УДК 519.713

СУЩНОСТЬ И МАТЕМАТИЧЕСКИЕ СВОЙСТВА ОДНОГО КЛАССА МНОГОМОДУЛЬНЫХ ПРЕОБРАЗОВАНИЙ

ГРИНЕНКО Т.А.

Предлагается и теоретически обосновывается алгоритм построения псевдослучайных последовательностей с требуемыми свойствами. Этот алгоритм основывается на применении многомодульных преобразований. Рассматриваются сущность и математические свойства многомодульных преобразований.

В ряде приложений необходимо применять псевдослучайные последовательности (ПСП) с требуемыми свойствами [1]. Основными из этих свойств, по которым предъявляются сложные требования, являются: основание алфавита – m, период повторения – L, восстанавливаемость, псевдослучайные свойства, а также структурные свойства.

К настоящему времени разработан ряд алгоритмов и средств формирования ПСП. Основной их особенностью является то, что они строятся для двоичного основания, т.е. m=2. Известен также класс линейных m-ичных последовательностей [2, 3]. Однако этот класс последовательностей обладает неудовлетворительными структурными свойствами в смысле значительной зависимости появления символов в последовательности. Так, для определения закона формирования таких ПСП необходимо и достаточно получить безошибочно $2l$ символов, где l – база линейного рекуррентного регистра [4]. Поэтому весьма важной и необходимой является задача разработки математических алгоритмов и средств с заведомо необходимыми свойствами и основанием алфавита. К наиболее перспективному классу таких преобразований, на наш взгляд, относится класс многомодульных преобразований.

Рассмотрим сущность и свойства преобразования элементов полей Галуа GF(p), которое в дальнейшем будем называть многомодульным. Это преобразование может использоваться при создании средств формирования ПСП.

Общее правило формирования последовательности многомодульного преобразования в поле GF(p) имеет вид

$$\begin{aligned} a_i &= \left(a_{i-1} * \theta_\nu\right) \bmod(P), \\ b_i &= a_i\left(\bmod\left(P_1, P_{2,\ldots,} P_{n-1}, P_n, m\right)\right), \end{aligned} \qquad (1)$$

где a_i и a_{i-1} – собственно i-й и $(i$-1$)$-й элементы формируемой последовательности; θ_υ – ν-й первообразный элемент поля GF(p); $P_1, P_2, \ldots, P_n$ – промежуточные модули; m-основание алфавита.

В соотношении (1) должно выполняться условие

$$P >> P_1 >> P_2 >> \ldots >> P_n >> m \geq 2, \qquad (2)$$

причем P_n – произвольное основание алфавита символов формируемой ПСП.

Применение правила (1) позволяет, с одной стороны, существенно повысить кодовую устойчивость, т.е. устойчивость против определения закона формирования ПСП, а с другой – формировать последовательность элементов с требуемым основанием алфавита.

Прежде чем перейти к методам и средствам формирования таких последовательностей и изучению их структурных и ансамблевых свойств, приведем ряд основных понятий и определений из теории многомодульных преобразований, сформулировав их в виде утверждений.

Определение. Показателем a по модулю m (будем называть его $P_m(a)$) называется наименьший положительный показатель степени a, сравнимый с единицей по модулю m [2].

Согласно определению, $P_m(a)$ означает положительное число, такое что $a^{P_m(a)} \equiv 1(\mathrm{mod}\, m)$, причем при всех r, таких что $1 \leq r \leq P_m(a)$, $a_r \neq 1(\mathrm{mod}\, m)$.

Утверждение 1. Если a по модулю m принадлежит показателю $P_m(a)$, то числа

$$1 = a^0, a^1, \ldots, a^{P_m(a)-1}$$

по модулю m несравнимы.

