

## ЛИНЕЙНЫЙ КОНГРУЭНТНЫЙ МЕТОД

### 1. Понятие линейной конгруэнтной последовательности (ЛКП)

Псевдослучайной числовой последовательностью порядка  $k$  над кольцом  $Z$  целых чисел называется потенциально бесконечная периодическая числовая последовательность, определяемая по некоторому закону (как правило, по закону рекурсии) случайно выбираемыми  $k$  начальными элементами. Аналогично определяются псевдослучайные последовательности вычетов над кольцом  $Z_m$ . Как разновидность таких последовательностей в предыдущих лекциях изучались псевдослучайные линейные рекуррентные последовательности (ЛРП) над полем  $F_p$  и способ их порождения с помощью линейных регистров сдвига (ЛРС).

В этой лекции изучается *линейный конгруэнтный метод* (ЛКМ) (Д.Х.Лемер, 1948) порождения псевдослучайных последовательностей над кольцом  $Z_m$ .

**Определение 1.** *Линейная конгруэнтная последовательность (ЛКП) над кольцом  $Z_m$  получается при выбранном начальном значении  $X_0, X_0 > 0$ , по закону рекурсии*

$$X_{n+1} = (aX_n + c) \bmod m, \quad n \geq 0, \quad (1)$$

где

$X_n \in Z_m$  – вычеты по модулю  $m$ ,

$a, a \in Z_m, a \neq 0$  – множитель (его «полезными» значениями могут быть только значения  $a \geq 2$ ;

$c, c \in Z_m$  – приращение;

$m, m \in N, m \neq 1$  – модуль.

При выбранных указанных параметрах ЛКП обозначают четверкой

$$(X_0, a, c, m).$$

При  $c = 0$ , ЛКМ называется *мультипликативным* конгруэнтным методом (тогда и ЛКП называется мультипликативной), при  $c \neq 0$ , – *смешанным конгруэнтным методом*.

Используется также обозначение

$$b = a - 1, b \geq 1.$$

При  $a \geq 2$  индукцией по  $k$  получается обобщенная формула:

$$X_{n+k} = (a^k X_n + (a^k - 1)c/b) \bmod m, \quad k \geq 0, \quad n \geq 0.$$

При  $n = 0$  получаем

$$X_k = (a^k X_0 + (a^k - 1)c/b) \bmod m, \quad k \geq 0, \quad (2)$$

– формулу для вычисления  $k$ -го члена ЛКП, определяемой законом рекурсии (1).

**Пример 1.** При  $m = 8$ ,  $a = 7$ ,  $c = 3$ ,  $X_0 = 2$  получается ЛКП

$$2, 1, 2, 1, \dots$$

Параметры  $a$ ,  $c$  и  $m$  рекуррентного уравнения (1) выбираются из соображений

- ускорения вычислений,
- получения ЛКП ,большого периода,
- получения ЛКП с удовлетворительными статистическими свойствами.

## 2. Выбор модуля $m$

Наиболее просто вычисления осуществляются, если  $m = w = 2^p$ , где  $w$  – увеличенное на 1 максимальное представимое в машине целое число (тогда результат получается в младших разрядах произведения и не требуется выполнять деление по общему алгоритму деления для вычисления остатка произведения по модулю  $m$ ) :

$$a \cdot X \bmod m = (a \cdot X)]_p,$$

где  $p$  – длина машинного слова .<sup>1</sup>

Но тогда, если  $d$  – делитель числа  $m$  и  $Y_n = X_n \bmod 2^d$ , то

$$Y_{n+1} = (a \cdot Y_n + c) \bmod 2^d,$$

и последовательность, образованная  $d$  младшими разрядами членов ЛКП имеет период, не превышающий  $2^d$ . Таким образом, младшие цифры числа  $X_n$  получаются намного менее случайными, чем старшие.

Так, если  $m = w = 2^p$ ,  $d = 4$  то младшие четыре бита чисел  $X_n$  представляют числа  $Y_n = X_n \bmod 16$  образуют конгруэнтную последовательность с периодом, не превышающим 16. Самый младший бит либо не изменяется, либо строго чередуется от 0 к 1.

Подобный эффект не возникает при  $m = w \pm 1$ , в этих случаях младшие биты ведут себя также случайно, как и старшие.

---

<sup>1</sup>Запись  $y]_p$  обозначает число, образуемое  $p$  младшими разрядами  $2p$ -разрядного числа  $y$ . (Язык Ассемблера позволяет обращаться с такими числами и использовать их старшую и младшую части раздельно).

