Math-Net.Ru

Общероссийский математический портал

О. В. Камловский, Частотные характеристики разрядных последовательностей линейных рекуррент над кольцами Галуа, *Изв. РАН. Сер. матем.*, 2013, том 77, выпуск 6, 71–96

DOI: <https://doi.org/10.4213/im7799>

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: 3.95.254.165

26 апреля 2023 г., 13:26:21

УДК 519.4

О. В. Камловский

Частотные характеристики разрядных последовательностей линейных рекуррент над кольцами Галуа

Рассматриваются некоторые свойства разрядных последовательностей линейных рекуррент над кольцами Галуа, которые характеризуют возможность их использования в качестве псевдослучайных последовательностей. Изучаются периодические свойства, линейная сложность и частотные характеристики рассматриваемых последовательностей. Ранее данные параметры изучались преимущественно в ситуации, когда линейная рекуррентная последовательность имела максимально возможный период. Исследуются разрядные последовательности линейных рекуррент не обязательно максимального периода. Получены оценки числа элементов и r -грамм на циклах и отрезках разрядных последовательностей, которые уточняют и обобщают ранее известные оценки.

Библиография: 27 наименований.

Ключевые слова: кольца Галуа, линейные рекуррентные последовательности, распределение элементов в последовательностях, разрядные последовательности, тригонометрические суммы.

DOI: 10.4213/im7799

Введение

С целью полноты изложения приведем некоторые сведения из теории колец Галуа (см., например, [1], [2]). *Кольцом Галуа* называется конечное коммутативное кольцо R с единицей e , в котором множество всех делителей нуля имеет вид pR для некоторого простого числа p . Каждое кольцо Галуа R имеет характеристику p^n и состоит из q^n элементов, где $q = p^t$, $n, t \in \mathbb{N}$. Примерами колец Галуа являются примарное кольцо вычетов $\mathbb{Z}_{p^n} = \{0, 1, \dots, p^n - 1\}$ и конечное поле $\text{GF}(q)$. Факторкольцо $\bar{R} = R/pR$ кольца R по идеалу pR является полем из q элементов. Назовем унитарный многочлен $F(x) \in R[x]$ *многочленом Галуа над кольцом R* , если его образ $\bar{F}(x)$ при действии естественного эпиморфизма колец $R[x] \rightarrow \bar{R}[x]$ неприводим над полем $\bar{R}$. Кольцо Галуа R , имеющее характеристику p^n и состоящее из q^n элементов, изоморфно кольцу $\mathbb{Z}_{p^n}[x]/F(x)$, где $F(x) \in \mathbb{Z}_{p^n}[x]$ – произвольный многочлен Галуа степени t над кольцом $\mathbb{Z}_{p^n}$. В связи с этим для рассматриваемого кольца R используется обозначение $R = \text{GR}(q^n, p^n)$.

Разрядным множеством кольца R называется любое его подмножество $K = \{k_0, k_1, \dots, k_{q-1}\}$ такое, что все его элементы попарно не сравнимы по

Работа выполнена при финансовой поддержке Программы Президента РФ “Поддержка ведущих научных школ России” (грант НШ-4.2010.10).

идеалу pR (см., например, [3]). Примером разрядного множества кольца R является так называемое p -адическое множество $K = \Gamma(R)$, состоящее из всех элементов $r \in R$ таких, что $r^q = r$. Это множество замкнуто относительно умножения в кольце R и является циклической группой. В кольце $\mathbb{Z}_{p^n}$ часто рассматривают так называемое p -ичное разрядное множество $K = \{0, 1, \dots, p-1\}$. В случае $p = 2$ p -адическое и p -ичное разрядные множества совпадают. Число всех разрядных множеств кольца R равно $|pR|^q = q^{q(n-1)}$.

Если K – разрядное множество кольца R , то каждый элемент $a \in R$ однозначно представим в виде

$$a = a_0 + pa_1 + p^2a_2 + \dots + p^{n-1}a_{n-1}, \quad (1)$$

где $a_i \in K$, $i = 0, 1, \dots, n-1$. Равенство (1) называется *разрядным представлением* элемента a в разрядном множестве K , а элемент a_s , где $s = 0, 1, \dots, n-1$, называется s -м *разрядом* элемента a в разрядном множестве K . При этом элемент a_{n-1} называется *старшим разрядом*. Для каждого $s \in \{0, \dots, n-1\}$ рассмотрим отображение $\varkappa_s^K: R \rightarrow K$, осуществляемое для всех $a \in R$ по правилу

$$\varkappa_s^K(a) = a_s.$$

Зададим на множестве K бинарные операции $\oplus$ и $\otimes$ по правилам

$$a \oplus b = \varkappa_0^K(a + b), \quad a \otimes b = \varkappa_0^K(ab)$$

для всех $a, b \in K$. Тогда алгебра $(K, \oplus, \otimes)$ будет полем из q элементов.

Пусть $u = (u(i))_{i=0}^\infty$ – последовательность над кольцом R , K – разрядное множество кольца R . Для каждого $s \in \{0, \dots, n-1\}$ рассмотрим последовательность u_s над полем K , полученную из последовательности u по правилу

$$u_s(i) = \varkappa_s^K(u(i)), \quad i \geq 0.$$

Последовательность u_s будем называть s -й *разрядной последовательностью* последовательности u в разрядном множестве K и в этом случае будем использовать обозначение $u_s = \varkappa_s^K(u)$.

Назовем последовательность u элементов кольца R *линейной рекуррентной последовательностью* (ЛРП) порядка m над кольцом R , если для некоторых элементов $a_0, a_1, \dots, a_{m-1}$ кольца R выполнены равенства

$$u(i+m) = a_0u(i) + a_1u(i+1) + \dots + a_{m-1}u(i+m-1), \quad i \geq 0.$$

В этом случае многочлен

$$F(x) = x^m - a_{m-1}x^{m-1} - \dots - a_1x - a_0$$

называется *характеристическим многочленом* ЛРП u (см., например, [3], [4]). В случае, когда u – ЛРП над кольцом R , старшую разрядную последовательность $u_{n-1} = \varkappa_{n-1}^K(u)$ часто рассматривают как усложнение последовательности u .

Последовательность u_{n-1} изучалась многими авторами (см., например, работы [3]–[18]). Результаты этих исследований показали, что последовательность u_{n-1} , полученная из ЛРП u максимального периода над кольцом $\mathbb{Z}_{p^n}$, пригодна для использования в качестве псевдослучайной последовательности.

В настоящей работе будут проведены дальнейшие исследования последовательности u_{n-1} , соответствующей ЛРП u над кольцом Галуа $R = \text{GR}(q^n, p^n)$. Основное внимание будет уделяться вопросам распределения элементов и r -грамм на отрезках рассматриваемой последовательности при условии, что характеристический многочлен $F(x)$ ЛРП u является многочленом Галуа (в частности, многочленом максимального периода) над кольцом R .

В § 1 по аналогии с результатами работы [3] будет показано, что практически всегда период последовательности u_{n-1} совпадает с периодом последовательности u . Кроме того, доказываются некоторые оценки снизу линейной сложности последовательности u_{n-1} . В § 2 получены оценки тригонометрических сумм от ЛРП, этот параграф носит вспомогательный характер. Здесь уточняются результаты работы [19], где были получены оценки сумм значений аддитивного характера кольца Галуа R от ЛРП u . Отметим, что классический метод из работы [20] (см. также [21, неравенства (117)]) в случае, когда R не является полем, устанавливает для таких сумм тривиальные оценки. В § 3 приводятся оценки частот появлений r -грамм на циклах и отрезках последовательности u_{n-1} . Полученные результаты справедливы и в более общей ситуации, когда вместо отображения χ_{n-1}^K рассматривается произвольное сбалансированное отображение $\Psi: R \rightarrow K$. Применительно к частному случаю, когда u – ЛРП максимального периода над кольцом $R = \mathbb{Z}_{p^n}$, оценки из § 3 при $m \geq 4n$ усиливают оценки снизу частот элементов на цикле ЛРП u_{n-1} , вытекающие из результатов работ [4, теорема 6.4] и [22, теорема 1]. В § 4 проведены исследования спектральных коэффициентов отображений, связанных с отображением χ_{n-1}^K и используемых при описании частотных характеристик последовательности u_{n-1} . В § 5 результаты из § 4 уточняются для случая, когда разрядное множество K кольца R образует арифметическую прогрессию. Именно такими являются все разрядные множества кольца $R = \mathbb{Z}_{2^n}$. В § 6 на основе результатов из § 4 и § 5 приводятся оценки для числа r -грамм на циклах и отрезках разрядных последовательностей ЛРП над кольцом $\mathbb{Z}_{p^n}$, уточняющие общие оценки из § 3. Оценки, доказанные в § 6, являются обобщением в случае произвольного p оценок из работы [9], где рассматривался случай $p = 2$ и были получены более точные оценки по сравнению с соответствующими оценками из работ [11]–[17]. Результаты, полученные в § 4–6, являются дальнейшим развитием спектрального метода исследования частотных характеристик разрядных последовательностей, впервые предложенного в работе [10].

§ 1. Период и ранг последовательности u_{n-1}

Пусть $R = \text{GR}(q^n, p^n)$, $F(x) \in R[x]$ – унитарный многочлен. Назовем многочлен $F(x)$ *реверсивным*, если для некоторого натурального числа t многочлен $F(x)$ делит $x^t - e$. Условие реверсивности $F(x)$ равносильно тому, что $F(0)$ – обратимый элемент кольца R . Известно (см., например, [23, утверждение 4.1]), что период $T(F)$ многочлена $F(x)$ связан с периодом многочлена $\bar{F}(x)$ соотношением $T(F) = p^{n-\lambda} T(\bar{F})$, где $\lambda \in \{1, \dots, n\}$. Обозначим через $\equiv$ отношение сравнимости многочленов из кольца $R[x]$ по модулю многочлена $F(x)$. В дальнейшем нам понадобится следующая лемма, доказательство которой аналогично доказательству, предложенному в работе [24, лемма 2, с. 345].

ЛЕММА 1. *Предположим, что $F(x)$ – реверсивный многочлен над кольцом $R = \text{GR}(q^n, p^n)$, $T(F) = p^{n-\lambda}\tau_0$, где $\tau_0 = T(\bar{F})$, $\lambda \in \{1, \dots, n-1\}$. Тогда для всех $k \in \{1, \dots, n-\lambda-1\}$ справедливы соотношения*

$$x^{p^k\tau_0} \stackrel{F}{\equiv} e + p^{\lambda+k}\Phi_{k+1}(x),$$

где $\Phi_{k+1}(x) \in R[x]$, $\deg \Phi_{k+1}(x) < m$, $\bar{\Phi}_{k+1}(x) \neq \bar{0}$. При этом если $p > 2$ или $p = n = 2$, то

$$x^{\tau_0} \stackrel{F}{\equiv} e + p^\lambda\Phi_1(x),$$

а если $p = 2$, $n > 2$, то возможен один из следующих вариантов:

а) $x^{\tau_0} \stackrel{F}{\equiv} e + 2^\lambda\Phi_1(x)$, $\lambda \geq 2$,

б) $x^{\tau_0} \stackrel{F}{\equiv} e + 2\Phi_1(x)$,

где $\Phi_1(x) \in R[x]$, $\deg \Phi_1(x) < m$, $\bar{\Phi}_1(x) \neq \bar{0}$.

Изучим периоды разрядных последовательностей ЛРП u над кольцом R . Будем использовать обозначение $\bar{u}$ для последовательности над полем $\bar{R} = R/pR$, полученной из последовательности u заменой всех элементов на образы при действии естественного эпиморфизма колец $R \rightarrow \bar{R}$. Образ элемента $r \in R$ при действии этого эпиморфизма обозначим $\bar{r}$. Если u – последовательность над разрядным множеством K кольца R , то, очевидно, имеет место равенство $T(u) = T(\bar{u})$. Кроме того, определим произведение многочлена $\bar{a}(x) = \sum_{i=0}^l \bar{a}_i x^i \in \bar{R}[x]$ на последовательность $u \in K^\infty$ по правилу

$$\bar{a}(x)u = \varkappa_0^K(a_0u) \oplus \varkappa_0^K(a_0xu) \oplus \dots \oplus \varkappa_0^K(a_lx^lu).$$

Несложно заметить, что многочлен $\bar{a}(x)$ аннулирует ЛРП $u \in K^\infty$ тогда и только тогда, когда этот многочлен аннулирует ЛРП $\bar{u}$. Обозначим через $M_u(x)$ минимальный многочлен последовательности u из кольца $\bar{R}[x]$. Он будет совпадать с минимальным многочленом $M_{\bar{u}}(x)$ ЛРП $\bar{u}$. Степень многочлена $M_u(x)$ назовем *рангом (линейной сложностью)* последовательности u и обозначим $\text{rank } u$.

