant \frac{d2^{n-1}-1}{d} 2^{\frac{m}{2}}. \tag{6}$$

Из формулы (5) имеем

$$C(f,g) = 1 + \sum_{k=0}^{d-1} \sum_{j,s \notin 2R} \nu_j \nu_s \left(\sum_{i=0}^{T(F)-1} \chi(\omega_{j,s}(i)) + \frac{1}{d} \right) - \frac{1}{d} \sum_{k=0}^{d-1} \sum_{j,s \notin 2R} \nu_j \nu_s.$$

Из равенства (3) получаем

$$\sum_{k=0}^{d-1} \sum_{j,s \notin 2R} \nu_j \nu_s = d \sum_{j \notin 2R} \nu_j \sum_{s \notin 2R} \nu_s = d \sum_{j=0}^{2^n-1} \nu_j \sum_{s=0}^{2^n-1} \nu_s = d\mu(0)\mu(0) = d,$$

следовательно,

$$C(f,g) = \sum_{k=0}^{d-1} \sum_{j,s \notin 2R} \nu_j \nu_s \left(\sum_{i=0}^{T(F)-1} \chi(\omega_{j,s}(i)) + \frac{1}{d} \right),$$

и, используя (6), получим

$$|C(f,g)| \leqslant \sum_{k=0}^{d-1} \left(\sum_{j \notin 2R} |\nu_j| \right) \left(\sum_{s \notin 2R} |\nu_s| \right) \frac{d2^{n-1}-1}{d} 2^{\frac{m}{2}}.$$

Значит, согласно (4),

$$|C(f,g)| \leqslant \left(\frac{2}{\pi} \ln 2^{n-1} + 1 \right)^2 (d2^{n-1} - 1) 2^{\frac{m}{2}}.$$

Остается воспользоваться равенством (2). □

3. Мощность исследуемого класса функций

Получим оценки мощности класса $D_m(F)$.

Утверждение 1. *Справедливы оценки*

$$(2^{mn} - 2^{(n-1)m})^d \geqslant |D_m(F)| \geqslant (2^m - 1)^d.$$

Доказательство. Так как $D_m(F) = \{f_{v_0,\dots,v_{d-1}} \colon v_0, \dots, v_{d-1} \in L_R^*(G)\}$, то мощность класса $D_m(F)$ не больше величины $|L_R^*(G)|^d$, которая равна $(2^{mn} - 2^{(n-1)m})^d$. Рассмотрим множество

$$M = \{(\varkappa_{n-1}(r_1), \dots, \varkappa_{n-1}(r_m)) \colon (r_1, \dots, r_m) \in R^m \backslash (pR)^m\}.$$

Ясно, что $|D_m(F)| \geqslant |M|^d$. Зададим на множестве R^m бинарное отношение $\sim$ по правилу: $\vec{a} \sim \vec{b}$ для $\vec{a} = (a_1, \dots, a_m)$, $\vec{b} = (b_1, \dots, b_m) \in R^m$ тогда и только тогда, когда $(\varkappa_{n-1}(a_1), \dots, \varkappa_{n-1}(a_m)) = (\varkappa_{n-1}(b_1), \dots, \varkappa_{n-1}(b_m))$. Данное отношение является отношением эквивалентности на R^m. Отображение $\varkappa_{n-1} \colon R \to P$ является сбалансированным, т. е. при каждом $a \in P$ уравнение $\varkappa_{n-1}(x) = a$ имеет ровно $|R|/|P| = 2^{n-1}$ решений относительно неизвестного $x \in R$ (см. [10]). Следовательно, множество R^m разбивается на 2^m классов эквивалентности мощности $2^{(n-1)m}$. Поэтому

$$|M| \geqslant \frac{|R^m \backslash (pR)^m|}{2^{(n-1)m}} = \frac{2^{mn} - 2^{m(n-1)}}{2^{m(n-1)}} = 2^m - 1.$$

Таким образом, $|D_m(F)| \geqslant (2^m - 1)^d$. □

Приведем условия достижимости верхней оценки.