При этом сохраняется простота алгоритма приведения по модулю. Заметим, что

$$\begin{aligned} a \cdot X &= q(w+1) + r, & \text{то есть} \\ a \cdot X &= q(2^p+1) + r, & \text{или} \\ a \cdot X &= q(2^p) + (r+q), \end{aligned}$$

где  $r \leq w$ ,  $q$  – старшая "половина" произведения, а  $s = r + q$  – младшая. При этом  $0 \leq q < w$ ,  $0 \leq s < w$  так что имеем

$$\begin{aligned} -w &< -q \leq 0, \\ 0 &\leq s < w, \end{aligned}$$

откуда получаются неравенства

$$-w < s - q < w.$$

Таким образом,

$$(a \cdot X) \bmod (w+1) = r = (s-q) \bmod (w+1) \begin{cases} s-q, & \text{если } s-q \geq 0, \\ s-q+(w+1), & \text{если } s-q < 0 \end{cases}$$

**Пример 2.** а) Пусть  $w = 16$ ,  $a = 7$ ,  $X = 5$ ,  $m = w+1 = 17$ .

$$a \cdot X = 0111 \cdot 0101 = 0010 \ 0011,$$

$$q = 0010 = 2, \ s = 0011 = 3, \ s - q = 1 \rightarrow r = s - q = 1.$$

б) Пусть  $w = 16$ ,  $a = 7$ ,  $X = 7$ ,  $m = w+1 = 17$ .

$$a \cdot X = 0111 \cdot 0111 = 0011 \ 0001,$$

$$q = 0011 = 3, \ s = 0001 = 1, \ s - q = -2 \rightarrow r = s - q + w + 1 = -2 + 17 = 15.$$

Аналогично, если  $m = w-1$ , то

$$\begin{aligned} a \cdot X &= q(w-1) + r, & \text{то есть} \\ a \cdot X &= q(2^p-1) + r, & \text{или} \\ a \cdot X &= q(2^p) + (r-q), \end{aligned}$$

где  $q$  – старшая "половина" произведения, а  $s = r - q$  – младшая.

Поскольку  $0 \leq q < w$ ,  $0 \leq s \leq w-1$ , имеем  $0 \leq s+q < 2w-1$ . Таким образом,

$$(a \cdot X) \bmod (w-1) = r = (s+q) \bmod (w-1) \begin{cases} s+q, & \text{если } s+q < w-1, \\ s+q-(w-1), & \text{если } s+q \geq w-1 \end{cases}$$

**Пример 3.** а) Пусть  $w = 16$ ,  $a = 7$ ,  $X = 7$ ,  $m = w-1 = 15$ .

$$a \cdot X = 0111 \cdot 0111 = 0011 \ 0001,$$

$$q = 0011 = 3, \ s = 0001 = 1, \ s + q = 4 \rightarrow r = s + q = 4.$$

б) Пусть  $w = 16$ ,  $a = 7$ ,  $X = 11$ ,  $m = w-1 = 15$ .

$$a \cdot X = 0111 \cdot 1011 = 0100 \ 1101,$$

$$q = 0100 = 4, \ s = 1101 = 13, \ s + q = 17 \rightarrow r = s + q - (w-1) = 17 - 15 = 2.$$

### 3. Выбор множителя $a$ и приращения $c$

Выбор множителя и приращения должен обеспечить большую длину периода.<sup>2</sup>

Из «автоматной» интерпретации, как и для ЛРП, следует, что длина периода не превышает величины модуля  $m$  в общем случае и величины  $m - 1$  при  $c = 0$  (то есть для мультипликативного ЛКМ.)

**ЛКМ максимального периода  $m$ .** Исследуем все способы выбора  $a$  и  $c$ , дающие период длины  $m$ . Учитывая, что в периоде длины  $m$  каждое число от 0 до  $m - 1$  встречается ровно один раз, можем заключить, что выбор начального значения  $X_0$  на длину периода не влияет.