Докажем по аналогии с результатами из работы [3, теорема 1.3] следующую теорему.

ТЕОРЕМА 1. *Пусть $F(x)$ – реверсивный многочлен Галуа степени m над кольцом $R = \text{GR}(q^n, p^n)$, $T(F) = p^{n-\lambda}\tau_0$, где $\tau_0 = T(\bar{F})$, $1 \leq \lambda < n$, u – ЛРП над кольцом R с характеристическим многочленом $F(x)$, $\bar{u} \neq (\bar{0})$, K – разрядное множество кольца R , $u_s = \varkappa_s^K(u)$, $s = 0, 1, \dots, n-1$. Тогда:*

1) *при $p > 2$ или $p = n = 2$*

$$\begin{aligned} T(u_0) &= \tau_0, & T(u_r) &\mid \tau_0, & r &= 1, 2, \dots, \lambda-1, \\ T(u_{\lambda+k}) &= p^{k+1}\tau_0, & k &= 0, 1, \dots, n-\lambda-1; \end{aligned}$$

2) *при $p = 2$ и $n > 2$ возможны два случая:*

$$\begin{aligned} T(u_0) &= \tau_0, & T(u_r) &\mid \tau_0, & r &= 1, 2, \dots, \lambda-1, \\ T(u_{\lambda+k}) &= 2^{k+1}\tau_0, & k &= 0, 1, \dots, n-\lambda-1; \end{aligned} \tag{2}$$

$$\begin{aligned} T(u_0) &= \tau_0, & T(u_1) &= 2\tau_0, & T(u_t) &\mid 2\tau_0, & t &= 2, \dots, \lambda, \\ T(u_{\lambda+k}) &= 2^{k+1}\tau_0, & k &= 1, 2, \dots, n-\lambda-1. \end{aligned} \tag{3}$$

ДОКАЗАТЕЛЬСТВО. Заметим сначала, что равенство $F(x)u = (0)$ влечет равенство $\bar{F}(x)\bar{u} = (\bar{0})$. Это по условию означает, что $\bar{u} = \bar{u}_0$ – ненулевая ЛРП с неприводимым характеристическим многочленом $\bar{F}(x)$. Значит, $T(u_0) = T(\bar{F}) = \tau_0$.

1. Пусть $p > 2$ либо $p = n = 2$. Методом математической индукции по параметру $r \in \{1, \dots, \lambda - 1\}$ покажем, что $T(u_r) \mid \tau_0$. При $r = 1$ из соотношений $x^{\tau_0} \stackrel{F}{\equiv} e + p^\lambda \Phi_1(x)$, $T(u_0) = \tau_0$ получим

$$\begin{aligned} (x^{\tau_0} - e)u &= (x^{\tau_0} - e)(pu_1 + p^2u_2 + \dots + p^{n-1}u_{n-1}) \\ &= (x^{\tau_0} - e)pu_1 + p^2v = p^\lambda \Phi_1(x)u, \end{aligned}$$

где v – некоторая последовательность над кольцом R . Отсюда получим $(x^{\tau_0} - \bar{e})\bar{u}_1 = (\bar{0})$, а значит, $T(u_1) \mid \tau_0$. Пусть доказываемое утверждение верно при всех $r = 1, 2, \dots, t - 1$. Докажем его при $r = t < \lambda$. С использованием предположения индукции и равенства $x^{\tau_0} \stackrel{F}{\equiv} e + p^\lambda \Phi_1(x)$ получим

$$\begin{aligned} (x^{\tau_0} - e)u &= (x^{\tau_0} - e)(p^t u_t + p^{t+1} u_{t+1} + \dots + p^{n-1} u_{n-1}) \\ &= (x^{\tau_0} - e)p^t u_t + p^{t+1} \omega = p^\lambda \Phi_1(x)u, \end{aligned}$$

где ω – некоторая последовательность над кольцом R . Отсюда получаем $(x^{\tau_0} - \bar{e})\bar{u}_t = (\bar{0})$, а значит, $T(u_t) \mid \tau_0$.

2. Пусть $p = 2$, $n > 2$. Согласно лемме 1 в этом случае

$$x^{\tau_0} \stackrel{F}{\equiv} e + 2^\lambda \Phi_1(x) \quad \text{либо} \quad x^{\tau_0} \stackrel{F}{\equiv} e + 2\Phi_1(x). \quad (4)$$

Если выполнено первое из соотношений (4), то, дословно повторяя доказательство из п. 1, получим $T(u_r) \mid \tau_0$ для всех $r \in \{1, \dots, \lambda - 1\}$. Пусть теперь справедливо второе из соотношений (4). С использованием равенства $T(u_0) = \tau_0$ получим

$$(x^{\tau_0} - e)u = (x^{\tau_0} - e)(2u_1 + 2^2u_2 + \dots + 2^{n-1}u_{n-1}) = 2\Phi_1(x)u.$$

Тогда $(x^{\tau_0} - \bar{e})\bar{u}_1 = \bar{\Phi}_1(x)\bar{u}$. Поскольку $\bar{\Phi}_1(x) \neq \bar{0}$, $\deg \Phi_1(x) < m$, то $\bar{\Phi}_1(x)\bar{u}$ – ненулевая ЛРП с характеристическим многочленом $\bar{F}(x)$. Тогда согласно [24, теорема 5, с. 304] имеем $M_{\bar{u}_1}(x) = \bar{F}(x)(x^{\tau_0} - \bar{e}, M_{\bar{u}_1}(x))$, а значит, многочлен $\bar{F}(x)^2$, имеющий период $2\tau_0$, делит $M_{\bar{u}_1}(x)$. С другой стороны, $(x^{2\tau_0} - \bar{e})\bar{u}_1 = (x^{\tau_0} - \bar{e})^2\bar{u}_1 = (\bar{0})$, значит, $T(u_1) = 2\tau_0$.

Теперь аналогично доказательству из п. 2 с использованием соотношения $x^{2\tau_0} - e \stackrel{F}{\equiv} 2^{\lambda+1}\Phi_2(x)$ несложно показать, что $T(u_t) \mid 2\tau_0$ для всех $t \in \{2, \dots, \lambda\}$.

3. Пусть $p > 2$ или $p = n = 2$. В этом случае методом математической индукции по $k \in \{0, \dots, n - \lambda - 1\}$ аналогично изложенному выше доказывается, что

$$\begin{aligned} (x^{p^k \tau_0} - \bar{e})\bar{u}_{\lambda+k} &= \bar{\Phi}_{k+1}(x)\bar{u}, & M_{\bar{u}_{\lambda+k}}(x) &= \bar{F}(x)(x^{\tau_0} - \bar{e}, M_{\bar{u}_{\lambda+k}}(x)), \\ \bar{F}(x)^{p^{k+1}} &\mid M_{\bar{u}_{\lambda+k}}(x), & T(u_{\lambda+k}) &= p^{k+1}\tau_0. \end{aligned}$$

4. Пусть $p = 2$, $n > 2$. Тогда если в условии леммы 1 имеет место случай а), то, дословно повторяя доказательство из п. 3, получим $T(u_{\lambda+k}) = 2^{k+1}\tau_0$, где $k = 0, 1, \dots, n - \lambda - 1$. Если в условии леммы 1 справедливо соотношение б), то, повторяя доказательство из п. 3, получим $T(u_{\lambda+k}) = 2^{k+1}\tau_0$, где $k = 1, 2, \dots, n - \lambda - 1$.

Отметим, что в теореме 1 не рассмотрен случай, когда $\lambda = n$, т. е. $T(F) = T(\bar{F}) = \tau_0$. В этом случае ясно, что $T(u_0) = \tau_0$, а периоды $T(u_1), \dots, T(u_{n-1})$ делят τ_0 . Кроме того, заметим, что, как правило, при $\lambda < n$ имеет место равенство $T(u_{n-1}) = p^{n-\lambda}\tau_0 = T(F)$. Исключение составляет случай, когда одновременно выполнены условия $p = 2$, $n > 2$, $\lambda = n - 1$ и многочлен $F(x)$ удовлетворяет условию б) леммы 1. В этом случае теорема 1 не позволяет установить равенство $T(u_{n-1}) = T(F)$.

СЛЕДСТВИЕ 1. В условиях теоремы 1 (за исключением случая, когда одновременно выполнены условия $p = 2$, $n > 2$, $\lambda = n - 1$, $x^{\tau_0} \stackrel{F}{\equiv} e + 2\Phi_1(x)$) имеют место соотношения

$$T(u_{n-1}) = T(F) = p^{n-\lambda}\tau_0, \quad \text{rank } u_{n-1} \geq m(p^{n-\lambda-1} + 1).$$

Таким образом, практически всегда для ЛРП u с характеристическим многочленом Галуа $F(x)$, содержащей среди элементов $u(0), u(1), \dots, u(m-1)$ хотя бы один обратимый элемент кольца R , последовательность $u_{n-1} = \varkappa_{n-1}^K(u)$ имеет период, равный $T(u)$. Кроме того, последовательность u_{n-1} обладает достаточно большой линейной сложностью, которая увеличивается экспоненциально с ростом параметра $n - \lambda$. В работе [3, теорема 1.3] было показано, что если u – ЛРП максимального периода $T(u) = p^{n-1}(q^m - 1)$ над кольцом $R = \text{GR}(q^n, p^n)$, то при всех $s \in \{0, 1, \dots, n-1\}$ для разрядной последовательности $u_s = \varkappa_s^K(u)$ выполнены соотношения

$$T(u_s) = p^s(q^m - 1), \quad \text{rank } u_s \geq m(p^{s-1} + 1).$$

Отметим, что оценка линейной сложности последовательности u_{n-1} , приведенная в следствии 1, является достаточно грубой для случая, когда $F(x)$ – многочлен максимального периода. На самом деле, если $R = \mathbb{Z}_{p^n}$, а K – разрядное множество кольца R , содержащее 0, то $\text{rank } u_{n-1} = O(m^{p^{n-1}})$ при $m \rightarrow \infty$ (см., например, [3, теорема 1.5], [4, теорема 5.2]).

СЛЕДСТВИЕ 2. Пусть $R = \mathbb{Z}_{p^n}$ в условиях теоремы 1. Тогда (за исключением случая, когда одновременно выполнены условия $p = 2$, $n > 2$, $\lambda = n - 1$, $x^{\tau_0} \stackrel{F}{\equiv} e + 2\Phi_1(x)$) в последовательности u_{n-1} появятся все элементы из множества K .

ДОКАЗАТЕЛЬСТВО. Из равенства

$$(x^{p^{n-\lambda-1}\tau_0} - \bar{e})\bar{u}_{n-1} = \bar{\Phi}_{n-\lambda}(x)\bar{u}$$

следует, что $\bar{u}_{n-1}(i + p^{n-\lambda-1}\tau_0) = \bar{u}_{n-1}(i) + \bar{\Phi}_{n-\lambda}(x)\bar{u}(i)$ для всех $i \geq 0$. Последовательность $v = \bar{\Phi}_{n-\lambda}(x)\bar{u}$ является ненулевой над полем $\bar{R}$. Пусть $v(s) \neq \bar{0}$; тогда справедливо равенство

$$\{u_{n-1}(s + jp^{n-\lambda-1}\tau_0) : j = 0, 1, \dots, p-1\} = K.$$

Следствие доказано.

Приведем результат из работы [8, следствие 1], показывающий, что при некоторых ограничениях периода многочлена $\bar{F}(x)$ разрядные последовательности различных ЛРП не совпадают.

