ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНІ ТА ОБЧИСЛЮВАЛЬНІ СИСТЕМИ І КОМПЛЕКСИ В ТЕХНОЛОГІЧНИХ ПРОЦЕСАХ

УДК 681.3.067

ОЦІНКА ПЕРІОДУ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ НА ОСНОВІ p-ЧИСЕЛ ФІБОНАЧЧІ

Є.В.Яремчук , О.Д. Азаров
Вінницький державний технічний університет

Вступ

Генератори послідовностей псевдовипадкових чисел (ПВЧ) знайшли широке застосування в багатьох галузях людської діяльності. Вони використовуються для моделювання, тестування та контролю складних систем та криптографічного захисту інформації.

Найбільш поширеними є лінійні конгруенц-генератори [1, 2]. У даній роботі розглядається лише один з багатьох видів таких генераторів, а саме, генератор, побудований на основі узагальнених послідовностей p-чисел Фібоначчі. Він потребує для обчислення кожного елемента послідовності лише три операції додавання-віднімання. Це найменша кількість з можливого. Математичну модель такого генератора можна зобразити у вигляді:

$$\begin{aligned} &< X_0 >= \{x_0, x_1, \ldots, x_p\}, \\ &< X >= \{x_{p+1}, x_{p+2}, \ldots, x_{T-1}\}, \\ &x_{i+1} = (x_i + x_{i-p}) \bmod m, \end{aligned} \tag{1}$$

де $< X_0 >$ – блок ініціалізації генератора; $< X >$ – послідовність, породжена генератором; m – модуль послідовності; p – параметр, який задає відстань між елементами, сума яких є наступним елементом послідовності.

Якщо характеристичний многочлен, що відповідає описаному генератору, є примітивним [3, 4], то згенерована послідовність буде мати максимальний період, який дорівнює:

$$T = m^{p+1} - 1. \tag{2}$$

Оскільки для генератора (1) характеристичний многочлен буде мати вигляд

$$h(x) = x^{p+1} + x^p + 1 ,$$

то його характер визначається лише параметром p.

Метою роботи є аналіз результатів визначення довжини послідовності ПВЧ, отриманої за допомогою генератора, характеристичний многочлен якого не є примітивним.

Дослідимо залежності довжини послідовності ПВЧ від параметрів p та m генератора. Нехай існує абстрактна функція $f(m, p)$, що визначає довжину періоду послідовності, заданої її двома аргументами.

Обробивши експериментальні дані, наведені в табл. 1, можна зробити такі два припущення:

1) для послідовностей, модулі яких можна представити як $m = a^k$, $k = 1, 2, \ldots$, має місце рівність:

$$f(a,p) = \frac{1}{2} f(a^2, p) = \ldots = \frac{1}{a^{k-1}} f(a^k, p);$$

2) періоди послідовностей, які мають модулі, кратні 6 ($m = 6k$, $k = 1, 2, \ldots$), при однакових p рівні:

$$f(6,p) = f(12,p) = \ldots = f(6k,p).$$

Періоди послідовностей ПВЧ

Таблиця 1

	p=1	p=2	p=3	p=4	p=5	p=6
M=2	3	7	15	21	63	127
M=3	8	8	80	78	728	728
m=4	6	14	30	42	126	254
M=5	20	31	312	24	3124	19531
M=6	24	56	240	546	6552	92456
M=7	16	57	342	336	2400	48
M=8	12	28	60	84	252	508
M=9	24	24	240	78	2184	2184
M=10	60	217	1560	168	196812	2480437
M=11	10	60	1330	120	118104	885775
M=12	24	56	240	546	6552	92456
M=13	28	168	2196	366	371292	5198088
M=14	48	399	1710	336	50400	6096
M=15	40	248	3120	312	568568	14218568
M=16	24	56	120	168	504	1016
M=17	36	288	96	288	88416	25640640
M=18	24	168	240	546	6552	277368
M=19	18	381	14480	180	2476098	49659541

Для перевірки припущення (1) розглянемо послідовності за модулем $m = 2$. Встановлено, що мають місце рівності

$$f(m,p) = 2^{p+1} - 1, \text{ для } p = 1,2,3,5,6,14,21, \tag{3}$$

$$f(m,p) = p(p+1), \text{ для } p = 4,8,16, \tag{4}$$

$$f(m,p) = (p+1)^2 - 1, \text{ для } p = 7,15. \tag{5}$$

Оскільки має місце рівність

$$f(2,p) = \frac{1}{2} f(4,p) = \frac{1}{4} f(8,p), \text{ де } p = 1,2,\ldots,6, \tag{6}$$