**Теорема 1.** *Длина периода линейной конгруэнтной последовательности равна  $m$  тогда и только тогда, когда*

*$c$  и  $m$  взаимно просты*

*$b = a - 1$  кратно  $p$  для любого простого  $p$ , являющегося делителем  $m$ ,*

*$b$  кратно 4, если  $m$  кратно 4.*

Иными словами, при разложении

$$m = 2^{e_0} p_1^{e_1} \dots p_t^{e_t}, \quad e_0 \geq 0, \quad e_i \geq 1, \quad i = 1, \dots, t$$

ЛКМ имеет максимальный период  $m$  тогда и только тогда, когда

$$\begin{aligned} (c, m) &= 1, \\ 2^{e_0} p_1 \dots p_t &\nmid b, \quad \text{если } e_0 < 2 \\ 2^2 p_1 \dots p_t &\nmid b, \quad \text{если } e_0 \geq 2. \end{aligned}$$

**Мультипликативные ЛКП наибольшего периода.** Факт, что не существуют мультипликативные ЛКП максимального периода согласуется с приведенной теоремой 1: при  $c = 0$ ,  $\text{НОД}(c, m) = 0$ .

Поэтому при  $c = 0$  исследуются способы выбора множителя  $a$ , обеспечивающие наибольшую возможную, хотя и меньшую, чем  $m$ , длину периода числовой последовательности.

В частности, число 0 не может войти в этот период, поскольку, все последующие числа будут нулевыми. Кроме того, если  $d$  – делитель модуля  $m$ , и если  $X_n$  кратно  $d$ , то все последующие числа  $X_{n+1}, X_{n+2} \dots$  также будут кратны числу  $d$ , а это ограничивает длину периода. Поэтому при  $c = 0$  желательно, чтобы  $X_n$  были взаимно просты с  $m$  для всех  $n$ .

Опишем условия, определяющие множитель  $a$  так, чтобы при нулевом приращении  $c$  длина периода была наибольшей.

**Лемма 1.** *Пусть разложение модуля  $m$  на простые множители имеет вид*

$$m = p_1^{e_1} \dots p_t^{e_t}.$$

---

<sup>2</sup>Однако, следует подчеркнуть, что большая длина периода еще не гарантирует случайность последовательности, а является одним из *необходимых* признаков случайности.

Длина  $\lambda$  периода ЛКП  $(X_0, a, c, m)$ , равна наименьшему общему кратному длин  $\lambda_j$  периодов линейных конгруэнтных последовательностей

$$(X_0 \bmod p_j^{e_j}, a \bmod p_j^{e_j}, c \bmod p_j^{e_j}, p_j^{e_j}), \quad 1 \leq j \leq t.$$

Таким образом, при  $c = 0$  период последовательности полностью определяется периодами  $\lambda(p^e)$  последовательностей таких, что  $m = p^e$ . Поэтому изучим эту ситуацию. В этом случае

$$X_{n+1} = aX_n \bmod m, \quad \text{откуда } X_n = a^n X_0 \bmod m.$$

Длина периода не превосходит  $e$ , если  $a$  кратно  $p$ . Поэтому выберем  $a$  взаимно простым с  $p^e$ . Тогда период  $\lambda(p^e)$  равен наименьшему целому  $\lambda$ , такому, что  $X_\lambda = a^\lambda X_0 \bmod p^e$ . Если наибольший общий делитель  $X_0$  и  $p^e$  есть  $p^f$ , это условие эквивалентно условию

$$a^\lambda \equiv 1 \pmod{p^{e-f}}. \quad (0.1)$$

По теореме Эйлера

$$a^{\varphi(p^{e-f})} \equiv 1 \pmod{p^{e-f}};$$

следовательно (с учетом следствия из теоремы Лагранжа),  $\lambda(p^e)$  есть делитель числа

$$\varphi(p^{e-f}) = p^{e-f-1}(p-1).$$

Тем более,  $\lambda(p^e)$  есть делитель числа

$$\varphi(p^e) = p^{e-1}(p-1).$$

Обратим внимание, что длина периода  $\lambda(p^e)$  есть порядок множителя  $a$ ,  $a \in Z_{p^e}$ . Он может быть вычислен по разложению числа  $\varphi(p^e) = p^e(p-1)$  на простые множители.

**Пример 4.** Рассмотрим ЛКП с нулевым смещением с множителем  $a = 5$ , модулем  $m = 3^3 = 27$ . вычислим  $\varphi(3^3) = 3^2 \cdot 2 = 18$ .

Заметим, что в кольце  $Z_{27} \text{ ord } 5=18$ , что подтверждает следующая таблица степеней этого элемента (в том, что порядок 5 совпадает с порядком мультипликативной группы можно убедиться и проще, проверив,  $5^{18/2} \bmod 27 \neq 1$   $5^{18/3} \bmod 27 \neq 1$ ).

$i$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
$5^i$	1	5	25	17	4	20	19	14	16	26	22	2	10	23	7	8	13	11

При  $X_0 = 2$  получаем период длины 18:

2,10,23,7,8,13,11,1,5,25,17,4,20,19,14,16,26,22.