ТЕОРЕМА 2. Пусть $F(x)$ – реверсивный многочлен Галуа степени m над кольцом $R = \text{GR}(q^n, p^n)$, $T(F) = p^\nu T(\bar{F})$, где $0 \leq \nu < n$, и пусть u, v – различные ЛРП над кольцом R с характеристическим многочленом $F(x)$, кроме того, K – разрядное множество кольца R , $u_{n-1} = \varkappa_{n-1}^K(u)$, $v_{n-1} = \varkappa_{n-1}^K(v)$. Тогда если выполнено неравенство

$$T(\bar{F}) \geq p^{n-1}(q^n - 1)q^{\frac{m}{2}},$$

то $u_{n-1} \neq v_{n-1}$.

В случае, когда $\bar{F}(x)$ – произвольный многочлен максимального периода, он будет удовлетворять условию теоремы 2 при всех значениях $m, n \in \mathbb{N}$ таких, что $m \geq 2(n + (n - 1) \log_q p)$. В частности, последнее неравенство выполнено при $m \geq 4n - 2$.

§ 2. Тригонометрические суммы от ЛРП

Пусть $R = \text{GR}(q^n, p^n)$, $F(x)$ – унитарный многочлен над кольцом R . Обозначим через $L_R(F)$ множество всех ЛРП над кольцом R с характеристическим многочленом $F(x)$, а через $L_R(F)^*$ подмножество множества $L_R(F)$, состоящее из всех ЛРП u , для которых $\bar{u} \neq (\bar{0})$. Рассмотрим аддитивный характер кольца R , определенный на элементах этого кольца равенством

$$\chi(x) = \exp \left\{ 2\pi i \frac{\text{Tr}_{R_0}^R(x)}{p^n} \right\}, \quad (5)$$

где $R_0 = \{0, e, 2e, \dots, (p^n - 1)e\}$, $\text{Tr}_{R_0}^R$ – функция следа из кольца R в кольцо R_0 . Далее понадобятся оценки для модуля суммы

$$S_l(v) = \sum_{i=0}^{l-1} \chi(v(i)), \quad (6)$$

где $l \in \mathbb{N}$, $v \in L_R(F)$.

УТВЕРЖДЕНИЕ 1 [19]. Если $F(x)$ – реверсивный многочлен Галуа степени m над кольцом $R = \text{GR}(q^n, p^n)$, $T(F) = p^\nu T(\bar{F}) = p^\nu(q^m - 1)/d$, $0 \leq \nu \leq n - 1$, $v \in L_R(F)$, $v \neq (0)$, χ – аддитивный характер кольца R , определенный равенством (5), то

$$\left| S_l(v) + \frac{p^\nu}{d} \right| \leq \frac{p^\nu(dp^{n-1} - 1)}{d} q^{\frac{m}{2}}.$$

ЛЕММА 2 [25]. Если $t, l \in \mathbb{N}$, $t \geq 2$, то

$$\frac{1}{t} \sum_{a=0}^{t-1} \left| \sum_{k=0}^{l-1} e^{-2\pi i \frac{ak}{t}} \right| < \frac{4}{\pi^2} \ln t + 0.38 + \frac{0.608}{t} + 0.116 \frac{d^2}{t^2} + \frac{l}{t},$$

где $d = (t, l)$. В частности, для всех $t, l \in \mathbb{N}$, $l \leq t$, справедлива более слабая оценка

$$\frac{1}{t} \sum_{a=0}^{t-1} \left| \sum_{k=0}^{l-1} e^{-2\pi i \frac{ak}{t}} \right| < \frac{4}{\pi^2} \ln t + \frac{9}{5}.$$

ЛЕММА 3. Пусть $F(x)$ – реверсивный многочлен Галуа степени m над кольцом $R = \text{GR}(q^n, p^n)$, $T(F) = T(\bar{F}) = t$, $v \in L_R(F)$, $v \neq (0)$, $l \in \mathbb{N}$, χ – характер кольца R , определенный равенством (5). Тогда для всех $l \leq T(F)$ выполнено неравенство

$$\left| \sum_{i=0}^{l-1} \chi(v(i)) \right| \leq p^{n-1} \left(\frac{4}{\pi^2} \ln t + \frac{9}{5} \right) q^{\frac{m}{2}}.$$

ДОКАЗАТЕЛЬСТВО. Достаточно повторить доказательство из [19, теорема 1] и воспользоваться оценкой из леммы 2.

УТВЕРЖДЕНИЕ 2. Пусть $F(x)$ – реверсивный многочлен Галуа степени m над кольцом $R = \text{GR}(q^n, p^n)$, $T(F) = p^\nu T(\bar{F})$, $0 \leq \nu \leq n-1$, $v \in L_R(F)$, $v \neq (0)$, и $l \in \mathbb{N}$, χ – характер кольца R , определенный равенством (5). Тогда для всех $l \leq T(F)$ выполнено неравенство

$$|S_l(v)| \leq p^{\nu+n-1} \left(\frac{4}{\pi^2} \ln T(\bar{F}) + \frac{9}{5} \right) q^{\frac{m}{2}}.$$

ДОКАЗАТЕЛЬСТВО. Рассмотрим последовательности v_s над кольцом R , определенные для всех $s = 0, 1, \dots, p^\nu - 1$ равенством

$$v_s(i) = v(s + p^\nu i), \quad i \geq 0.$$

Пусть представление ЛРП v с использованием функции следа имеет вид

$$v(i) = \text{Tr}_R^S(b\alpha^i),$$

где $S = \text{GR}(q^{mn}, p^n)$ – кольцо Галуа, являющееся расширением степени m кольца R , Tr_R^S – функция следа из кольца S в кольцо R , α – корень многочлена $F(x)$ в кольце S , b – ненулевой элемент кольца S . Поскольку $F(x)$ – реверсивный многочлен Галуа, α является обратимым элементом кольца S , причем порядок элемента α будет равен $T(F)$. Представление каждой ЛРП v_s с использованием функции следа будет следующим:

$$v_s(i) = v(s + p^\nu i) = \text{Tr}_R^S(b\alpha^s \alpha_0^i),$$

где $\alpha_0 = \alpha^{p^\nu}$ – элемент порядка $t = T(\bar{F})$. Элемент α_0 – корень некоторого реверсивного многочлена Галуа $G(x)$ степени m над кольцом R , причем $T(G) = T(\bar{G}) = T(\bar{F})$. Таким образом, при всех $s = 0, 1, \dots, p^\nu - 1$ последовательность v_s является ненулевой ЛРП с реверсивным характеристическим многочленом Галуа $G(x)$, для которого $T(G) = T(\bar{G}) = t$. Тогда, используя лемму 3, получим

$$|S_l(v)| \leq \sum_{s=0}^{p^\nu-1} \left| S_{\left[\frac{l-1-p^\nu s}{p^\nu}\right]}(v_s) \right| \leq p^{\nu+n-1} \left(\frac{4}{\pi^2} \ln t + \frac{9}{5} \right) q^{\frac{m}{2}}.$$

Утверждение доказано.

§ 3. Частотные характеристики разрядных последовательностей

Рассмотрим теперь вопрос о распределении элементов в старшей разрядной последовательности $\varkappa_{n-1}^K(u)$ ЛПП u в разрядном множестве K кольца $R = \text{GR}(q^n, p^n)$. Сформулируем более общую задачу. Пусть Ψ – произвольное отображение из множества R в поле $K = \text{GF}(q)$. Назовем отображение Ψ *сбалансированным*, если для каждого элемента $k \in K$ множество $\Psi^{-1}(k)$ его прообразов имеет мощность $|R|/q = q^{n-1}$. Отображение $\varkappa_{n-1}^K$ является сбалансированным. Более того, сбалансированным является каждое отображение Ψ , удовлетворяющее условию

$$\Psi(a) = g(a_{n-1}) \oplus \eta(a_0, a_1, \dots, a_{n-2}), \quad a \in K, \quad (7)$$

где g – произвольная подстановка на множестве K , $\eta: K^{n-1} \rightarrow K$, а элементы $a_0, a_1, \dots, a_{n-1}$ определены равенством (1). Такие отображения Ψ достаточно широко исследуются на пригодность в качестве функции усложнения (см., например, работы [6], [18] и цитированную в них литературу).

Для каждой последовательности u над кольцом R обозначим через $\omega = \Psi(u)$ последовательность элементов кольца R , задаваемую равенством

$$\omega(i) = \Psi(u(i)), \quad i \geq 0.$$

Рассмотрим последовательности $u_1, \dots, u_r$ над кольцом R . Пусть $\omega_1 = \Psi(u_1), \dots, \omega_r = \Psi(u_r)$, $l \in \mathbb{N}$, $\bar{z} \in K^r$. Обозначим через $N_l(\bar{z}, \omega_1, \dots, \omega_r)$ количество появлений вектора $\bar{z}$ среди r -грамм $(\omega_1(i), \dots, \omega_r(i))$, где $i = 0, 1, \dots, l-1$. В случае, когда последовательности $u_1, \dots, u_r$ являются сдвигами одной последовательности u , т. е. $u_1 = x^{s_1}u, \dots, u_r = x^{s_r}u$ для некоторых целых неотрицательных чисел $s_1, \dots, s_r$, величина $N_l(\bar{z}, \omega_1, \dots, \omega_r)$ равна количеству появлений вектора $\bar{z}$ среди r -грамм $(\Psi(u(i+s_1)), \dots, \Psi(u(i+s_r)))$, где $i = 0, 1, \dots, l-1$.

Назовем последовательности $u_1, \dots, u_r$ *линейно независимыми* над кольцом R , если для всех ненулевых векторов $\bar{c} = (c_1, \dots, c_r) \in R^r$ последовательность $c_1 u_1 + \dots + c_r u_r$ является ненулевой.

ТЕОРЕМА 3. Пусть $F(x)$ – реверсивный многочлен Галуа степени m над кольцом $R = \text{GR}(q^n, p^n)$, $T(F) = p^\nu(q^m - 1)/d$, $0 \leq \nu \leq n-1$, $u_1, \dots, u_r$ – линейно независимая система ЛПП из множества $L_R(F)$, $K = \text{GF}(q)$, $\Psi: R \rightarrow K$ – сбалансированное отображение, $\Psi(u_t) = \omega_t$, где $t = 1, 2, \dots, r$. Тогда для всех $\bar{z} = (z_1, \dots, z_r) \in K^r$ справедливы следующие оценки:

1) если $l \leq T(F)$, то

$$\left| N_l(\bar{z}, \omega_1, \dots, \omega_r) - \frac{l}{q^r} \right| \leq \frac{q^{nr} - 1}{q^r} \max_{v \in L_R(F), v \neq (0)} |S_l(v)|; \quad (8)$$

2) если $l = T(F)$, то

$$|N_l(\bar{z}, \omega_1, \dots, \omega_r) - \delta(\bar{z})| \leq \frac{q^{nr} - 1}{q^r} \max_{v \in L_R(F), v \neq (0)} \left| S_l(v) + \frac{p^\nu}{d} \right|, \quad (9)$$

где

$$\delta(\bar{z}) = \begin{cases} \frac{q^{m-r} - 1}{q^m - 1} T(F), & \text{если } \bar{z} = (\Psi(0), \dots, \Psi(0)), \\ \frac{q^{m-r}}{q^m - 1} T(F), & \text{если } \bar{z} \neq (\Psi(0), \dots, \Psi(0)). \end{cases}$$

ДОКАЗАТЕЛЬСТВО. Пусть Ψ_r – отображение из множества R^r в множество K^r , осуществляемое по правилу

$$\Psi_r(a_1, \dots, a_r) = (\Psi(a_1), \dots, \Psi(a_r))$$

для всех $a_1, \dots, a_r \in R$. Справедливо (см., например, [19]) следующее соотношение ортогональности:

$$\frac{1}{q^n} \sum_{c \in R} \chi(cx) = \begin{cases} 1, & \text{если } x = 0, \\ 0, & \text{если } x \neq 0. \end{cases} \quad (10)$$