Учитывая определение и утверждение 1, можно построить последовательность $\{X\}=\{x_1, x_2, , x_n\}$ вида

$$x_i = R_m\left(\theta^i\right), \; i = 0,1,\ldots, P_m(\theta), \qquad (3)$$

где $R_m(\theta^i)$ – остаток от деления целого числа θ^i на m, который будет иметь период $L = P_m(\mathrm{q})$, причем каждое значение x_i на периоде L встречается только один раз.

Для построения управляющей q-ичной ПСП $\{B\}=\{b_1, b_2, , b_n\}$ предлагается использовать следующее правило:

$$b_i = R_q\left(x_i\right) = R_q\left(R_m\left(\theta^i\right)\right), \; \mathrm{i} = 0,1,\ldots, \mathrm{P_m}(\theta), \qquad (4)$$

где $1 < q < m$, $q < P_m(\mathrm{q})$.

Пусть $m=p^\alpha$, где p – простое число, α – любое целое положительное число. Тогда существует первообразный элемент q по модулю m, который принадлежит показателю

$$P_m(\theta) = \varphi(m) = p^{\alpha-1}\left(p-1\right), \qquad (5)$$

где $\varphi(m)$ – функция Эйлера от m. Учитывая утверждение 1, правило формирования ПСП $\{B\}$ можно переписать в следующем виде:

$$b_i = R_q\left(x_i\right) = R_q\left(R_m\left(\theta^i\right)\right), \; 0 \leq i \leq p^{\alpha-1}\left(p-1\right), \qquad (6)$$

где $1 < q < p^{\mathrm{a}}$.

Частотой появления элемента a на отрезке периодической последовательности длиной в период будем называть отношение числа появления элемента a, т.е. числа элементов отрезка, совпадающих с a, к длине отрезка, т.е. числу элементов отрезка.

Определим частоту появления каждого из элементов 0,1,2,...,q_1-1 на отрезке последовательности b_i (6) длиной $\varphi(p^\alpha)$.

Утверждение 2. Пусть $p^{\alpha-1} = M_1 q + R_1$,
$p^\alpha = M_2 q + R_2$,

где $R_1 = R_q p^{\alpha-1}$, $R_2 = R_q p^\alpha$.

Тогда частота появления каждого из элементов $b_i=\{0,1,2,\ldots,q\text{-}1\}$ на отрезке последовательности b_i длиной $L = \varphi(p^\alpha) = p^{\alpha-1}(\mathrm{p}\text{-}1)$ равна либо M_2-M_1, либо M_2-M_1+1, либо M_2-M_1-1.

Доказательство. Обозначим через N_{p^α} упорядоченное множество наименьших неотрицательных вычетов по модулю p^α, т.е.

$$N_{p^\alpha} = \{0,1,2,\ldots, p^\alpha - 1\}. \quad (7)$$

Пусть $N^*_{p^\alpha}$ обозначает упорядоченное подмножество в N_{p^α}, состоящее из элементов взаимно-простых с p, а $\overline{N_{p^\alpha}}$ – упорядоченное подмножество в N_{p^α}, состоящее из элементов не взаимно-простых с p. Для N_{p^α}, $N^*_{p^\alpha}$, $\overline{N_{p^\alpha}}$ верны соотношения

$$\begin{aligned} N_{p^\alpha} &= N^*_{p^\alpha} \bigcup \overline{N_{p^\alpha}}, \\ \overline{N_{p^\alpha}} &= N_{p^\alpha} \setminus N^*_{p^\alpha}, \\ N^*_{p^\alpha} &\cap \overline{N_{p^\alpha}} = \varnothing. \end{aligned} \quad (8)$$

Перейдем в упорядоченном множестве N_{p^α} к остаткам по mod$q$. Получившееся множество остатков обозначим через $N_{p^\alpha,q}$. Тогда

$$N_{p^\alpha,q} = \{\underbrace{0,1,2,\ldots,q-1,\ldots,0,1,2,\ldots,q-1}_{M_2 \text{ групп}},0,1,2,\ldots,R_2-1\}. \quad (9)$$

Таким образом, в $N_{p^\alpha,q}$ элементы $0,1,2,\ldots,R_2$-1 встречаются M_2+1 раз каждый, а элементы $R_2, R_2+1,\ldots, q-1$ встречаются M_2 раз каждый.