Если в качестве множителя брать элементы меньшего порядка, то получим ЛКП меньших периодов

Соответственно имеем периоды:

$5^{2i} X_0$ ,  $i = 0, 1, 2, 3, 4, 5, 6, 7, 8 : 2, 23, 8, 11, 5, 17, 20, 14, 26$ .

$5^{3i} X_0$ ,  $i = 0, 1, 2, 3, 4, 5 : 2, 7, 11, 25, 20, 16$ .

$5^{6i} X_0$ ,  $i = 0, 1, 2 : 2, 11, 20$ .

$5^{9i} X_0$ ,  $i = 0, 1 : 2, 25$ .

Элемент  $a$  мультипликативной группы  $Z_m^*$  максимально возможного порядка  $\lambda(m)$  называется *первообразным элементом* этой группы. Из рассмотренных элементов  $5, 5^2=25, 5^3=17, 5^6=19$  и  $5^9=26$  первообразным элементом группы  $Z_{27}^*$  является элемент  $5$ .

**Примечание.** Если группа  $Z_m^*$  – циклическая, в частности, если  $m$  – простое число, то первообразный элемент по модулю  $m$  есть образующий элемент мультипликативной группы  $Z_m^*$ , а его порядок есть порядок этой группы. Рассмотренная выше группа  $Z_{27}^*$  циклическая и первообразный элемент является образующим элементом. Другими первообразными (и одновременно образующими) элементами этой группы являются элементы  $5^i, i = 5, 7, 11, 13, 15, 17$ . всего имеем 6 первообразных по числу степеней любого из них, взаимно простых с порядком группы. Общая формула для числа первообразных группы  $Z_{p^e}, p > 2$  следующая

$$\varphi(\varphi(p^e)) = \varphi(p^{e-1}(p-1)).$$

Можно найти точные значения  $\lambda(m)$  в следующих случаях:

$$\lambda(2) = 1, \lambda(4) = 2, \lambda(2^e) = 2^{e-2}, \text{ если } e \geq 3,$$

$$\lambda(p^e) = p^{e-1}(p-1), \text{ если } p > 2,$$

$$\lambda(p_1^{e_1} \cdots p_t^{e_t}) = \text{НОК}(\lambda(p_1^{e_1}), \dots, \lambda(p_t^{e_t})).$$

(3)

Пример. Рассмотрим группу  $Z_{2^4} = Z_{16}$ . В этом случае  $\lambda(m) = 2^2 = 4$ . Для элемента  $a = 5$  получаем множество из четырех различных степеней:  $5^4 = 5^0 = 1, 5^1 = 5, 5^2 = 9, 5^3 = 13$ . Остальные элементы группы  $Z_{16}^*$  получим как степени элемента  $11$ :  $11^4 = 11^0 = 1, 11^2 = 9, 11^3 = 3$ .

Далее рассмотрим группу  $Z_{3^2} = Z_9$ . В этом случае  $\lambda(m) = 3 \times 2 = 6$ . Для элемента  $a = 5$  получаем множество из шести различных степеней:  $5^6 = 5^0 = 1, 5^1 = 5, 5^2 = 7, 5^3 = 8, 5^4 = 4, 5^5 = 2$ .

Различные степени элемента  $5$  в кольце  $Z_{16 \times 9} = Z_{144}$  представлены в первой строке таблицы.

i	0	1	2	3	4	5	6	7	8	9	10	11
$5^i$	1	5	25	125	49	101	73	77	97	53	121	29
$11^i$	1	11	121	35	97	59	73	83	49	107	25	131
$13^i$	1	13	25	37	49	61	73	85	97	109	121	133

Заметим, что порядок группы  $Z_{144}^*$  равен  $\varphi(144) = 2^3 \times (3 \times 2) = 48$  и эта группа не циклическая.

$$Z_{144}^* = \{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, 47, 49,$$

$$53, 55, 59, 61, 65, 67, 71, 73, 77, 79, 83, 85, 89, 91, 95, 97$$

$$101, 103, 107, 109, 113, 115, 119, 121, 125, 127, 131, 133, 137, 139, 143\}$$

Элемент 5 является ее первообразным, но не образующим элементом. Некоторые другие элементы группы перечислены во второй и третьей строках таблицы как степени некоторых первообразных элементов. В качестве упражнения с помощью Алгебраического процессора можно найти прочие первообразные элементы и вычислить недостающие элементы группы. Все 16 первообразных :

$$\{1, 5, 11, 13, 29, 43, 47, 61, 67, 77, 83, 85, 101, 115, 131, 133\}$$

Справедлива теорема

**Теорема 2.** (Р. Кармайкл, 1910) Максимально возможный при  $s = 0$  период равен  $\lambda(t)$ , где  $\lambda(t)$  определяется выражениями (3). Такой период реализуется, если

- $X_0$  и  $t$  – взаимно простые числа;
- $a$  – первообразный элемент по модулю  $t$ .