С использованием соотношения (10) получим

$$N_l(\bar{z}, \omega_1, \dots, \omega_r) = \sum_{i=0}^{l-1} \sum_{\substack{\bar{a}=(a_1, \dots, a_r) \in R^r \\ \Psi_r(\bar{a})=\bar{z}}} \prod_{j=1}^r \frac{1}{q^r} \sum_{c_j \in R} \chi(c_j(u_j(i) - a_j)).$$

Для всех векторов $\bar{c} = (c_1, \dots, c_r) \in R^r$ введем обозначения $\bar{c}\bar{a} = c_1a_1 + \dots + c_ra_r$, $u_{\bar{c}} = c_1u_1 + \dots + c_ru_r$. Тогда получим равенство

$$N_l(\bar{z}, \omega_1, \dots, \omega_r) = \frac{1}{q^{nr}} \sum_{\bar{a} \in R^r, \Psi_r(\bar{a})=\bar{z}} \sum_{\bar{c} \in R^r} \chi(-\bar{c}\bar{a}) \sum_{i=0}^{l-1} \chi(u_{\bar{c}}(i)).$$

Выделим в полученном равенстве слагаемое, соответствующее значению $\bar{c} = \bar{0}$, и заметим, что количество векторов $\bar{a} \in R^r$ таких, что $\Psi_r(\bar{a}) = \bar{z}$, равно $q^{(n-1)r}$. Тогда

$$N_l(\bar{z}, \omega_1, \dots, \omega_r) - \frac{l}{q^r} = \frac{1}{q^{nr}} \sum_{\bar{a} \in R^r, \Psi_r(\bar{a})=\bar{z}} \sum_{\bar{c} \in R^r, \bar{c} \neq \bar{0}} \chi(-\bar{c}\bar{a}) \sum_{i=0}^{l-1} \chi(u_{\bar{c}}(i)). \quad (11)$$

Переходя в равенстве (11) к рассмотрению абсолютных величин, будем иметь

$$\left| N_l(\bar{z}, \omega_1, \dots, \omega_r) - \frac{l}{q^r} \right| \leq \frac{1}{q^{nr}} \sum_{\bar{a} \in R^r, \Psi_r(\bar{a})=\bar{z}} \sum_{\bar{c} \in R^r, \bar{c} \neq \bar{0}} \max_{\bar{c} \in R^r, \bar{c} \neq \bar{0}} |S_l(u_{\bar{c}})|.$$

При всех $\bar{c} \neq \bar{0}$ последовательность $u_{\bar{c}}$ – ненулевая ЛРП из множества $L_R(F)$; тогда получим

$$\left| N_l(\bar{z}, \omega_1, \dots, \omega_r) - \frac{l}{q^r} \right| \leq \frac{q^{nr} - 1}{q^r} \max_{v \in L_R(F), v \neq (0)} |S_l(v)|.$$

Таким образом, оценка (8) доказана.

Докажем оценку (9). Пусть $l = T(F)$. Используя равенство (11), получим

$$\begin{aligned} N_l(\bar{z}, \omega_1, \dots, \omega_r) - \frac{l}{q^r} + \sigma(\bar{z}) \\ = \frac{1}{q^{nr}} \sum_{\bar{a} \in R^r, \Psi_r(\bar{a})=\bar{z}} \sum_{\bar{c} \in R^r, \bar{c} \neq \bar{0}} \chi(-\bar{c}\bar{a}) \left(\sum_{i=0}^{l-1} \chi(u_{\bar{c}}(i)) + \frac{p^\nu}{d} \right), \end{aligned}$$

где

$$\sigma(\bar{z}) = \frac{p^\nu}{dq^{nr}} \sum_{\bar{a} \in R^r, \Psi_r(\bar{a}) = \bar{z}} \sum_{\bar{c} \in R^r, \bar{c} \neq \bar{0}} \chi(-\bar{c}\bar{a}).$$

Как показано в работе [19], имеет место соотношение

$$\sum_{\bar{c} \in R^r, \bar{c} \neq \bar{0}} \chi(-\bar{c}\bar{a}) = \begin{cases} q^{nr} - 1, & \text{если } \bar{a} = \bar{0}, \\ -1, & \text{если } \bar{a} \neq \bar{0}. \end{cases}$$

Тогда

$$\sigma(\bar{z}) = \begin{cases} -\frac{p^\nu}{dq^r}, & \text{если } \bar{z} = \Psi_r(\bar{0}), \\ \frac{p^\nu(q^r - 1)}{dq^r}, & \text{если } \bar{z} \neq \Psi_r(\bar{0}), \end{cases}$$

а значит, $T(F)/q^r - \sigma(\bar{z}) = \delta(\bar{z})$ и справедливо неравенство

$$|N_l(\bar{z}, \omega_1, \dots, \omega_r) - \delta(\bar{z})| \leq \frac{q^{nr} - 1}{q^r} \max_{v \in L_R(F), v \neq (0)} \left| S_l(v) + \frac{p^\nu}{d} \right|.$$

Теорема 3 показывает, что отклонение частот $N_l(\bar{z}, \omega_1, \dots, \omega_r)$ от своих “естественных” средних значений $l/|K|^r$ имеет величину, не большую, чем $(q^{nr} - 1)S/q^r$, где S – оценка сверху тригонометрической суммы $S_l(v)$ или $S_l(v) + p^\nu/d$ при $l = T(F)$. Отметим, что доказательство теоремы 3 легко исправить так, чтобы получить оценки и в случае, когда отображение Ψ не является сбалансированным.

Непосредственно из теоремы 3 и утверждений 1, 2 получим

СЛЕДСТВИЕ 3. Пусть K – разрядное множество кольца R в условиях теоремы 3, $\Psi = \varkappa_{n-1}^K$, $\omega_t = \Psi(u_t)$, где $t = 1, 2, \dots, r$. Тогда для всех $\bar{z} \in K^r$ справедливы следующие оценки:

1) если $l \leq T(F)$, то

$$\left| N_l(\bar{z}, \omega_1, \dots, \omega_r) - \frac{l}{q^r} \right| \leq \frac{p^{\nu+n-1}(q^{nr} - 1)}{q^r} \left(\frac{4}{\pi^2} \ln T(\bar{F}) + \frac{9}{5} \right) q^{\frac{m}{2}};$$

2) если $l = T(F)$, то

$$|N_l(\bar{z}, \omega_1, \dots, \omega_r) - \delta(\bar{z})| \leq \frac{p^\nu(q^{nr} - 1)(dp^{n-1} - 1)}{q^r d} q^{\frac{m}{2}}.$$

Точно такие же оценки справедливы и в случае отображений Ψ , удовлетворяющих равенству (7). Отметим, что рассматриваемые оценки являются нетривиальными только при условии $T(\bar{F}) \geq q^{(n-1)r} p^{n-1} q^{m/2}$. В частности, если $\bar{F}(x)$ – многочлен максимального периода, то это неравенство выполнено при $m > 2(n-1)(r+1)$.

Оценки из теоремы 3 не удается существенно усилить даже в частных случаях. Так, в работах [9], [12], [13] и [16] в частном случае, когда $R = \mathbb{Z}_{2^n}$, были получены аналогичные оценки, отличающиеся от оценок из теоремы 3 только заменой множителя $(2^{nr} - 1)/2^r$ (не зависящего от m) на множитель $(\ln 2^{n-1})^r$. При этом главный множитель $2^{m/2}$, участвующий во всех рассматриваемых оценках, не может быть заменен на множитель $a^{m/2}$, где $a < 2$ (см. [9]).

§ 4. Спектральные коэффициенты разрядных отображений

Пусть $R = \mathbb{Z}_{p^n}$, где p – простое число, $n \in \mathbb{N}$, а $K = \{k_0, k_1, \dots, k_{p-1}\}$ – разрядное множество кольца R . Обозначим через $\stackrel{p}{\equiv}$ отношение сравнимости по модулю p на множестве целых чисел. Всюду в дальнейшем будем считать, что для всех $i \in \{0, 1, \dots, p-1\}$ выполнено соотношение $k_i \stackrel{p}{\equiv} i$. Операции $\oplus$ и $\otimes$, задающие на K структуру поля, определяются для всех $i, j \in \{0, 1, \dots, p-1\}$ соотношениями

$$k_i \oplus k_j = k_{r_p(i+j)} \stackrel{p}{\equiv} i + j, \quad k_i \otimes k_j = k_{r_p(i \cdot j)} \stackrel{p}{\equiv} i \cdot j,$$

где $r_p(a)$ – остаток от деления числа a на p .

Характер χ , определенный равенством (5), в случае кольца $R = \mathbb{Z}_{p^n}$ принимает вид

$$\chi(x) = e^{2\pi i \frac{x}{p^n}}. \quad (12)$$

Для каждого элемента $c \in K$ рассмотрим отображение $\mu_c: R \rightarrow \mathbb{C}$, осуществляемое по правилу

$$\mu_c(a) = \exp\left\{2\pi i \frac{c \otimes \varkappa_{n-1}^K(a)}{p}\right\} = \exp\left\{2\pi i \frac{c \cdot \varkappa_{n-1}^K(a)}{p}\right\}, \quad a \in R. \quad (13)$$

Следующий результат является частным случаем разложения Фурье отображения μ_c по базису аддитивных характеров кольца R (см., например, [26, равенства (12), (13)]).

УТВЕРЖДЕНИЕ 3. Пусть K – разрядное множество кольца $\mathbb{Z}_{p^n}$. Тогда для всех $a \in \mathbb{Z}_{p^n}$, $c \in K$ имеет место равенство

$$\mu_c(a) = \sum_{j=0}^{p^n-1} \mu_{c,j} \chi(a j), \quad (14)$$

где

$$\mu_{c,j} = \frac{1}{p^n} \sum_{s=0}^{p^n-1} \mu_c(s) \chi(-s j). \quad (15)$$

Величины $\mu_{c,j}$, участвующие в равенстве (14), можно рассматривать как соответствующие спектральные коэффициенты в представлении отображения μ_c через аддитивные характеры кольца $R = \mathbb{Z}_{p^n}$. Укажем свойства этих коэффициентов, которые понадобятся в дальнейшем. Для каждого $i \in \{0, 1, \dots, p-1\}$ рассмотрим множество

$$A_i = \{a \in R: \varkappa_{n-1}^K(a) = k_i\}.$$

Несложно заметить, что $A_s = A_0 + s p^{n-1}$ для всех $s = 0, 1, \dots, p-1$.

УТВЕРЖДЕНИЕ 4. Пусть K – разрядное множество кольца $R = \mathbb{Z}_{p^n}$, и пусть $c \in K$, $c \neq k_0$. Тогда

$$\mu_{c,j} = \begin{cases} 0, & \text{если } j \not\stackrel{p}{\equiv} c, \\ \frac{1}{p^{n-1}} \sum_{a \in A_0} \chi(-a j), & \text{если } j \stackrel{p}{\equiv} c. \end{cases}$$

ДОКАЗАТЕЛЬСТВО. С использованием равенств $A_s = A_0 + sp^{n-1}$, где $s = 0, 1, \dots, p-1$, получим

$$\mu_{c,j} = \frac{1}{p^n} \sum_{s=0}^{p-1} \sum_{a \in A_0} \mu_c(a + sp^{n-1}) \chi(-(a + sp^{n-1})j).$$

Отсюда следует равенство

$$\mu_{c,j} = \frac{1}{p^n} \sum_{s=0}^{p-1} \sum_{a \in A_0} e^{2\pi i \frac{c k_s s}{p}} \chi(-aj) e^{-2\pi i \frac{s j}{p}}.$$

Изменив порядок суммирования и воспользовавшись соотношением $k_s \stackrel{p}{\equiv} s$, получим

$$\mu_{c,j} = \frac{1}{p^n} \sum_{a \in A_0} \chi(-aj) \sum_{s=0}^{p-1} e^{2\pi i \frac{(c-j)s}{p}}.$$

Для завершения доказательства остается воспользоваться равенствами

$$\sum_{s=0}^{p-1} e^{2\pi i \frac{(c-j)s}{p}} = \begin{cases} 0, & \text{если } j \not\equiv c, \\ p, & \text{если } j \equiv c. \end{cases}$$

В дальнейшем потребуется оценить сверху величину

$$\sum_{j=0}^{p^n-1} |\mu_{c,j}|, \quad (16)$$

представляющую собой сумму модулей спектральных коэффициентов. С использованием соотношений $|\mu_{c,j}| \leq |A_0|/p^{n-1} = 1$ получим оценку

$$\sum_{j=0}^{p^n-1} |\mu_{c,j}| \leq p^{n-1}.$$

Уточним данную оценку.