Утверждение 2. *Пусть $G(x)$ — отмеченный многочлен степени m над кольцом $R = \mathbb{Z}_{2^n}$, $T(G) = (2^m - 1)/d \geqslant 2^{n-1}(2^n - 1)2^{m/2}$. Тогда в классе функций $D_m(F)$ все функции различны и имеет место равенство*

$$|D_m(F)| = (2^{mn} - 2^{(n-1)m})^d.$$

Доказательство. Из результатов [11] следует, что если в каждой ЛРП $v \in L_R(G)^*$ появляются все элементы кольца R, то $\varkappa_{n-1}(v_1) \neq \varkappa_{n-1}(v_2)$ для любых различных ЛРП $v_1, v_2 \in L_R(G)^*$. Остается заметить, что если $T(G) = (2^m - 1)/d \geqslant 2^{n-1}(2^n - 1)2^{m/2}$, то в каждой ЛРП $v \in L_R(G)^*$ появляются все элементы кольца R (см. [12, следствие 5]). □

4. Оценка нелинейности

Пусть $\mathrm{nl}(g)$ — нелинейность (см., например, [13]) булевой функции g от m переменных, определенная равенством

$$\mathrm{nl}(g) = 2^{m-1} - \frac{1}{2} \max_{\vec{a} \in P^m} |W_g(\vec{a})|,$$

где $W_g(\vec{a})$ — коэффициент Уолша–Адамара функции g. Величина $\mathrm{nl}(g)$ равна расстоянию Хэмминга от функции g до класса всех аффинных булевых функций от m переменных.

Теорема 2. *Пусть* $f \in D_m(F)$, $n > 1$. *Тогда*

$$\mathrm{nl}(f) \geqslant 2^{m-1} - \left(\frac{2}{\pi}\ln 2^{n-1} + 1\right)(d2^{n-1} - 1)2^{\frac{m}{2}-1}.$$

Доказательство. Пусть $f = f_{v_0,\ldots,v_{d-1}}$, $\vec{a} \in P^m$. Рассмотрим коэффициент Уолша-Адамара $W_f(\vec{a})$:

$$W_f(\vec{a}) = \sum_{\vec{c}\in P^m} (-1)^{a_1c_1+\cdots+a_mc_m+f(\vec{c})}$$
$$= 1 + \sum_{k=0}^{d-1}\sum_{i=0}^{\frac{2^m-1}{d}-1} (-1)^{a_1u_k(i)+\cdots+a_mu_k(i+m-1)+f(u_k(i),\ldots,u_k(i+m-1))}.$$

Учитывая равенство $(-1)^x = \chi(2^{n-1}x)$, $x \in P$, имеем

$$W_f(\vec{a}) = 1 + \sum_{k=0}^{d-1}\sum_{i=0}^{\frac{2^m-1}{d}-1} \chi(2^{n-1}(a_1u_k(i) + \cdots + a_ku_k(i+m-1)))(-1)^{\varkappa_{n-1}(v_k(i))}$$
$$= 1 + \sum_{k=0}^{d-1}\sum_{i=0}^{\frac{2^m-1}{d}-1} \chi(2^{n-1}(a_1u_k(i) + \cdots + a_ku_k(i+m-1)))\sum_{j=0}^{2^n-1}\nu_j\chi_j(v_k(i))$$
$$= \sum_{j=0}^{2^n-1}\nu_j + \sum_{j=0}^{2^n-1}\nu_j\sum_{k=0}^{d-1}\sum_{i=0}^{\frac{2^m-1}{d}-1}\chi\left(\sum_{l=0}^{m-1}2^{n-1}a_{l+1}u_k(i+l) + jv_k(i)\right)$$
$$= \sum_{j=0}^{2^n-1}\nu_j\left(\sum_{k=0}^{d-1}\sum_{i=0}^{\frac{2^m-1}{d}-1}\chi(\delta^{(k)}_{a_1,\ldots,a_m,j}(i)) + 1\right)$$
$$= \sum_{j=0}^{2^n-1}\nu_j\left(\sum_{k=0}^{d-1}\left(\sum_{i=0}^{\frac{2^m-1}{d}-1}\chi(\delta^{(k)}_{a_1,\ldots,a_m,j}(i)) + \frac{1}{d}\right)\right),$$