Отсюда, если  $t$  – простое число, то можно получить период длины  $t - 1$ , то есть всего на единицу меньше максимально возможного при  $s \neq 0$ .

**Теорема 3.** Число  $a$  есть первообразный элемент по модулю  $p^e$  тогда и только тогда, когда

- а)  $p^e = 2$ ,  $a$  – нечетное; или  $p^e = 4$ ,  $a \bmod 4 = 3$ ; или  $p^e = 8$ ,  $a \bmod 8 = 3, 5, 7$ ; или  $p = 2$ ,  $e \geq 4$ ,  $a \bmod 8 = 3$  или 5;
- б)  $p$  – нечетное,  $e = 1$ ,  $a \not\equiv 0 \pmod{p}$  и  $a^{(p-1)/q} \not\equiv 1 \pmod{p}$  для любого простого делителя  $q$  числа  $p - 1$ ;
- в)  $p$  – нечетное,  $e > 1$ ,  $a$  удовлетворяет условиям б) и  $a^{p-1} \not\equiv 1 \pmod{p^2}$  (подразумевается, что  $p$  – простое).

Для важного случая  $t = 2^e$  при  $e \geq 4$  приведенные условия сводятся к единственному требованию, чтобы  $a \equiv 3$  или  $5 \pmod{8}$ . В этом случае четвертая часть всех возможных множителей дает максимальный период.

Приведем алгоритм 1 поиска элемента максимального порядка группы  $Z_{p \cdot q}^*$ . Пусть  $n = p \cdot q$ , где  $p$  и  $q$  – различные нечетные простые числа. Тогда  $Z_{p \cdot q}^*$  – группа порядка  $\varphi(n) = (p-1)(q-1)$ , не являющаяся циклической (см. рис. refcaption 1.7). Его можно обобщить для общего случая модуля.

#### 4. Необходимое условие обеспечения статистических свойств ЛКП. Мощность ЛКП.

Заметим, что множитель  $a = z^k + 1$ ,  $1 \leq k < e$ , где  $z$  – основание системы счисления, а  $e$  – длина машинного слова, удовлетворяет (при  $k > 1$ , если  $z = 2, e > 1$ ) условиям теоремы 1, то есть обеспечивает максимально возможный период. При этом можно также принять  $s = 1$ . Тогда рекуррентное соотношение примет вид

$$X_{n+1} = ((z^k + 1)X_n + 1) \bmod z^e.$$

### Алгоритм 1.

ВХОД: два различных нечетных простых числа  $p$  и  $q$ ,  
факторизация чисел  $p - 1$  и  $q - 1$ .  
ВЫХОД: элемент  $\alpha$  максимального порядка  $\text{НОК}(p - 1, q - 1)$   
группы  $Z_n^*$ ,  $n = p \cdot q$ .

1. Применяя известный алгоритм к  $G = Z_p^*$  и факторизацию числа  $p - 1$ , найти образующий элемент  $a$  группы  $G_p^*$ .
2. Применяя известный алгоритм к  $G = Z_q^*$  и факторизацию числа  $q - 1$ , найти образующий элемент  $b$  группы  $G_q^*$ .
3. Найти целое  $\alpha$ ,  $1 \leq \alpha \leq n - 1$ , удовлетворяющее сравнениям  
 $\alpha \equiv a \pmod{p}$ ,  
 $\alpha \equiv b \pmod{q}$ .
4. Вернуть  $\alpha$ .

Рис. 1: Алгоритм поиска элемента максимального порядка мультипликативной группы.

Правая часть легко вычислима, поскольку можно избежать умножения, заменив его сложением и сдвигом. Однако, такой вариант линейного соотношения, как правило, приводит к недостаточно случайным числам. Объяснение этого связано с концепцией мощности.

*Мощностью* линейной конгруэнтной последовательности максимального периода называется наименьшее целое число  $s$ , такое, что

$$b^s \equiv 0 \pmod{m}.$$

Такое число всегда существует, поскольку удовлетворяются условия Теоремы 1 (в частности, если  $b$  кратно любому простому делителю  $m$ ). При анализе можем считать, что  $X_n = 0$ , так как 0 принадлежит максимальному периоду.