ТЕОРЕМА 4. Пусть K – разрядное множество кольца $R = \mathbb{Z}_{p^n}$, $c \in K$, $c \neq k_0$. Тогда

$$\sum_{j=0}^{p^n-1} |\mu_{c,j}| \leq p^{\frac{n-1}{2}}.$$

ДОКАЗАТЕЛЬСТВО. Согласно равенству Парсеваля (см., например, [26, равенство (16)]) имеем

$$\sum_{j=0}^{p^n-1} |\mu_{c,j}|^2 = 1.$$

Используя неравенство Коши

$$\sum_{i=1}^t a_i b_i \leq \left(\sum_{i=1}^t a_i^2 \right)^{\frac{1}{2}} \left(\sum_{i=1}^t b_i^2 \right)^{\frac{1}{2}},$$

справедливое для всех чисел $t \in \mathbb{N}$, $a_i, b_i \in \mathbb{R}$, где $i = 1, 2, \dots, t$, и утверждение 4, получим

$$\sum_{j=0}^{p^n-1} |\mu_{c,j}| = \sum_{i=0}^{p^{n-1}-1} |\mu_{c,c+pi}| \leq p^{\frac{n-1}{2}}.$$

Автор выражает благодарность Ю. В. Нестеренко, указавшему что первоначальное доказательство теоремы 4 можно существенно сократить.

§ 5. Разрядные множества, образующие арифметическую прогрессию

Рассмотрим разрядное множество $K = \{k_0, k_1, \dots, k_{p-1}\}$ кольца $R = \mathbb{Z}_{p^n}$. Как и ранее, предполагается, что элементы множества K занумерованы так, что $k_i \stackrel{p}{=} i$ для всех $i = 0, 1, \dots, p-1$. Будем говорить, что K образует арифметическую прогрессию, если

$$K = \{a, a + d, a + 2d, \dots, a + (p-1)d\} \quad (17)$$

для некоторых элементов $a, d \in R$, $a \stackrel{p}{=} 0$, $(d, p) = 1$. В этом случае будем использовать обозначение $K = K_{a,d}$. Важным примером разрядного множества, образующего арифметическую прогрессию, является p -ичное разрядное множество $K_{0,1} = \{0, 1, \dots, p-1\}$. Напомним, что для разрядного множества K кольца R через $A_0 = A_0(K)$ обозначено множество всех элементов $a \in R$, для которых их старшая координата $\varkappa_{n-1}^K(a)$ равна k_0 . Другими словами,

$$A_0 = \{k_{i_0} + pk_{i_1} + \dots + p^{n-2}k_{i_{n-2}} : k_{i_0}, k_{i_1}, \dots, k_{i_{n-2}} \in K\}.$$

По аналогии будем говорить, что множество A_0 образует арифметическую прогрессию, если

$$A_0 = \{b, b + r, b + 2r, \dots, b + (p^{n-1} - 1)r\}$$

для некоторых элементов $b, r \in R$, $b \stackrel{p}{=} 0$, $(r, p) = 1$. В дальнейшем нам понадобится следующий вспомогательный результат.

ЛЕММА 4. В кольце $R = \mathbb{Z}_{p^n}$, где $n \geq 2$, для некоторых элементов $i \in \{1, 2, \dots, n-1\}$, $a, a', d, d' \in R$ таких, что $(d, p) = (d', p) = 1$, равенство

$$\{a, a + d, a + 2d, \dots, a + (p^i - 1)d\} = \{a', a' + d', a' + 2d', \dots, a' + (p^i - 1)d'\} \quad (18)$$

имеет место тогда и только тогда, когда $a' = a$, $d' = d$ либо $a' = a + (p^i - 1)d$, $d' = -d$.

ДОКАЗАТЕЛЬСТВО. Очевидно, что равенство (18) имеет место в каждом из рассматриваемых случаев. Пусть выполнено соотношение (18); тогда

$$\{0, d, 2d, \dots, (p^i - 1)d\} = \{a' - a, a' - a + d', a' - a + 2d', \dots, a' - a + (p^i - 1)d'\}.$$

Отсюда в силу обратимости d в кольце R получим

$$\{0, 1, 2, \dots, p^i - 1\} = \{b, b + r, b + 2r, \dots, b + (p^i - 1)r\}, \quad (19)$$

где $b = d^{-1}(a' - a)$, $r = d^{-1}d'$. Из равенства (19) следует, что для некоторого $k \in \{0, 1, \dots, p^i - 2\}$

$$\{0, 1, 2, \dots, p^i - 1\} = \{-(p^i - k - 1)r, \dots, -r, 0, r, \dots, kr\}. \quad (20)$$

1) Пусть $k \neq 0$ в равенстве (20); тогда, учитывая, что $r \in \{1, \dots, p^i - 1\}$, $-r \in \{p^n - p^i + 1, \dots, p^n - 1\}$, получим $k = p^i - 1$ и

$$\{0, 1, 2, \dots, p^i - 1\} = \{0, r, \dots, (p^i - 1)r\}. \quad (21)$$

Покажем, что это равенство выполнено только при $r = 1$. Если $i = 1$ и $p = 2$, то это именно так. Пусть $p^i > 2$ и $r \neq 1$. Тогда рассмотрим относительно неизвестного $j \in \{0, 1, \dots, p^i - 1\}$ неравенства

$$p^i \leq rj \leq p^n - 1. \quad (22)$$

Они равносильны неравенствам $p^i/r \leq j \leq (p^n - 1)/r$. Поскольку $r \in \{1, \dots, p^i - 1\}$, $((p^n - 1)/r) - (p^i/r) \geq 1$, то неравенства (22) имеют решение, что противоречит соотношению (19). Значит, $r = 1$, $d = d'$, и в силу (20) выполнено $a = a'$.

2) Пусть $k = 0$ в равенстве (20); тогда

$$\{0, 1, 2, \dots, p^i - 1\} = \{-(p^i - 1)r, \dots, -r, 0\}. \quad (23)$$

Отсюда следует, что $-r \in \{0, 1, \dots, p^i - 1\}$. Покажем, что равенство (23) имеет место только при $r = -1$. Если $i = 1$ и $p = 2$, то это очевидно. Пусть $p^i > 2$ и $r \neq -1$; тогда, как показано в п. 1), неравенства $p^i \leq (-r)j \leq p^n - 1$ имеют решение относительно неизвестного $j \in \{0, 1, \dots, p^i - 1\}$. Это противоречит соотношению (23). Значит, $r = -1$, $d' = -d$, и из (19) имеем $a' = a + (p^i - 1)d$.

Опишем свойства разрядных множеств кольца $\mathbb{Z}_{p^n}$, образующих арифметическую прогрессию.

ТЕОРЕМА 5. Пусть $R = \mathbb{Z}_{p^n}$, $n \geq 2$. Тогда:

- 1) при $p = 2$ каждое разрядное множество K кольца R образует арифметическую прогрессию;
- 2) разрядные множества $K_{a,d}$ и $K_{a',d'}$ совпадают, если и только если $a' = a$, $d' = d$ либо $a' = a + (p - 1)d$, $d' = -d$;
- 3) число разрядных множеств кольца R , образующих арифметическую прогрессию, равно $(p - 1)p^{2n-1}/2$;
- 4) разрядное множество $\Gamma(R)$ образует арифметическую прогрессию, если и только если $p = 2$ или $p = 3$;
- 5) если $K = K_{a,d}$, то

$$A_0(K) = \left\{ \frac{p^{n-1} - 1}{p - 1}a + dj : j = 0, 1, \dots, p^{n-1} - 1 \right\},$$

т.е. множество $A_0 = A_0(K)$ образует арифметическую прогрессию;

- 6) если множество $A_0 = A_0(K)$ образует арифметическую прогрессию, то найдется единственное разрядное множество $K_{a,d}$ такое, что $A_0 = A_0(K_{a,d})$.

ДОКАЗАТЕЛЬСТВО. В случае $p = 2$ для каждого разрядного множества $K = \{k_0, k_1\}$ выполнено равенство $K = K_{k_0, k_1 - k_0}$. Утверждение 1) доказано.

Утверждение 2) непосредственно следует из леммы 4, а утверждение 3) следует из 2).

Докажем утверждение 4). Рассмотрим множество $\Gamma(R) = \{x \in R: x^p = x\}$. При $p = 2$ имеем $\Gamma(R) = \{0, 1\} = K_{0,1}$, а при $p = 3$ получаем $\Gamma(R) = \{0, 1, -1\} = K_{-1,1}$. Покажем, что при $p > 3$ множество $\Gamma(R)$ не образует арифметической прогрессии. Допустим противное:

$$\Gamma(R) = \{-ds, \dots, -d, 0, d, \dots, dk\}, \quad (24)$$

где $d \in R$. Поскольку для каждого $a \in \Gamma(R)$ выполнено включение $-a \in \Gamma(R)$, то $s = k = (p - 1)/2$. Тогда из равенств (24) и $d^{-1}\Gamma(R) = \Gamma(R)$ получим

$$\Gamma(R) = \left\{ -\frac{p-1}{2}, \dots, -1, 0, 1, \dots, \frac{p-1}{2} \right\}.$$

Значит, $2 \cdot (p - 1)/2 = p - 1 \notin \Gamma(R)$, что противоречит замкнутости множества $\Gamma(R)$ относительно умножения.

Докажем утверждение 5). Пусть $K = K_{a,d}$; тогда из равенств

$$A_0 = \{k_{i_0} + pk_{i_1} + \dots + p^{n-2}k_{i_{n-2}}: k_{i_0}, k_{i_1}, \dots, k_{i_{n-2}} \in K\},$$

где $k_{i_j} = a + di_j$, $i_j \in \{0, 1, \dots, p - 1\}$ для всех $j = 0, 1, \dots, n - 1$, будем иметь

$$A_0 = \left\{ \frac{p^{n-1} - 1}{p - 1}a + d(i_0 + pi_1 + \dots + p^{n-2}i_{n-2}): i_0, i_1, \dots, i_{n-2} \in \{0, \dots, p - 1\} \right\}.$$

Значит, $A_0 = \{(p^{n-1} - 1)a/(p - 1) + dj: j = 0, 1, \dots, p^{n-1} - 1\}$.

Докажем утверждение 6). Пусть $A_0 = A_0(K) = \{b + rj: j = 0, 1, \dots, p^{n-1} - 1\}$. Рассмотрим разрядное множество $K_{a,d}$, $a = f^{-1}b$, $d = r$, $f = (p^{n-1} - 1)/(p - 1)$. Из доказательства утверждения 5) имеем $A_0(K_{a,d}) = A_0$. Допустим, что найдутся элементы $a', d' \in R$ такие, что $A_0(K_{a',d'}) = A_0$. Тогда согласно 5)

$$A_0 = \{fa' + d'j: j = 0, 1, \dots, p^{n-1} - 1\} = \{b + rj: j = 0, 1, \dots, p^{n-1} - 1\}.$$

В силу леммы 4 имеем $fa' = b$, $d' = r$ либо $fa' = b + (p^{n-1} - 1)r$, $d' = -r$. В первом случае $a' = a$, $d' = d$, а во втором $a' = a + (p - 1)d$, $d' = -d$. Каждый из этих случаев согласно утверждению 2) приводит к равенству $K_{a,d} = K_{a',d'}$. Теорема доказана.

В дальнейшем понадобится следующая

ЛЕММА 5. Пусть функция $f(x)$ определена на отрезке $[a, b]$ и выпукла вниз. Тогда для каждого $t \in \mathbb{R}$, $0 \leq t \leq b - a$, справедливо неравенство

$$f(a + t) + f(b - t) \leq f(a) + f(b).$$

ДОКАЗАТЕЛЬСТВО. Для выпуклой вниз функции $f(x)$ при всех $x_1, x_2 \in [a, b]$ и всех $\alpha, \beta \in \mathbb{R}$ таких, что $\alpha \geq 0$, $\beta \geq 0$, $\alpha + \beta = 1$, выполнено неравенство

$$f(\alpha x_1 + \beta x_2) \leq \alpha f(x_1) + \beta f(x_2).$$

Отсюда получим

$$\begin{aligned} f(a+t) &\leq \frac{b-a-t}{b-a}f(a) + \frac{t}{b-a}f(b), \\ f(b-t) &\leq \frac{t}{b-a}f(a) + \frac{b-a-t}{b-a}f(b). \end{aligned}$$

Сложив почленно обе части последних неравенств, получим требуемое.