Рассмотрим подмножество $\overline{N_{p^\alpha}}$. Его элементы имеют вид kp, $k = 0, 1, 2, \ldots, p^{\alpha-1}-1$ и подмножество $\overline{N_{p^\alpha}}$ содержит $p^{\alpha-1}$ элементов.

Если p имеет при делении на q остаток r=0 (p и q взаимно-простые), т.е. $r = R_q(p) \neq 0$, то остатки элементов множества $\overline{N_{p^\alpha}}$ при делении на q совпадают с остатками элементов последовательности вида $\{0, r, 2r,\ldots, (p^{\alpha-1}-1)r\}$, т.е.

$$\overline{N_{p^\alpha,q}} = \{\underbrace{0,r,2r,\ldots,(q-1)r,\ldots,0,r,2r,\ldots,(q-1)r}_{M_1 \text{ групп}}, 0,r,2r,\ldots,(R_1-1)r\}, \quad (10)$$

где (r,q)=1, иначе НОД(r,q) делил бы простое число p. Так что среди остатков элементов $0, r, 2r,\ldots, (q-1)r$ ровно по одному разу встречаются все остатки $0, 1, 2,\ldots, q$-1 (может быть в другом порядке), и все остатки элементов $0, r, 2r,\ldots, (R_1-1)r$ различны. Следовательно, среди элементов множества $\overline{N_{p^\alpha,q}}$ каждый остаток $0, 1, 2,\ldots, q$-1 встречается либо M_1, либо M_1+1 раз.

Если $r = R_q(p^{\alpha-1}) = 0$, то очевидно, что M_1=0.

Так как, не обращая внимания на упорядоченность, имеет место соотношение

$$\left\{1, R_{p^\alpha}(\theta), R_{p^\alpha}(\theta^2),\ldots, R_{p^\alpha}\left(\theta^{\varphi(p^\alpha)-1}\right)\right\} = N_{p^\alpha} \setminus \overline{N_{p^\alpha}},$$

то, не обращая внимание на упорядоченность, имеет место соотношение

$$\left\{b_0, b_1, b_2,\ldots, b_{\varphi(p^\alpha)-1}\right\} = N_{p^\alpha,q} \setminus \overline{N_{p^\alpha,q}}. \quad (11)$$

Из (11) следует справедливость утверждения 2, из которого вытекают следующие следствия.

Следствие 1. Если $r_1 = r_2 \neq 0$, $q < p^{\alpha-1}$, то все элементы последовательности $\{B\}=\{b_1, b_2,, b_n\}$ будут иметь одну и ту же частоту M_2 - M_1.

Действительно, пусть

$$p^\alpha = M_2 q + r_2,\ p^{\alpha-1} = M_1 q + r_1,$$

тогда $q(M_2 - M_1) = p^\alpha - p^{\alpha-1} = \varphi(p^\alpha)$ и, следовательно, $q \times \varphi(p^\alpha)$. Но так как $\varphi(p^\alpha)$ есть период последовательности x_n, то все элементы последовательности b_n имеют одну и ту же частоту.

Следствие 2. Если $r_1 = r_2 \neq 0$, $p^{\alpha-1} < q < p^\alpha$, то в последовательности b_n имеют место две частоты M_2 и $M_2 + 1$. Действительно, пусть

$$p^\alpha = M_2 q + r_2,\ p^{\alpha-1} = M_1 q + r_1,$$

так как $p^{\alpha-1} < q$, то $M_1 = 0$ и элементы 1,2, , r-1 будут иметь частоту $M_2 + 1$, а элементы r, $r + 1,\ldots, q$ - 1 – частоту M_2.