Если  $a = 1$ , то мощность равна 1  $X_n \equiv cn \pmod{m}$ , то есть последовательность (1) явно не случайна. Не случайно выше отмечено, что «полезными» могут быть только значения множителя  $a \geq 2$ .

При  $X_0 = 0$ ,  $a \geq 2$ , по формуле общего члена ЛКП (2)

$$X_n = ((a^n - 1)c/b) \pmod{m}.$$

Разложение  $a^n - 1 = (b + 1)^n - 1$  по формуле бинома Ньютона позволяет заключить, что

$$\begin{aligned} X_n &= (((b + 1)^n - 1)c/b) \pmod{m} = \\ &= \left( \left( n + \binom{n}{2}b + \dots + \binom{n}{s}b^{s-1} \right) - 1 \right) c/b \pmod{m}, \end{aligned}$$



поскольку все члены с  $b^s$ ,  $b^{s+1}$  и т.д. можно опустить как кратные  $m$ .

При мощности 2

$$X_n \equiv \left( \frac{cn}{2} + c \binom{n}{2} - \frac{c}{2} \right) \pmod{m}.$$

Это также последовательность с определенно выраженной закономерностью: разность между соседними случайными числами

$$X_n - X_{n-1} \equiv cn - \frac{c}{2} \pmod{m}.$$

выражается простой зависимостью от  $n$ .

Для достаточно случайных последовательностей потребуется мощность не менее 5.

## 5. Спектральный тест

**Конечное преобразование Фурье.** Рассмотрим конечное преобразование Фурье функции, определённой на конечном множестве. Пусть  $F(t_1, t_2, \dots, t_n)$  – функция, определённая для всех комбинаций целых чисел  $t_k$ ,  $0 \leq t_k < m$  и принимающая комплексные значения. Преобразование Фурье функции  $F(t_1, t_2, \dots, t_n)$  определяется как функция

$$\begin{aligned} f(s_1, \dots, s_n) &= \\ &= \sum_{0 \leq t_1, \dots, t_n < m} \exp \left( \frac{-2\pi i}{m} (s_1 t_1 + \dots s_n t_n) \right) F(t_1, \dots, t_n), \end{aligned}$$

определённая для всех комбинаций целых  $s_k$ , Эта функция периодическая в том смысле, что

$$f(s_1, \dots, s_n) = f(s_1 \bmod m, \dots, s_n \bmod m).$$

Исходная функция восстанавливается по её преобразованию Фурье следующим образом:

$$\begin{aligned} F(t_1, t_2, \dots, t_n) &= \\ &= \frac{1}{m^n} \sum_{0 \leq s_1, \dots, s_n < m} \exp \left( \frac{-2\pi i}{m} (t_1 s_1 + \dots t_n s_n) \right) f(s_1, \dots, s_n). \end{aligned}$$

При этом величина

$$(1/m^n) f(s_1, \dots, s_n)$$

представляет  $n$ -мерную комплексную волну с частотами  $s_1/m, \dots, s_n/m$ .

**Функция предельной плотности для числовой последовательности и её конечное преобразование Фурье.** Будем использовать функцию

$$\delta(z) = \begin{cases} 1 & \text{если } z \text{ — целое,} \\ 0 & \text{если } z \text{ — не целое.} \end{cases}$$

Пусть дана бесконечная последовательность чисел  $X_0, X_1, \dots$ ,  $0 \leq X_k < m$  и пусть  $n$  – фиксированное натуральное число.

Определим функцию

$$F(t_1, \dots, t_n) = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{0 \leq k < N} \delta(X_k/t_1) \cdot \delta(X_{k+1}/t_2) \cdots \delta(X_{k+n-1}/t_n).$$

Эта функция равна предельной плотности числа появлений комбинации  $(t_1, \dots, t_n)$  в виде  $n$  следующих друг за другом элементами последовательности  $X_0, X_1, \dots$ . Если последовательность периодическая, то этот предел существует, причём для его вычисления можно принять  $N$  равным единице периода. Если последовательность действительно случайна, то все комбинации чисел появляются с одинаковой частотой и для любых  $t_1, \dots, t_n$  значение  $F(t_1, \dots, t_n) = \frac{1}{m^n}$ .