ТЕОРЕМА 6. Пусть $K = K_{a,d}$ – разрядное множество кольца $R = \mathbb{Z}_{p^n}$, $n \geq 2$, $c \in K$, $c \neq k_0$. Тогда

$$\sum_{j=0}^{p^n-1} |\mu_{c,j}| < \frac{2}{\pi} \ln(p^{n-1}) + \frac{13}{40}p + \frac{7}{20}.$$

ДОКАЗАТЕЛЬСТВО. При $p = 2$ неравенство доказано ранее (см. [9]). Будем рассматривать случай $p \geq 3$. В случае $K = K_{a,d}$ согласно утверждению 3 и теореме 5, 5) справедливо равенство

$$\sum_{j=0}^{p^n-1} |\mu_{c,j}| = \frac{1}{p^{n-1}} \sum_{s=0}^{p^{n-1}-1} \left| \sum_{t=0}^{p^{n-1}-1} \chi((b+dt)(c+sp)) \right|,$$

где $b = (p^{n-1} - 1)a/(p - 1)$. С использованием равенства $|\chi(b(c+sp))| = 1$ получим

$$\sum_{j=0}^{p^n-1} |\mu_{c,j}| = \frac{1}{p^{n-1}} \sum_{s=0}^{p^{n-1}-1} \left| \sum_{t=0}^{p^{n-1}-1} \chi(dt(c+sp)) \right|. \quad (25)$$

Элемент d обратим в кольце R , поэтому числа $d(c+sp)$, где $s = 0, 1, \dots, p^{n-1} - 1$, попарно не сравнимы по модулю p^n . Пусть элемент $k \in \{0, 1, \dots, p^{n-1} - 1\}$ выбран так, что $k \equiv dc$; тогда $k \neq 0$ и выполнены равенства

$$\{d(c+sp) : s = 0, 1, \dots, p^{n-1} - 1\} = dc + pR = k + pR,$$

то есть

$$\{d(c+sp) : s = 0, 1, \dots, p^{n-1} - 1\} = \{k + sp : s = 0, 1, \dots, p^{n-1} - 1\}.$$

Значит, с учетом равенства (25) получим

$$\sum_{j=0}^{p^n-1} |\mu_{c,j}| = \frac{1}{p^{n-1}} \sum_{s=0}^{p^{n-1}-1} \left| \sum_{t=0}^{p^{n-1}-1} \chi(t(k+sp)) \right|.$$

Из определения характера χ следуют равенства

$$\sum_{j=0}^{p^n-1} |\mu_{c,j}| = \frac{1}{p^{n-1}} \sum_{s=0}^{p^{n-1}-1} \left| \sum_{t=0}^{p^{n-1}-1} e^{2\pi i \frac{k+sp}{p^n} t} \right| = \frac{1}{p^{n-1}} \sum_{s=0}^{p^{n-1}-1} \frac{|e^{2\pi i \frac{k}{p}} - 1|}{|e^{2\pi i \frac{k+sp}{p^n}} - 1|}.$$

С использованием равенства $|e^{i\varphi} - 1| = 2|\sin(\varphi/2)|$ получим

$$\sum_{j=0}^{p^n-1} |\mu_{c,j}| \leq \frac{1}{p^{n-1}} \sum_{s=0}^{p^{n-1}-1} \frac{1}{\sin\left(\frac{k+sp}{p^n}\pi\right)}. \quad (26)$$

Введем обозначения $f(x) = 1/\sin x$, $a_k(s) = \pi(k+sp)/p^n$, где $k = 1, 2, \dots, p-1$, $s = 0, 1, \dots, p^{n-1}-1$. Докажем, что при всех $k \in \{1, 2, \dots, p-1\}$ выполнено неравенство

$$\sum_{s=0}^{p^{n-1}-1} f(a_k(s)) \leq \sum_{s=0}^{p^{n-1}-1} f(a_1(s)). \quad (27)$$

Заметим, что для всех рассматриваемых значений k и s справедливо равенство $f(a_k(s)) = f(a_{p-k}(p^{n-1}-1-s))$, поэтому неравенство (27) достаточно доказать для всех $k \in \{1, 2, \dots, (p-1)/2\}$. Имеет место соотношение

$$\sum_{s=0}^{p^{n-1}-1} f(a_k(s)) = f\left(a_k\left(\frac{p^{n-1}-1}{2}\right)\right) + \sum_{s=0}^{(p^{n-1}-1)/2-1} (f(a_k(s)) + f(a_{p-k}(s))). \quad (28)$$

Функция $f(x)$ убывает и выпукла вниз на интервале $(0, \pi/2)$, значит, согласно лемме 5

$$\begin{aligned} f\left(a_1\left(\frac{p^{n-1}-1}{2}\right)\right) &\geq f\left(a_k\left(\frac{p^{n-1}-1}{2}\right)\right), \\ f(a_1(s)) + f(a_{p-1}(s)) &\geq f(a_k(s)) + f(a_{p-k}(s)) \end{aligned}$$

для всех $k = 1, 2, \dots, (p-1)/2$, $s = 0, 1, \dots, (p^{n-1}-1)/2-1$. Тогда с использованием равенства (28) получим, что имеет место соотношение (27), а значит, с учетом (26)

$$\sum_{j=0}^{p^n-1} |\mu_{c,j}| \leq \frac{1}{p^{n-1}} \sum_{s=0}^{p^{n-1}-1} f(a_1(s)). \quad (29)$$

Получим оценку сверху для величины

$$\frac{1}{p^{n-1}} \sum_{s=0}^{p^{n-1}-1} f(a_1(s)) = \frac{1}{p^{n-1}} \sum_{s=0}^{p^{n-1}-1} \frac{1}{\sin\left(\frac{1+sp}{p^n}\pi\right)}.$$

Согласно интегральному неравенству Йенсена (см., например, [27, с. 153]) для выпуклой вниз и дифференцируемой функции $f(x)$ на отрезке $[a, b]$ имеет место неравенство

$$f\left(\frac{a+b}{2}\right) \leq \frac{1}{b-a} \int_a^b f(x) dx.$$

С использованием этого неравенства получим

$$\frac{1}{p^{n-1}} \sum_{s=0}^{p^{n-1}-1} f(a_1(s)) \leq \frac{f(a_1(0))}{p^{n-1}} + \frac{1}{p^{n-1}} \sum_{s=1}^{p^{n-1}-1} \frac{p^{n-1}}{\pi} \int_{a_1(s)-\frac{\pi}{2p^{n-1}}}^{a_1(s)+\frac{\pi}{2p^{n-1}}} f(x) dx.$$

Отсюда следует соотношение

$$\frac{1}{p^{n-1}} \sum_{s=0}^{p^{n-1}-1} f(a_1(s)) \leq \frac{f(a_1(0))}{p^{n-1}} + \frac{1}{\pi} \int_{a_1(1) - \frac{\pi}{2p^{n-1}}}^{a_1(p^{n-1}-1) + \frac{\pi}{2p^{n-1}}} f(x) dx.$$

Вычислив значение интеграла, получим

$$\frac{1}{p^{n-1}} \sum_{s=0}^{p^{n-1}-1} f(a_1(s)) \leq \frac{f(a_1(0))}{p^{n-1}} - \frac{1}{\pi} \left(\ln \left(\operatorname{tg} \left(\frac{p-2}{4p^n} \pi \right) \right) + \ln \left(\operatorname{tg} \left(\frac{p+2}{4p^n} \pi \right) \right) \right).$$

С учетом неравенства $\operatorname{tg} x > x$, справедливого при всех $x \in (0, \pi/4)$, будем иметь

$$\frac{1}{p^{n-1}} \sum_{s=0}^{p^{n-1}-1} f(a_1(s)) \leq \frac{f(a_1(0))}{p^{n-1}} + \frac{1}{\pi} \ln \left(\frac{4p^n}{(p-2)\pi} \right) + \frac{1}{\pi} \ln \left(\frac{4p^n}{(p+2)\pi} \right),$$

а значит,

$$\frac{1}{p^{n-1}} \sum_{s=0}^{p^{n-1}-1} f(a_1(s)) \leq \frac{f(a_1(0))}{p^{n-1}} + \frac{1}{\pi} \ln \left(\frac{(4p^n)^2}{(p-2)(p+2)\pi^2} \right). \quad (30)$$

Рассмотрим отдельно каждое слагаемое из правой части в (30). Функция $(\sin x)/x$ убывает на интервале $(0, \pi/4)$, поэтому при $n \geq 2$ справедливо неравенство

$$\frac{\sin\left(\frac{\pi}{p^n}\right)}{\frac{\pi}{p^n}} \geq \frac{\sin\left(\frac{\pi}{9}\right)}{\frac{\pi}{9}},$$

а значит,

$$\frac{f(a_1(0))}{p^{n-1}} = \frac{1}{p^{n-1} \sin\left(\frac{\pi}{p^n}\right)} \leq \frac{p}{9 \sin\left(\frac{\pi}{9}\right)} < \frac{13}{40} p. \quad (31)$$

Для второго слагаемого будем иметь

$$\frac{1}{\pi} \ln \left(\frac{(4p^n)^2}{(p-2)(p+2)\pi^2} \right) = \frac{2}{\pi} \ln(p^{n-1}) + \frac{2}{\pi} \ln \left(\frac{4}{\pi} \right) + \frac{2}{\pi} \ln \left(\frac{p}{\sqrt{p^2-4}} \right).$$

Поскольку функция $x/\sqrt{x^2-4}$ убывает на интервале $(2, +\infty)$, имеем

$$\frac{2}{\pi} \ln \left(\frac{4}{\pi} \right) + \frac{2}{\pi} \ln \left(\frac{p}{\sqrt{p^2-4}} \right) \leq \frac{2}{\pi} \ln \left(\frac{4}{\pi} \right) + \frac{2}{\pi} \ln \left(\frac{3}{\sqrt{5}} \right) < \frac{7}{20},$$

что приводит к соотношению

$$\frac{1}{\pi} \ln \left(\frac{(4p^n)^2}{(p-2)(p+2)\pi^2} \right) < \frac{2}{\pi} \ln(p^{n-1}) + \frac{7}{20}. \quad (32)$$

В итоге с использованием равенств (30)–(32) получим

$$\frac{1}{p^{n-1}} \sum_{s=0}^{p^{n-1}-1} f(a_1(s)) < \frac{2}{\pi} \ln(p^{n-1}) + \frac{13}{40} p + \frac{7}{20}.$$

Для завершения доказательства теоремы остается воспользоваться соотношением (29).

Несложно заметить, что для всех простых чисел p оценка из теоремы 4 точнее оценки из теоремы 6 при $n = 2$. Однако при всех $n \geq 3$ результат теоремы 6 существенно усиливает оценку из теоремы 4.

