8 Линейный конгруэнтный метод

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.

8.1 Определение

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

$$X_{n+1} = (aX_n + c) \bmod m,\ n \geq 0, \qquad (8.1)$$

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 $c = 0$, – *смешанным конгруэнтным методом.*

Используется также обозначение

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

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

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

При $n = 0$ получаем

$$X_k = (a^k X_0 + (a^k - 1)c/b) \bmod m,\ k \geq 0, \qquad (8.2)$$

– формулу для вычисления k-го члена ЛКП, определяемой законом рекурсии (8.1).

Пример 8.1. При $m = 8,\ a = 7,\ c = 3, X_0 = 2$ получается ЛКП

$$2, 1, 2, 1, \ldots$$

Параметры a, c и m рекуррентного уравнения 8.1 выбираются из соображений

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

8.2 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 . [1]

Но тогда, если 2^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.

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

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

[1] 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).

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

$$\begin{array}{l} -w < -q \le 0, \\ 0 \le s < w, \end{array}$$

откуда получаются неравенства

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

Таким образом,

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

Пример 8.2. а) Пусть $w = 16,\ a = 7,\ X = 5,\ m = w + 1 = 17.$

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

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

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

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

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

Аналогично, если $m = w - 1$, то

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

где q – старшая "половина"произведения, а $s = r - q$ – младшая. Поскольку $0 \le q < w,\ 0 \le s \le w - 1$, имеем $0 \le s + q < 2w - 1$. Таким образом,

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

Пример 8.3. а) Пусть $w = 16,\ a = 7,\ X = 7,\ m = w - 1 = 15.$

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

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

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

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

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

8.3 Выбор множителя a и приращения c

Выбор множителя и приращения должен обеспечить большую длину периода. [2]

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.)

ЛКП 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 8.1 . *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

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

ЛКМ имеет максимальный период m тогда и только тогда, когда

$$\begin{array}{ll} (c,m) = 1, & \\ 2^{e_0} p_1 ... p_t | b, & \text{если } e_0 < 2 \\ 2^2 p_1 ... p_t | b, & \text{если } e_0 \geq 2. \end{array}$$

Мультипликативные ЛКП наибольшего периода. Факт, что не существуют мультипликативные ЛКП максимального периода согласуется с приведенной теоремой 8.1: при $c=0$, НОД$(c,m) = m$.

Поэтому при $c=0$ исследуются способы выбора множителя a, обеспечивающие наибольшую возможную длину периода числовой последовательности, хотя и меньшую, чем m .(число 0 не может войти в этот период, поскольку, все последующие числа будут нулевыми).

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

Лемма 8.1. *Пусть разложение модуля m на простые множители имеет вид*

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

Длина λ периода ЛКП (X_0, a, c, m), равна наименьшему общему кратному длин λ_j периодов линейных конгруэнтных последовательностей

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

[2]Однако, следует подчеркнуть, что большая длина периода еще не гарантирует случайность последовательности, а является одним из *необходимых* признаков случайности.

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

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

Если a кратно p, то последовательность имеет период (0) длины 1, и ненулевой предпериод, не превышающий e, поскольку в этом случае $X_e = a^e X_0 \mod p^e = 0$. Поэтому выберем a взаимно простым с p^e. Тогда период $\lambda(p^e)$ равен наименьшему целому λ, такому, что

$$X_\lambda = a^\lambda X_0 \bmod p^e = X_0 \bmod p^e,$$

что получается при

$$a^\lambda \equiv 1 \mod p^e. \qquad (8.3)$$

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

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

Обратим внимание, что при X_0, не кратном p, 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.

Если наибольший общий делитель X_0 и p^e есть p^f, то условие (8.3) эквивалентно условию

$$a^\lambda \equiv 1 (\mathrm{mod}\ p^{e-f}). \qquad (8.4)$$

По теореме Эйлера

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

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

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

Отсюда длина периода уменьшается в p^f раз.

Таким образом, множитель a следует выбирать из числа образующих элементов группы $Z^*_{p^e}$, а начальный элемент X_0 взаимно простым с p.

Пример 8.4. Рассмотрим ЛКП с нулевым смещением $c = 0$, множителем $a = 5$ и модулем $m = 3^3 = 27$. Вычислим $\varphi(3^3) = 3^2 \cdot 2 = 18$.

Заметим, что в кольце Z_{27} 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.

Приведем также периоды последовательностей (3, 5, 0, 27), (6, 5, 0, 27), и (18, 5, 0, 27), с начальными элементами, кратными $p = 3$.

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
$3 \cdot 5^i$	3	15	21	24	12	6	.	.	.	.	.	.	.	.	.	.	.	.
$6 \cdot 5^i$	6	3	15	21	24	12	.	.	.	.	.	.	.	.	.	.	.	.
$18 \cdot 5^i$	18	9	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.

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 – нечетное простое число, то первооообразный 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 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:

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

$\lambda(p^e) = p^{e-1}(p-1)$, если $p > 2$, (8.5)

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

Пример 8.5. 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 в числе степеней элементов

11: $11^4 = 11^0 = 1,\ 11^1 = 11,\ 11^2 = 9,\ 11^3 = 3;$

7: $7^2 = 7^0 = 1;\ 7^1 = 7;$

15: $15^2 = 15^0 = 1;\ 15^1 = 15.$

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 :

$$\{1, 5, 11, 13, 29, 43, 59, 61, 67, 77, 83, 85, 101, 115, 131, 133\}$$

Справедлива теорема

Теорема 8.2 (Р. Кармайкл, 1910) *Максимально возможный при* $c = 0$ *период равен* $\lambda(m)$, *где* $\lambda(m)$ *определяется выражениями* (8.5). *Такой период реализуется, если*

X_0 *и* m *– взаимно простые числа;*

a *– первообразный элемент по модулю* m.

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

Первообразный элемент можно искать, используя следующую теорему.

Теорема 8.3 *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,* $e = 1$, $a \not\equiv 0$ (mod) p *и* $a^{p^{e-1}(p-1)/q} \not\equiv 1 \pmod{p}$ *для любого простого делителя* q *числа* $p^{e-1}(p-1)$;

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

Приведем алгоритм 8.1 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. 1). Его можно обобщить для общего случая модуля.

8.4 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 8.1, то есть обеспечивает максимально возможный период. При этом можно также принять $c = 1$. Тогда рекуррентное соотношение примет вид

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

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

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

Алгоритм 8.1

ВХОД: два различных нечетных простых числа p и q,
факторизация чисел $p-1$ и $q-1$.
ВЫХОД: элемент α максимального порядка 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 α, $1 \le \alpha \le n-1$, удовлетворяющее сравнениям
$\alpha \equiv a \pmod{p}$,
$\alpha \equiv b \pmod{q}$.
4. Вернуть α.

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

Такое число всегда существует, поскольку удовлетворяются условия Теоремы 8.1 (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 $X_n \equiv cn \bmod m$, то есть последовательность (8.1) явно не случайна. Не случайно выше отмечено, что «полезными» могут быть только значения множителя $a \ge 2$.

При $X_0 = 0,\ a \ge 2$, по формуле общего члена ЛКП (8.2)

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

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

$$X_n = (((b+1)^n - 1)c/b) \bmod m =$$

$$= \left(\left(n + \binom{n}{2} b + \cdots + \binom{n}{s} b^{s-1}\right) - 1)c/b)\right) \bmod m,$$

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.

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.