Преобразованием Фурье данной функции является функция

$$f(s_1, \dots, s_n) = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{0 \leq k < N} \exp \left( \frac{-2\pi i}{m} (s_1 X_k + s_2 X_{k+1} + \dots + s_n X_{k+n-1}) \right).$$

Если последовательность является действительно случайной, должен получиться образ константы  $\frac{1}{m^n}$ . То есть для случайной последовательности должно быть

$$f(s_1, \dots, s_n) = \begin{cases} 1, & \text{если } s_1 \equiv \dots \equiv s_n \equiv 0 \pmod{m}, \\ 0 & \text{в противном случае} \end{cases}. \quad (4)$$

Величину отклонения  $f(s_1, \dots, s_n)$  от значений (4), отвечающих действительно случайной последовательности можно использовать для оценки случайности.

Для линейной конгруэнтной последовательности, имеющей максимальный период, выражение для  $f(s_1, \dots, s_n)$  имеет более простой вид:

$$\begin{aligned} f(s_1, \dots, s_n) &= \frac{1}{m} \sum_{0 \leq k < m} \exp \left( \frac{-2\pi i}{m} (s_1 X_k + s_2 X_{k+1} + \dots + s_n X_{k+n-1}) \right) = \\ &= \frac{1}{m} \sum_{0 \leq k < m} \exp \left( \frac{-2\pi i}{m} \left( s(a)X_k + \frac{s(a) - s(1)}{a-1}c \right) \right), \end{aligned}$$

где

$$s(a) = s_1 + s_2 a + s_3 a^2 + \dots + s_n a^{n-1},$$

что следует из представления

$$X_{k+r} \equiv a^r X_k + \frac{a^r}{a-1} c \pmod{m},$$

полученного выше.

Учитывая, что в последовательности максимального периода встречаются все значения  $X_n$ , можно заключить, что

$$f(s_1, \dots, s_n) = \frac{1}{m} \sum_{0 \leq k < m} \exp \left( \frac{-2\pi i}{m} \left( s(a)k + \frac{s(a) - s(1)}{a-1}c \right) \right).$$

Рассматривая последнее выражение как сумму геометрической прогрессии, можно получить следующую основную формулу

$$f(s_1, \dots, s_n) = \exp \left( \frac{-2\pi i c}{m} \left( \frac{s(a) - s(1)}{a-1} \right) \right) \delta \left( \frac{s(a)}{m} \right). \quad (5)$$

Напомним, что  $f(s_1, \dots, s_n)/m^n$  интерпретируется физически как амплитуда  $n$ -мерной комплексной плоской волны, соответствующей "частоте"  $(s_1/m, \dots, s_n/m)$  этой волны. При этом по следующей формуле определяется "волновое число", соответствующее этой частоте:

$$\nu = \sqrt{s_1^2 + \dots + s_n^2}$$

при  $|s_k| \leq \frac{m}{2}$ ,  $1 \leq k < n$ .

Существование компонент с ненулевой частотой говорит об отклонении от случайности. Низкочастотные компоненты сильнее влияют на случайность, чем высокочастотные.

Формула (5) даёт "спектр" линейной конгруэнтной последовательности, указывая, какие типы волн имеются в преобразовании Фурье функции  $F(t_1, \dots, t_n)$ . Значение  $f(s_1, \dots, s_n) = 0$  всегда, кроме случаев, когда

$$s_1 + s_2 a + s_3 a^2 + \dots + s_n a^{n-1} \equiv 0 \pmod{m}, \quad (6)$$

то есть, когда  $|f(s_1, \dots, s_n)| = 1$ . Следовательно, для линейных конгруэнтных последовательностей с максимальным периодом наименьшее ненулевое волновое число в спектре равно

$$\nu_n = \min \sqrt{s_1^2 + s_2^2 + \dots + s_n^2}, \quad (7)$$

где минимум берётся по всем  $n$ -наборам целых чисел  $\{s_1, s_2, \dots, s_n\} \neq 0$ , удовлетворяющих условию (6). Если  $\nu_n$  – наименьшее значение волнового числа (7), для которого  $f(s_1, \dots, s_n) \neq 0$  в линейной конгруэнтной последовательности с максимальным периодом, то последовательность

$$X_0/m, X_1/m, X_2/m \dots$$

можно считать последовательностью случайных чисел, равномерно распределённых между 0 и 1 и представленных с "точностью" ("ошибкой округления")  $1/\nu_n$ , при этом имеется в виду независимость  $n$  последовательных значений при усреднении по полному периоду.