§ 6. Уточнение оценок в случае кольца вычетов

Получим оценки числа r -грамм на отрезках старшей разрядной последовательности $\varkappa_{n-1}^K(u)$ ЛРП u , рассматриваемой в разрядном множестве K кольца $R = \mathbb{Z}_{p^n}$. Будем считать, что $K = \{k_0, k_1, \dots, k_{p-1}\}$, причем $k_i \stackrel{p}{\equiv} i$ для всех $i \in \{0, 1, \dots, p-1\}$. Как и ранее, рассмотрим задачу в более общем виде. Пусть $u_1, \dots, u_r$ – последовательности над кольцом R , $\omega_1 = \varkappa_{n-1}^K(u_1), \dots, \omega_r = \varkappa_{n-1}^K(u_r)$, $l \in \mathbb{N}$, $\bar{z} \in K^r$. Пусть $N_l(\bar{z}, \omega_1, \dots, \omega_r)$ – количество появлений вектора $\bar{z}$ среди r -грамм $(\omega_1(i), \dots, \omega_r(i))$, где $i = 0, 1, \dots, l-1$. В случае выполнения равенств $u_1 = x^{s_1}u, \dots, u_r = x^{s_r}u$ для некоторых целых неотрицательных чисел $s_1, \dots, s_r$ величина $N_l(\bar{z}, \omega_1, \dots, \omega_r)$ равна количеству появлений вектора $\bar{z}$ среди r -грамм $(\varkappa_{n-1}^K(u(i+s_1)), \dots, \varkappa_{n-1}^K(u(i+s_r)))$, где $i = 0, 1, \dots, l-1$. Напомним, что последовательности $u_1, \dots, u_r$ называются линейно независимыми над кольцом R , если для всех ненулевых векторов $\bar{c} = (c_1, \dots, c_r) \in R^r$ последовательность $c_1u_1 + \dots + c_ru_r$ является ненулевой.

Как показано в теоремах 4, 6, для спектральных коэффициентов, определенных равенством (15), при $n \geq 2$ имеет место оценка

$$\sum_{j \in R} |\mu_{c,j}| \leq \sigma,$$

где величина $\sigma = \sigma(K)$ определяется соотношением

$$\sigma = \begin{cases} \frac{2}{\pi} \ln(p^{n-1}) + \frac{13}{40}p + \frac{7}{20}, & \text{если } K \text{ имеет вид (17),} \\ p^{\frac{n-1}{2}} & \text{для всех } K. \end{cases}$$

Далее понадобится еще одно свойство спектральных коэффициентов $\mu_{c,j}$, определенных равенством (15).

ЛЕММА 6. Пусть $R = \mathbb{Z}_{p^n}$. Тогда для всех $d_1, \dots, d_k \in K \setminus \{k_0\}$ имеет место равенство

$$\sum_{(j_1, \dots, j_k) \in R^k} \mu_{d_1, j_1} \cdots \mu_{d_k, j_k} = e^{2\pi i \frac{(d_1 + \dots + d_k) \varkappa_{n-1}^K(0)}{p}}.$$

ДОКАЗАТЕЛЬСТВО. Запишем исследуемую величину в виде

$$\sum_{(j_1, \dots, j_k) \in R^k} \mu_{d_1, j_1} \cdots \mu_{d_k, j_k} = \left(\sum_{j_1 \in R} \mu_{d_1, j_1} \right) \cdots \left(\sum_{j_k \in R} \mu_{d_k, j_k} \right).$$

Пусть $d \in K$, $d \neq k_0$; тогда с использованием равенства (14) получим

$$\sum_{j \in R} \mu_{d,j} = \mu_d(0),$$

а значит,

$$\sum_{(j_1, \dots, j_k) \in R^k} \mu_{d_1, j_1} \cdots \mu_{d_k, j_k} = \mu_{d_1}(0) \cdots \mu_{d_k}(0) = e^{2\pi i \frac{(d_1 + \dots + d_k) \chi_{n-1}^K(0)}{p}}.$$

ТЕОРЕМА 7. Пусть $F(x)$ – реверсивный многочлен Галуа степени m над кольцом $R = \mathbb{Z}_{p^n}$, $T(F) = p^\nu(p^m - 1)/d$, $0 \leq \nu \leq n - 1$, $u_1, \dots, u_r$ – линейно независимая система ЛРП из множества $L_R(F)$, K – разрядное множество кольца R , $\chi_{n-1}^K(u_t) = \omega_t$, где $t = 1, 2, \dots, r$. Тогда для всех $\bar{z} = (z_1, \dots, z_r) \in K^r$ справедливы оценки:

1) если $l \leq T(F)$, то

$$\left| N_l(\bar{z}, \omega_1, \dots, \omega_r) - \frac{l}{p^r} \right| \leq \frac{((p-1)\sigma + 1)^r - 1}{p^r} \max_{v \in L_R(F), v \neq (0)} |S_l(v)|;$$

2) если $l = T(F)$, то

$$|N_l(\bar{z}, \omega_1, \dots, \omega_r) - \delta(\bar{z})| \leq \frac{((p-1)\sigma + 1)^r - 1}{p^r} \max_{v \in L_R(F), v \neq (0)} \left| S_l(v) + \frac{p^\nu}{d} \right|,$$

где

$$\delta(\bar{z}) = \begin{cases} \frac{p^{m-r} - 1}{p^m - 1} T(F), & \text{если } \bar{z} = (\chi_{n-1}^K(0), \dots, \chi_{n-1}^K(0)), \\ \frac{p^{m-r}}{p^m - 1} T(F), & \text{если } \bar{z} \neq (\chi_{n-1}^K(0), \dots, \chi_{n-1}^K(0)). \end{cases}$$

ДОКАЗАТЕЛЬСТВО. 1) Используя соотношение ортогональности, получим

$$N_l(\bar{z}, \omega_1, \dots, \omega_r) = \frac{1}{p^r} \sum_{s=0}^{l-1} \left(\sum_{c_1 \in K} e^{2\pi i \frac{c_1(\omega_1(s) - z_1)}{p}} \right) \cdots \left(\sum_{c_r \in K} e^{2\pi i \frac{c_r(\omega_r(s) - z_r)}{p}} \right).$$

Введем обозначение $\bar{c} = (c_1, \dots, c_r)$, $\bar{c}\bar{z} = c_1 z_1 + \dots + c_r z_r$; тогда с использованием формулы (13) будем иметь

$$N_l(\bar{z}, \omega_1, \dots, \omega_r) = \frac{1}{p^r} \sum_{\bar{c} \in K^r} e^{-2\pi i \frac{\bar{c}\bar{z}}{p}} \sum_{s=0}^{l-1} \mu_{c_1}(u_1(s)) \cdots \mu_{c_r}(u_r(s)).$$

Введем обозначение

$$D_l(\bar{c}) = \sum_{s=0}^{l-1} \mu_{c_1}(u_1(s)) \cdots \mu_{c_r}(u_r(s)).$$

Назовем *весом* набора $\bar{c} \in K^r$ число его элементов, отличных от k_0 . Обозначим эту величину $|\bar{c}|$. Тогда

$$N_l(\bar{z}, \omega_1, \dots, \omega_r) = \frac{1}{p^r} \sum_{k=0}^r \sum_{\bar{c}: |\bar{c}|=k} e^{-2\pi i \frac{\bar{c}\bar{z}}{p}} D_l(\bar{c}). \quad (33)$$

Пусть набор $\bar{c} \in K^r$ имеет вес $|\bar{c}| = k$; тогда для некоторого набора чисел $\{t_1, \dots, t_k\} \subset \{1, \dots, r\}$ выполнены равенства $c_{t_1} = d_1, \dots, c_{t_k} = d_k$, где

$d_1, \dots, d_k \in K \setminus \{k_0\}$. Представим величину $D_l(\bar{c})$ с использованием равенства (15) в следующем виде:

$$D_l(\bar{c}) = \sum_{(j_1, \dots, j_k) \in R^k} \mu_{d_1, j_1} \cdots \mu_{d_k, j_k} \sum_{s=0}^{l-1} \chi(j_1 u_{t_1}(s) + \cdots + j_k u_{t_k}(s)). \quad (34)$$

Заметим, что $\mu_{d_1, 0} = \cdots = \mu_{d_k, 0} = 0$, поэтому в первой сумме достаточно ограничиться суммированием по всем наборам $(j_1, \dots, j_k) \in (R \setminus \{0\})^k$. При каждом таком наборе в силу линейной независимости системы $u_1, \dots, u_r$ последовательность v с элементами

$$v(s) = j_1 u_{t_1}(s) + \cdots + j_k u_{t_k}(s), \quad s \geq 0, \quad (35)$$

является ненулевой ЛРП с характеристическим многочленом $F(x)$. Тогда

$$|D_l(\bar{c})| \leq \sum_{(j_1, \dots, j_k) \in R^k} |\mu_{d_1, j_1} \cdots \mu_{d_k, j_k}| \max_{v \in L_R(F), v \neq (0)} |S_l(v)|,$$

где $S_l(v)$ – величина, определенная равенством (6). С использованием соотношений

$$\sum_{(j_1, \dots, j_k) \in R^k} |\mu_{d_1, j_1} \cdots \mu_{d_k, j_k}| = \left(\sum_{j_1 \in R} |\mu_{d_1, j_1}| \right) \cdots \left(\sum_{j_k \in R} |\mu_{d_k, j_k}| \right) \leq \sigma^k \quad (36)$$

получим

$$|D_l(\bar{c})| \leq \sigma^k \max_{v \in L_R(F), v \neq (0)} |S_l(v)|.$$

Выделяя в равенстве (33) слагаемое, соответствующее $\bar{c}$, где $|\bar{c}| = 0$, имеем

$$\left| N_l(\bar{z}, \omega_1, \dots, \omega_r) - \frac{l}{p^r} \right| \leq \frac{1}{p^r} \sum_{k=1}^r \binom{r}{k} (p-1)^k \sigma^k \max_{v \in L_R(F), v \neq (0)} |S_l(v)|.$$

Таким образом,

$$\left| N_l(\bar{z}, \omega_1, \dots, \omega_r) - \frac{l}{p^r} \right| \leq \frac{((p-1)\sigma + 1)^r - 1}{p^r} \max_{v \in L_R(F), v \neq (0)} |S_l(v)|.$$

2) Пусть теперь $l = T(F)$. С использованием равенств (34), (35), леммы 6 и соотношения $d_1 + \cdots + d_k \stackrel{p}{\equiv} c_1 + \cdots + c_r$ будем иметь

$$D_l(\bar{c}) = \sum_{(j_1, \dots, j_k) \in R^k} \mu_{d_1, j_1} \cdots \mu_{d_k, j_k} \left(\sum_{s=0}^{l-1} \chi(v(s)) + \frac{p^\nu}{d} \right) - \frac{p^\nu}{d} e^{2\pi i \frac{(c_1 + \cdots + c_r) \kappa_{n-1}^K(0)}{p}}.$$

Подставляя данное выражение в равенство (33), получим

$$\begin{aligned} & N_l(\bar{z}, \omega_1, \dots, \omega_r) - \frac{l}{p^r} \\ &= \frac{1}{p^r} \sum_{k=1}^r \sum_{\bar{c}: |\bar{c}|=k} e^{-2\pi i \frac{\bar{c}\bar{z}}{p}} \sum_{(j_1, \dots, j_k) \in R^k} \mu_{d_1, j_1} \cdots \mu_{d_k, j_k} \left(\sum_{s=0}^{l-1} \chi(v(s)) + \frac{p^\nu}{d} \right) - \sigma(\bar{z}), \end{aligned} \quad (37)$$

где

$$\sigma(\bar{z}) = \frac{p^{\nu-r}}{d} \sum_{k=1}^r \sum_{\bar{c}: |\bar{c}|=k} \exp \left\{ \frac{2\pi i}{p} (c_1(\mathfrak{x}_{n-1}^K(0) - z_1) + \dots + c_r(\mathfrak{x}_{n-1}^K(0) - z_r)) \right\}.$$

Для величины $\sigma(\bar{z})$ справедливы равенства

$$\sigma(\bar{z}) = \begin{cases} \frac{p^{\nu-r}}{d} (p^r - 1), & \text{если } \bar{z} = (\mathfrak{x}_{n-1}^K(0), \dots, \mathfrak{x}_{n-1}^K(0)), \\ -\frac{p^{\nu-r}}{d}, & \text{если } \bar{z} \neq (\mathfrak{x}_{n-1}^K(0), \dots, \mathfrak{x}_{n-1}^K(0)), \end{cases}$$

значит,

$$\frac{l}{p^r} - \sigma(\bar{z}) = \frac{p^{\nu}(p^m - 1)}{dp^r} - \sigma(\bar{z}) = \delta(\bar{z}).$$

Переходя к исследованию абсолютных величин в равенстве (37), будем иметь

$$\begin{aligned} |N_l(\bar{z}, \omega_1, \dots, \omega_r) - \delta(\bar{z})| &\leq \\ &\leq \frac{1}{p^r} \sum_{k=1}^r \sum_{\bar{c}: |\bar{c}|=k} \sum_{(j_1, \dots, j_k) \in R^k} |\mu_{d_1, j_1} \dots \mu_{d_k, j_k}| \max_{v \in L_R(F), v \neq (0)} |S_l(v) + \frac{p^{\nu}}{d}|. \end{aligned}$$

Отсюда с использованием неравенства (36) получим

$$|N_l(\bar{z}, \omega_1, \dots, \omega_r) - \delta(\bar{z})| \leq \frac{1}{p^r} \sum_{k=1}^r \binom{r}{k} (p-1)^k \sigma^k \max_{v \in L_R(F), v \neq (0)} |S_l(v) + \frac{p^{\nu}}{d}|,$$

а значит,

$$|N_l(\bar{z}, \omega_1, \dots, \omega_r) - \delta(\bar{z})| \leq \frac{((p-1)\sigma + 1)^r - 1}{p^r} \max_{v \in L_R(F), v \neq (0)} |S_l(v) + \frac{p^{\nu}}{d}|.$$

Теорема доказана.