то формули (3)-(5) можна подати у вигляді:

$$f(m,p) = 2^{k-1}(2^{p+1} - 1), \text{ для } p = 1,2,3,5,6,14,21, \tag{7}$$

$$f(m,p) = 2^{k-1} p(p+1), \text{ для } p = 4,8,16, \tag{8}$$

$$f(m,p) = 2^{k-1}((p+1)^2 - 1), \text{ для } p = 7,15. \tag{9}$$

Тепер розглянемо послідовності за модулем $m = 3$. Отримаємо такі співвідношення:

$$f(m,p) = 3^{p+1} - 1, \text{ для } p = 1,2,3,5, \tag{10}$$

$$f(m,p) = 3^p - 1, \text{ для } p = 4,6. \tag{11}$$

Рівність (6) виконується і для ряду $m = 3^k$, $k = 1,2,\ldots$. Тоді представимо (6) у вигляді:

$$m = a^k, \quad a \in \{2,3\}, \quad k = 1,2,\ldots;$$

$$f(a,p) = \frac{1}{a} f(a^2,p) = \ldots = \frac{1}{a^{k-1}} f(a^k,p). \tag{12}$$

З урахуванням формул (7)-(12) маємо:

$$m = a^k, k = 1,2,\ldots;$$

$$f(m,p) = a^{k-1}(a^{p+1} - 1), \begin{cases} a = 2, & p = 1,2,3,5,6,14,21; \\ a = 3, & p = 1,3,5. \end{cases} \tag{13}$$

Усі послідовності, розглянуті вище, відносяться до одного типу, модуль яких можна представити

як $m = a^k$, $k = 1, 2, \ldots$, але існує ще два інших типи:

1) послідовності за модулем $m = n \cdot k$, де n, k – натуральні числа;

2) послідовності за модулем m, де m – просте число.

Розглянемо послідовності першого типу. Період послідовностей цього типу можна зобразити як

$$f(m, p) = C \cdot f(n, p) \cdot f(k, p), \qquad (14)$$

де $C\ (0 < C \le 1)$ – константа.

Наприклад, для $m = 6, n = 2, k = 3$ маємо:

$$p = 1, \quad T = 24 = f(2,1) \cdot f(3,1);$$
$$p = 2, \quad T = 56 = f(2,2) \cdot f(3,2);$$
$$p = 3, \quad T = 240 = \frac{1}{5} f(2,3) \cdot f(3,3);$$
$$p = 4, \quad T = 546 = \frac{1}{3} f(2,4) \cdot f(3,4);$$
$$p = 5, \quad T = 6552 = \frac{1}{7} f(2,1) \cdot f(3,1).$$

Потрібно зауважити, що для послідовностей за модулем $m = 12$ справедливі усі рівності, що й для $m = 6$, тобто справджується співвідношення 2.

Для повноти картини розглянемо ряд послідовностей за модулем $m = 18$. Для них виконується рівність (14) і в даному випадку існує два можливих розкладання на множники числа 18: $n_1 = 2, k_1 = 9$ та $n_2 = 3, k_2 = 6$. Але маємо:

$$f(18,1) = f(2,1) \cdot f(3,1) = f(6,1) = f(9,1);$$
$$f(18,2) = f(2,2) \cdot f(9,2) = 3 f(2,2) \cdot f(3,2);$$
$$f(18,3) = \frac{1}{5} f(2,3) \cdot f(3,3) = f(6,3) = f(9,3);$$
$$f(18,4) = \frac{1}{3} f(2,4) \cdot f(3,4) = f(6,4) = \frac{1}{3} f(2,4) \cdot f(9,4);$$
$$f(18,5) = \frac{1}{7} f(2,5) \cdot f(3,5) = f(6,5) = \frac{1}{21} f(2,5) \cdot f(9,5);$$
$$f(18,6) = 3 f(6,6) = f(2,6) \cdot f(9,6).$$

Отже, для $p = 1, 3, 4, 5$ справджується припущення 2.

Тепер розглянемо тип послідовностей, у яких модуль m – просте число. Для них справедливі співвідношення таких двох видів:

1) $f(m, p) = a\left(m^p \pm 1\right)$;

2) $f(m, p) = m\left(m\left(\ldots m\left(m \cdot a \pm a\right) \ldots \pm a\right) \pm a\right) \pm a$.