Действительно, если взять случайную последовательность целых чисел  $X_0, X_1, X_2 \dots$  с  $m = 2^e$ , то можно заметить, что при отбрасывании (обнулении) одного, двух и т.д. разрядов двоичных представлений таких чисел будут появляться компоненты с волновыми числами  $2^{e-1}$ ,  $2^{e-2}$ ,  $2^{e-3}$  и т.д.

Реализация спектрального теста описана в [1]. Соответствующий алгоритм применяется для оценки множителя  $a$  в линейной конгруэнтной последовательности с максимальным периодом при заданном модуле  $m$ . Алгоритм проверяет статистическую независимость последовательных отрезков из  $n$  чисел,  $n = 2, 3, 4$ .

В алгоритме предполагается, что заданы  $a$ ,  $m$  и  $n$ ; вычисляется  $q = \nu_n^2$ .

## 5. Теоретические тесты для линейного конгруэнтного метода

Линейный конгруэнтный метод позволяет применять *априорные* тесты, позволяющие теоретически предсказать результаты испытаний датчика теми или иными эмпирическими тестами, рассмотренными в предыдущей лекции. Такой подход позволяет более надёжно выбирать правильные значения параметров  $a$ ,  $m$  и  $c$  линейного конгруэнтного генератора.

Приведенные ниже результаты теории линейного конгруэнтного метода относятся к характеристикам линейного конгруэнтного генератора на полном периоде, что допустимо при проверке серий, интервалов, перестановок и т.д.

Суть следующей теоремы состоит в том, что если датчик обладает высокой мощностью, то примерно в половине случаев будет выполняться неравенство  $X_{n+1} < X_n$ .

**Теорема 4.** Пусть  $X_0$ ,  $a$ , и  $m$  определяют линейную конгруэнтную последовательность максимального периода; пусть  $b = a - 1$ ,  $d = \text{НОД}(m, b)$ . Тогда вероятность того, что  $X_{n+1} < X_n$ , равна  $\frac{1}{2} + r$ , где

$$r = \frac{(2(c \bmod d) - d)}{2m};$$

следовательно,  $|r| < \frac{d}{2m}$ .

Из теоремы следует, что практически при любом выборе  $a$  и  $c$  неравенство  $X_{n+1} < X_n$  будет выполняться с нужной частотой, во всяком случае на полном периоде, кроме тех случаев, когда  $d$  велико, что соответствует малой мощности и отвергается заранее.

Следующая теорема позволяет оценить коэффициент последовательной корреляции на полном периоде.

**Теорема 5.** Коэффициент последовательной корреляции при любых  $a$ ,  $m$ , и  $c$ , обеспечивающих максимальный период, определяется приближенно выражением

$$C \approx \frac{1}{a} \left( 1 - 6 \frac{c}{m} + 6 \left( \frac{c}{m} \right)^2 \right)$$

Из теоремы следует, что надо избегать малых значений  $a$ . В то же время, большие значения  $a$  еще не гарантируют малую корреляцию, поскольку ошибка в оценке может достигать  $a/m$ . При  $a = \sqrt{m}$  значения коэффициента корреляции ограничены величиной  $2/\sqrt{m}$ .

С помощью приведенных формул можно вычислять коэффициент корреляции между  $X_n$  и  $X_{n+t}$ , если вместо  $a$  и  $c$  подставлять

$$a_t = a^t \bmod m, \quad c_t = (a^t - 1)c/(a - 1) \bmod m.$$

Это следует из того, что

$$X_{n+1} = (aX_n + c) \bmod m.$$

Концепция мощности дает только один из критериев выбора множителя. Наиболее эффективным критерием является критерий на основе "спектрального теста" (см. выше). Он включает мощность и величину множителя.

## 6. Контрольные вопросы

1. Дайте определение линейной конгруэнтной последовательности и запишите формулу ее общего члена.
2. Каким образом выбирается модуль ЛКП, при котором исключается этап приведения по модулю  $m$  очередного вычисляемого элемента последовательности?

3. При каких условиях период ЛКП равен ее модулю  $m$ ?
4. Как определить максимальный период ЛКП?
5. При каких множителях ЛКП имеет заведомо слабые статистические свойства?
6. Какой спектральный параметр ЛКП контролируется спектральным тестом?
7. Какие еще теоретические тесты для ЛКП Вам известны? Литература.

[1] Кнут Д. искусство программирования для ЭВМ. М.: Мир. 1978. Кнут Д. искусство программирования. Т. 2, Киев, Санкт-Петербург: Вильямс. 2000.

[2] Иванов М.А., Чугунков И.В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. – М.: КУДИЦ-ОБРАЗ, 2003.