По сравнению с оценками из теоремы 3 (для случая $R = \mathbb{Z}_{p^n}$), в оценках из теоремы 7 множитель

$$\frac{p^{nr} - 1}{p^r}$$

заменен на существенно меньшую величину

$$\frac{((p-1)\sigma + 1)^r - 1}{p^r}.$$

Непосредственно из теоремы 7 и утверждений 1, 2 получим

СЛЕДСТВИЕ 4. В условиях теоремы 7 справедливы следующие оценки:

1) если $l \leq T(F)$, то

$$\left| N_l(\bar{z}, \omega_1, \dots, \omega_r) - \frac{l}{p^r} \right| \leq \frac{((p-1)\sigma + 1)^r - 1}{p^r} \left(\frac{4}{\pi^2} \ln T(\bar{F}) + \frac{9}{5} \right) p^{\frac{m}{2} + \nu + n - 1},$$

2) если $l = T(F)$, то

$$|N_l(\bar{z}, \omega_1, \dots, \omega_r) - \delta(\bar{z})| \leq \frac{(((p-1)\sigma + 1)^r - 1)(dp^{n-1} - 1)}{dp^r} p^{\frac{m}{2} + \nu}.$$

Отметим, что при $p = 2$ каждое разрядное множество K кольца $R = \mathbb{Z}_{p^n}$ образует арифметическую прогрессию, поэтому, подставляя в оценки из следствия 4 значение

$$\sigma = \frac{2}{\pi} \ln(2^{n-1}) + 1,$$

получим оценки из работы [9]. Таким образом, следствие 4 обобщает эти оценки на случай произвольного p .

В следствии 2 показано, что в старшей разрядной последовательности, как правило, появляются все элементы множества K . Приведем теперь условия, при которых появляются все r -граммы.

СЛЕДСТВИЕ 5. Пусть в условиях теоремы 7

$$T(\overline{F}) \geq (((p-1)\sigma + 1)^r - 1)p^{\frac{m}{2}+n-1}. \quad (38)$$

Тогда среди r -грамм $(\omega_1(i), \dots, \omega_r(i))$, где $i \geq 0$, появятся все элементы множества K^r .

ДОКАЗАТЕЛЬСТВО. С использованием оценки из п. 2) следствия 4 при $l = T(F)$ получим

$$N_l(\bar{z}, \omega_1, \dots, \omega_r) \geq \frac{p^{m-r} - 1}{p^m - 1} T(F) - \frac{(((p-1)\sigma + 1)^r - 1)(dp^{n-1} - 1)}{dp^r} p^{\frac{m}{2}+\nu}. \quad (39)$$

Докажем, что правая часть неравенства (39) больше нуля при выполнении условия (38). Это так, если

$$\frac{p^{m-r} - 1}{p^m - 1} (((p-1)\sigma + 1)^r - 1)p^{\frac{m}{2}+\nu+n-1} > \frac{(((p-1)\sigma + 1)^r - 1)(dp^{n-1} - 1)}{dp^r} p^{\frac{m}{2}+\nu}.$$

Данное неравенство выполняется тогда и только тогда, когда

$$\frac{p^m - p^r}{p^m - 1} p^{n-1} > p^{n-1} - \frac{1}{d},$$

то есть

$$T(\overline{F}) = \frac{p^m - 1}{d} > (p^r - 1)p^{n-1}.$$

Остается заметить, что последнее неравенство выполнено при условии (38). Следствие доказано.

В частности, если $\overline{F}(x)$ – многочлен максимального периода $T(\overline{F}) = p^m - 1$, то он удовлетворяет неравенству (38) при $m \geq 2(n - 1 + r \log_p((p-1)\sigma + 1))$.

Таким образом, результаты работы подтверждают целесообразность использования старших разрядных последовательностей ЛРП u над кольцом Галуа в качестве псевдослучайных последовательностей. Последовательность $u_{n-1} = \varkappa_{n-1}^K(u)$ обладает рядом хороших свойств даже в случае, когда характеристический многочлен $F(x)$ ЛРП u не является многочленом максимального периода. Помимо гарантирования достаточно большого периода последовательности u_{n-1} и большой линейной сложности, удастся обосновать достаточно хорошие ее частотные характеристики.

Список литературы

1. А. А. Нечаев, “Код Кердока в циклической форме”, *Дискрет. матем.*, **1:4** (1989), 123–139; англ. пер.: A. A. Nechaev, “Kerdock code in a cyclic form”, *Discrete Math. Appl.*, **1:4** (1991), 365–384.
2. B. R. McDonald, *Finite rings with identity*, Dekker, New York, 1974.
3. А. С. Кузьмин, А. А. Нечаев, “Линейные рекуррентные последовательности над кольцами Галуа”, *Алгебра и логика*, **34:2** (1995), 169–189; англ. пер.: A. S. Kuzmin, A. A. Nechaev, “Linear recurring sequences over Galois rings”, *Algebra and Logic*, **34:2** (1995), 87–100.
4. А. С. Кузьмин, В. Л. Куракин, А. А. Нечаев, “Псевдослучайные и полилинейные последовательности”, *Труды по дискретной математике*, т. 1, ТВП, М., 1997, 139–202.
5. V. L. Kurakin, A. S. Kuzmin, A. V. Mikhalev, A. A. Nechaev, “Linear recurring sequences over rings and modules”, *J. Math. Sci.*, **76:6** (1995), 2793–2915.
6. А. С. Кузьмин, Г. Б. Маршалко, А. А. Нечаев, “Восстановление линейной рекурренты над примарным кольцом вычетов по ее усложнению”, *Матем. вопр. криптогр.*, **1:2** (2010), 31–56.
7. В. Л. Куракин, “Первая координатная последовательность линейной рекурренты максимального периода над кольцом Галуа”, *Дискрет. матем.*, **6:2** (1994), 88–100; англ. пер.: V. L. Kurakin, “The first coordinate sequence of a linear recurrence of maximal period over a Galois ring”, *Discrete Math. Appl.*, **4:2** (1994), 129–141.
8. Д. Н. Былков, “Класс усложнений линейных рекуррент над кольцом Галуа, не приводящий к потере информации”, *Пробл. передачи информ.*, **46:3** (2010), 51–59; англ. пер.: D. N. Bylkov, “A class of injective compressing maps on linear recurring sequences over a Galois ring”, *Problems Inform. Transmission*, **46:3** (2010), 245–252.
9. О. В. Камловский, “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.
10. L. Lathtonen, S. Ling, P. Solé, D. Zinoviev, “ $\mathbb{Z}_8$ -Kerdock codes and pseudorandom binary sequences”, *J. Complexity*, **20:2–3** (2004), 318–330.
11. P. Solé, D. Zinoviev, “The most significant bit of maximum-length sequences over $\mathbb{Z}_{2^l}$: autocorrelation and imbalance”, *IEEE Trans. Inform. Theory*, **50:8** (2004), 1844–1846.
12. P. Solé, D. Zinoviev, “Distribution of r -patterns in the most significant bit of a maximum length sequence over $\mathbb{Z}_{2^l}$ ”, *Sequences and their applications – SETA 2004* (Seoul, Korea, 2004), Lecture Notes in Comput. Sci., **3486**, Springer-Verlag, Berlin, 2005, 275–281.
13. P. Solé, D. Zinoviev, “Galois rings and pseudo-random sequences”, *Cryptography and coding*, Lecture Notes in Comput. Sci., **4887**, Springer-Verlag, Berlin, 2007, 16–33.
14. S. Fan, W. Han, “Random properties of the highest level sequences of primitive sequences over $\mathbb{Z}_{2^e}$ ”, *IEEE Trans. Inform. Theory*, **49:6** (2003), 1553–1557.
15. Z.-D. Dai, D. Ye, P. Wang, G. Fang, “Distribution of R -patterns in the highest level of p -adic expansion of some linear recursion sequences over Galois rings”, *Mathematical properties of sequences and other combinatorial structures* (Los Angeles, CA, USA, 2002), Kluwer Acad. Publ., Dordrecht, 2003, 77–83.
16. H. Hu, D. Feng, W. Wu, “Incomplete exponential sums over galois rings with applications to some binary sequences derived from $\mathbb{Z}_{2^l}$ ”, *IEEE Trans. Inform. Theory*, **52:5** (2006), 2260–2265.
17. W. Qi, J. Zhou, “Distribution of 0 and 1 in the highest level of primitive sequences over $\mathbb{Z}_{2^e}$ ”, *Sci. China Ser. A*, **40:6** (1997), 606–611.
18. Q. X. Zheng, W. F. Qi, “Distribution properties of compressing sequences derived from primitive sequences over $\mathbb{Z}_{p^e}$ ”, *IEEE Trans. Inform. Theory*, **56:1** (2010), 555–563.

19. О. В. Камловский, “Частотные характеристики линейных рекуррентных последовательностей над кольцами Галуа”, *Матем. сб.*, **200**:4 (2009), 31–52; англ. пер.: O. V. Kamlovskii, “Frequency characteristics of linear recurrence sequences over Galois rings”, *Sb. Math.*, **200**:4 (2009), 499–519.
20. Н. М. Коробов, “Распределение невычетов и первообразных корней в рекуррентных рядах”, *Докл. АН СССР*, **88**:4 (1953), 603–606.
21. Н. М. Коробов, *Тригонометрические суммы и их приложения*, Наука, М., 1989.
22. А. С. Кузьмин, “Распределение элементов на циклах линейных рекуррент над кольцами вычетов”, *УМН*, **47**:6 (1992), 213–214; англ. пер.: A. S. Kuz'min, “The distribution of elements on cycles of linear recurrences over rings of residues”, *Russian Math. Surveys*, **47**:6 (1992), 219–221.
23. А. А. Нечаев, “Цикловые типы линейных подстановок над конечными коммутативными кольцами”, *Матем. сб.*, **184**:3 (1993), 21–56; англ. пер.: A. A. Nechaev, “Cycle types of linear substitutions over finite commutative rings”, *Russian Acad. Sci. Sb. Math.*, **78**:2 (1994), 283–311.
24. М. М. Глухов, В. П. Елизаров, А. А. Нечаев, *Алгебра: учебник*, т. 2, Гелиос АРВ, М., 2003.
25. Т. Cochran, “On a trigonometric inequality of Vinogradov”, *J. Number Theory*, **27**:1 (1987), 9–16.
26. В. И. Солодовников, “Бент-функции из конечной абелевой группы в конечную абелеву группу”, *Дискрет. матем.*, **14**:1 (2002), 99–113; англ. пер.: V. I. Solodovnikov, “Bent functions from a finite abelian group into a finite abelian group”, *Discrete Math. Appl.*, **12**:2 (2002), 111–126.
27. Г. М. Фиктенгольц, *Курс дифференциального и интегрального исчисления*, т. 2, Наука, М., 1968; нем. пер.: G. M. Fikhtengol'ts, *Differential- und Integralrechnung*, v. II, VEB, Berlin, 1986.

О. В. КАМЛОВСКИЙ
(O. V. KAMLOVSKII)
ООО “Центр сертификационных исследований”,
г. Москва
E-mail: ov-kam@yandex.ru

Поступило в редакцию
08.06.2011
12.09.2012