Следствие 3. Если $r_1 \neq r_2$, $2 \le q < p^\alpha$, то в последовательности b_n имеют место по крайней мере две частоты, одна из которых равна M_2 - M_1.

Определим наименьший положительный период периодической последовательности b_i.

Утверждение 3. Пусть последовательность b_i определяется как

$$b_i = R_q\left(R_{p^\alpha}\left(\theta^i\right)\right),\quad 0 \le i \le \varphi\left(p^\alpha\right), \quad (12)$$

где $2 \le q \le p^\alpha$, $q \neq p^z$, z=0,1,…,α-1.

Тогда последовательность b_i будет иметь положительный период $L = \varphi(p^\alpha)$.

Доказательство. Если $r_1 \neq r_2$, то (следствие 3) элементы последовательности b_i будут иметь различные частоты, одной из которых является частота $M_2 - M_1$.

Пусть последовательность b_i имеет период $d \le \varphi(p^\alpha)$, $kd = \varphi(p^\alpha)$, тогда k должно делить все частоты элементов 0, 1, 2,..., q-1. Но для любой пары частот имеют место соотношения

$$\begin{aligned} (M_2 - M_1,\ M_2 - M_1 - 1) &= 1, \\ (M_2 - M_1,\ M_2 - M_1 + 1) &= 1. \end{aligned}$$

Следовательно, $\varphi(p^\alpha) = kd = 1 \times d = d$.

Если в последовательности элементы имеют три различные частоты, тогда

$$\left(M_2 - M_1 + 1,\ M_2 - M_1,\ M_2 - M_1 - 1\right) = 1\ ,$$

и $d = \varphi\left(p^{\alpha}\right)$.

Если $r_1 = r_2$, $p^{\alpha-1} < q < p^{\alpha}$, тогда (следствие 2) имеет место соотношение $\left(M_2 + 1,\ M_2\right) = 1$ и, следовательно, $d = \varphi\left(p^{\alpha}\right)$.

Если $r_1 = r_2$, $q < p^{\alpha-1}$, то (следствие 1) все элементы последовательности b_i имеют одинаковую частоту M_2-M_1.

Пусть последовательность b_i имеет период $d \le \varphi\left(p^{\alpha}\right)$, $kd = \varphi\left(p^{\alpha}\right)$. Предположим, что последовательность b_i имеет четное количество периодов k. Тогда, очевидно, $b_0 = b_{\frac{\varphi\left(p^{\alpha}\right)}{2}}$ или

$$\theta^{0} \bmod p^{\alpha} \equiv \theta^{\frac{\varphi\left(p^{\alpha}\right)}{2}} \bmod p^{\alpha} \left(\bmod q\right).$$

Так как θ — первообразный элемент, а p — простое число, то

$$\theta^{\frac{\varphi\left(p^{\alpha}\right)}{2}} \equiv \left(p^{\alpha} - 1\right) \bmod p^{\alpha}.$$

Следовательно, можно записать

$$p^{\alpha} - 1 \equiv 1 \bmod \text{ или } p^{\alpha} \equiv 2 \bmod q\ .$$

Но, так как все элементы b_i имеют одну частоту, то $q \mid \varphi\left(p^{\alpha}\right)$ или $p^{\alpha-1}\left(p-1\right) \equiv 0 \bmod q$, откуда $p \equiv 1 \bmod q$. Тогда и $p^{\alpha} \equiv 1 \bmod q$. Таким образом, мы получили противоречие и, следовательно, последовательность b_i имеет период $L = \varphi(p^{\alpha})$.

Предположим, что последовательность b_i имеет нечетное количество периодов k.

Утверждение 3 доказано.

Таким образом, доказано, что используя выражение (6), можно построить m-ичные ПСП сколь угодно большого периода. При этом также теоретически обосновано, что на всей длине периода появление любого числа из интервала [0, q − 1] практически равновероятно, если выполняется условие (2).