где $\delta^{(k)}_{a_1,\ldots,a_m,j}$ — последовательность над кольцом R с элементами

$$\delta^{(k)}_{a_1,\ldots,a_m,j}(i) = jv_k(i) + 2^{n-1}a_1u_k(i) + \cdots + 2^{n-1}a_mu_k(i+m-1), \quad i \geqslant 0.$$

Заметим, что $\nu_j = 0$ для всех $j \in 2R$ (см. [5]). Поэтому достаточно ограничиться суммированием по всем обратимым элементам кольца R. При $n > 1$ последовательность $\delta_{a_1,\ldots,a_m,j}(k)$ будет ненулевой, так как $\varkappa_0(\delta^{(k)}_{a_1,\ldots,a_m,j}(i)) = \varkappa_0(jv_k(i))$, $k = 0,\ldots,d-1$, и последовательности jv_k, $k = 0,\ldots,d-1$, содержат хотя бы один обратимый элемент кольца R. Кроме того, последовательности $\delta^{(k)}_{a_1,\ldots,a_m,j}$, $k = 0,\ldots,d-1$, являются последовательностями с характеристическим многочленом $G(x)$. Значит, в силу оценки (6)

$$|W_f(\vec{a})| \leqslant \left(\sum_{j=0}^{2^n-1}|\nu_j|\right)(d2^{n-1} - 1)2^{\frac{m}{2}} \leqslant \left(\frac{2}{\pi}\ln 2^{n-1} + 1\right)(d2^{n-1} - 1)2^{\frac{m}{2}}. \qquad (7)$$

Таким образом,

$$\mathrm{nl}(f) \geqslant 2^{m-1} - \left(\frac{2}{\pi}\ln 2^{n-1} + 1\right)(d2^{n-1} - 1)2^{\frac{m}{2}-1}. \qquad \square$$

Следствие 1. *Пусть выполнены условия теоремы* 2, $n > 1$ *и*

$$m > 2\log_2\left(\left(\frac{2}{\pi}\ln 2^{n-1} + 1\right)(d2^{n-1} - 1)\right).$$

Тогда в классе $D_m(F)$ *нет аффинных функций.*

Доказательство. Если в классе функций $D_m(F)$ есть аффинная функция, то существует такой вектор $\vec{b} \in P^m$, что $|W_f(\vec{b})| = 2^m$. С другой стороны, в силу оценки (7) имеем

$$|W_f(\vec{b})| \leqslant \left(\frac{2}{\pi}\ln 2^{n-1} + 1\right)(d2^{n-1} - 1)2^{\frac{m}{2}}.$$

Следовательно,

$$2^m \leqslant \left(\frac{2}{\pi}\ln 2^{n-1} + 1\right)(d2^{n-1} - 1)2^{\frac{m}{2}},$$

что противоречит выбору n, d и m. $\square$

Следствие 2. *В условиях теоремы* 2 *справедливо неравенство*

$$|\|f\| - 2^{m-1}| \leqslant \left(\frac{2}{\pi}\ln 2^{n-1} + 1\right)(d2^{n-1} - 1)2^{m/2}.$$

Доказательство. Справедлива цепочка равенств

$$W_f(\vec{0}) = \sum_{\vec{x}\in P^m}(-1)^{f(\vec{x})} = |\{\vec{x}\colon f(\vec{x}) = 0\}| - |\{\vec{x}\colon f(\vec{x}) = 1\}| = 2^m - 2|\vec{x}\colon f(\vec{x}) = 1| = 2^m - 2\|f\|.$$

Отсюда, согласно доказательству теоремы 2, следует, что

$$|\|f\| - 2^{m-1}| \leqslant \left(\frac{2}{\pi}\ln 2^{n-1} + 1\right)(d2^{n-1} - 1)2^{\frac{m}{2}-1}. \qquad \square$$

5. Результаты вычислительных экспериментов

Для изучения свойств функций класса

$$D_m(F) = \{f_{v_0,\ldots,v_{d-1}}\colon v_0, \ldots, v_{d-1} \in L_R(G)^*\}$$

были проведены вычислительные эксперименты, которые показали наличие функций в исследуемом классе с более интересными параметрами по сравнению с функциями из [5]. В частности:

(1) найдены сбалансированные функции в следующих случаях:
при $d = 3$, $n = 2$ $G(x) = x^8 + 3x^7 + 2x^6 + 3x^5 + 2x^3 + 3x + 1$,
при $d = 3$, $n = 3$ $G(x) = x^8 + 3x^7 + 2x^6 + 3x^5 + 4x^4 + 6x^3 + 4x^2 + 7x + 1$,
при $d = 3$, $n = 4$ $G(x) = x^8 + 11x^7 + 10x^6 + 11x^5 + 4x^4 + 6x^3 + 4x^2 + 7x + 1$,
при $d = 5$, $n = 2$ $G(x) = x^8 + 2x^6 + 3x^4 + 3x^3 + 3x + 1$,
при $d = 5$, $n = 3$ $G(x) = x^8 + 4x^7 + 2x^6 + 4x^5 + 3x^4 + 3x^3 + 4x^2 + 7x + 1$,
при $d = 5$, $n = 4$ $G(x) = x^8 + 4x^7 + 10x^6 + 12x^5 + 11x^4 + 11x^3 + 12x^2 + 7x + 1$,

(2) при $d = 3$, $n = 2$, $G(x) = x^6 + 2x^5 + 3x^4 + 3x^2 + x + 1$ найдено 8 бент-функций степени 3 (ранее при $d = 1$ были построены только квадратичные бент-функции от 6 переменных);

(3) при $d = 3$, $n = 3$, $G(x) = x^6 + 3x^5 + 7x^4 + 7x^2 + 2x + 1$ найдено 425 функций степени 6 (ранее при $d = 1$ были построены только функции со степенью 4);

(4) при $d = 3$, $n = 3$, $G(x) = x^6 + 2x^5 + 7x^4 + 7x^2 + 5x + 1$ найдено 2 функции с большей степенью, чем в случае $d = 1$, при таких же значениях других параметров.

Список литературы

1. Лидл Р., Ниддерайтер Г., *Конечные поля*, т. 1,2, М.: Мир, 1988, 822 с.
2. Нечаев А. А., "Цикловые типы линейных подстановок над конечными коммутативными кольцами", *Матем. сборник*, **183**:3 (1993), 21–56.
3. Былков Д. Н., Камловский О. В., "Параметры булевых функций, построенных с использованием старших координатных последовательностей линейных рекуррент", *Матем. вопр. криптогр.*, **3**:4 (2012), 25–53.
4. Былков Д. Н., "Об одном классе булевых функций, построенных с использованием старших разрядных последовательностей линейных рекуррент", *ПДМ. Приложение*, 2014, №7, 59–60.
5. Бугров А. Д., Камловский О. В., "Параметры одного класса линейных функций, заданных на конечном поле", *Матем. вопр. криптогр.*, **9**:4 (2018), 35–52.
6. Солодовников В. И., "Бент-функции из конечной абелевой группы в конечную абелеву группу", *Дискретная математика*, **14**:1 (2000), 99–113.
7. Камловский О. В., "Спектральный метод оценки числа решений систем нелинейных уравнений с линейными рекуррентными аргументами", *Дискретная математика*, **28**:2 (2016), 27–43.
8. Камловский О. В., "Метод тригонометрических сумм для исследования частот r-грамм в старших координатных последовательностях линейных рекуррент над кольцом $\mathbb{Z}_{2^n}$", *Матем. вопр. криптогр.*, **1**:4 (2010), 33–62.
9. Камловский О. В., Кузьмин А. С., "Оценки частот появления элементов в линейных рекуррентных последовательностях над кольцами Галуа", *Фундамент. и прикл. матем.*, **6**:4 (2000), 1083–1094.
10. *Словарь криптографических терминов*, ред. Погорелов Б. А., Сачков В. Н., М.: МЦНМО, 2006, 92 с.
11. Былков Д. Н., "Класс усложнений линейных рекуррент над кольцом Галуа, не приводящий к потере информации", *Проблемы передачи информации*, **46**:3 (2010), 51–59.
12. Камловский О. В., "Частотные характеристики линейных рекуррентных последовательностей над кольцами Галуа", *Матем. сборник*, **200**:4 (2009), 31–52.
13. Логачёв О. А., Сальников А. А., Ященко В. В., *Булевы функции в теории кодирования и криптологии*, М.: МЦНМО, 2004, 470 с.

Статья поступила 16.11.2022.