Литература: 1. *Завадская Л.А., Фаль А.М.* Криптографически сильные генераторы псевдослучайных последовательностей // Безопасность информации.1997. №1. С.7-11. 2. *Горбенко И.Д.* Новые алгоритмы синтеза оптимальных дискретных сигналов // Радиотехника и электроника АН СССР, 1989. № 11. С.18-25. 3. *Горбенко И.Д.* Свойства характеристических дискретных сигналов // Радиотехника и электроника, 1990. № 2. С.11-20. 4. *Горбенко И.Д.* Теория дискретных сигналов. Ч 1. Оптимальные дискретные сигналы с одно-двух- уровневой ПФАК. Учебное пособие. МО СССР, 1983. С.55-69.

Поступила в редколлегию 07.06.99

Рецензент: д-р техн. наук Стасев Ю.В.

Гриненко Татьяна Алексеевна, инженер кафедры ЭВМ ХТУРЭ. Научные интересы: криптографические методы защиты информации в компьютерных системах. Адрес: Украина, 61726, Харьков, пр. Ленина, 14, тел. 40-94-13.

УДК 658.52.011.56

ОБ ОДНОМ ОБОБЩЕНИИ ЗАДАЧИ О НАЗНАЧЕНИЯХ

ПАНИШЕВ А.В., КОСТИКОВА М.В., СКАКАЛИНА Е.В.

Рассматриваются результаты изучения задачи о назначении. Предлагается использование теории паросочетаний для нахождения множества оптимальных решений задачи с заданными свойствами. Для ее решения предлагается модифицированный алгоритм Кана-Мункреса.

Изложенные здесь результаты представляют попытку углубить знания об известной задаче о назначении, располагающей широким спектром практических приложений на транспорте.

Доказано, что задача о назначении эффективно разрешима. При этом предполагается, что для достижения оптимума ее целевой функции достаточно найти единственное решение задачи.

Однако в практических ситуациях возникает потребность в нахождении множества оптимальных решений с заданными свойствами. Результаты изучения задачи о назначении в подобной постановке составляют содержание данной статьи. Они излагаются в терминах теории паросочетаний и связанной с нею проблемой оптимизации на графах и сетях. Используемые здесь определения и понятия заимствованы из [1].

Пусть π — совершенное паросочетание в двудольном графе $G=(V, E)$ с разбиением множества вершин $V=X\cup Y$, где X=Y, $|\alpha| = |Y| = m$ и $\left\|\beta_{ij}^{0}\right\|_m$ — заданная матрица весов ребер графа G. Определим вес паросочетания π как сумму весов его ребер (x_i, y_j) $x_i \in X, y_i \in Y$:

$$\rho(\pi) = \sum_{(x_i, y_j) \in \pi} \beta_{ij}^{0}\ .$$

Упорядочим по невозрастанию веса его ребер. В результате получим последовательность

$$\beta_1(\pi) \ge \beta_2(\pi) \ge \ldots \ge \beta_m(\pi)\ .$$

Будем говорить, что последовательность весов ребер совершенного паросочетания $\pi\,\beta_1(\pi) \ge \beta_2(\pi) \ge \ldots \ge \beta_m(\pi)$ совпадает с последовательностью весов ребер совершенного паросочетания $\pi'\,\beta_1(\pi') \ge \beta_2(\pi') \ge \ldots \ge \beta_m(\pi')$, если для всех i, $i = \overline{1, m}$, $\beta_i(\pi) = \beta_i(\pi')$.

Для заданной матрицы $\left\|\beta_{ij}^{0}\right\|_m$ найдем паросочетание π^* с максимальным весом:

$$\rho(\pi^*) = \max_{\pi \in p} \rho(\pi)\ , \qquad (1)$$

p — множество всех совершенных паросочетаний.