Для прикладу розглянемо послідовності за модулем $m = 11$. Маємо:

$$p = 1, \quad T = f(11,1) = 10 = 11 - 1;$$
$$p = 2, \quad T = f(11,2) = 60 = 6(11 - 1);$$
$$p = 3, \quad T = f(11,3) = 1330 = 11^3 - 1;$$
$$p = 4, \quad T = f(11,4) = 120 = 11^2 - 1;$$
$$p = 5, \quad T = f(11,5) = 118104 = 11\left(11\left(11\left(11\left(11 - 3\right) + 1\right) - 3\right) + 1\right) - 3;$$
$$p = 6, \quad T = f(11,6) = 11\left(11\left(11\left(11\left(11 \cdot 5 + 5\right) + 5\right) + 5\right) + 5\right).$$

Таким чином, можна записати нерівність для функції визначення періоду послідовності, яка буде справедлива для переважної більшості розглянутих випадків:

$$m^{p-1} - 1 \le f(m, p) \le m^{p+1} - 1. \qquad (15)$$

Висновки

Розроблені математичні моделі дозволяють отримувати наближені значення періодів послідовностей ПВЧ, що дає змогу використовувати на практиці усі можливі генератори, незалежно від характеру многочленів, які покладені в їх основу.

Обираючи відповідним чином значення параметрів m та p, можна регулювати довжину послідовності, що дозволяє заощадити ресурси обчислювальної техніки та збільшити швидкодію як програмних, так і апаратних реалізацій запропонованого генератора.

Література

1. Кнут Д. Искусство программирования для ЭВМ. Т.2. Получисленные алгоритмы. – М.: Мир, 1977. – 724 с.

2. Ярмолик В.Н., Демиденко С.Н. Генерирование и применение псевдослучайных сигналов в системах испытаний и контроля / Под. ред. А.М.Чеголина. – М.: Наука и техника, 1986. – 200 с.

3. Берлекэмп Э. Алгебраическая теория кодирования. – М.: Мир, 1971. – 478 с.

4. Макуильямс Ф., Слоан Н. Псевдослучайные последовательности и таблицы // ТИИЭР. – 1976. – № 12. – С. 80-95.

5. Сарвате Д.В., Пресли М.Б. Взаимно-кореляционные свойства псевдослучайных и родственных последовательностей // ТИИЭР. – 1980. – № 5. – С. 59-90.

УДК 681.325

РЕШЕНИЯ ТРАЕКТОРНЫХ ЗАДАЧ В МИКРОСИСТЕМАХ УПРАВЛЕНИЯ ТАБЛИЧНО-АЛГОРИТМИЧЕСКИМ СПОСОБОМ

В.М. Лукашенко

Черкасский инженерно-технологический институт

Важнейшим звеном в системах управления движением автоматизированных устройств – металлообрабатывающих станков, роботов-манипуляторов, чертежно-графических автоматов, оперативных устройств визуального отображения информации является использование микропроцессорных средств (МПС). В функции МПС систем числового программного управления (ЧПУ) для многокоординатного контурного управления входит, наряду с другими, и область с экстремальными, критичными по времени задачами интерполяции и регулирования с высокой точностью и помехоустойчивостью микропроцессорных средств.

Известно, что микропроцессорные средства характеризуются относительно низким быстродействием, которое дополнительно усугубляется ограниченной, с точки зрения вычислительных возможностей, системой команд и длиной слова, что заставляет работать с операндами двойной и тройной длины [1]. Аппаратурное решение линейной и круговой кодовой интерполяции функций вида:

$$Y = R \text{Ч} \sin(a); \quad X = R \text{Ч} \cos(a),$$

где R-радиус интерполируемой окружности либо величина межтактового приращения по длине интерполируемой прямой; а - центральный угол окружности либо угол наклона прямой, таких задач может быть осуществлено как за счет создания специализированных и проблемно-ориентированных, так и реализации вычислителей на существующих БИС-структурах.

Анализ методов и средств решения траекторных задач, учитывающий специфику контуров деталей, обрабатываемых на станках с ЧПУ, ограниченных отрезками прямых и дуг окружностей (до 95%), специфику применяемых средств, возможность использования методов для решения широкого круга траекторных задач без существенного изменения структуры алгоритмов показал, что эффективным при сокращении объема памяти, уменьшении времени вычисления и, как следствие, повышение надежности функционирования является использование таблично-алгоритмического метода.

Суть таблично-алгоритмических методов состоит в реализации определенной последовательности элементарных актов по использованию множества значений констант, соответствующих исходным данным, необходимых для получения результата [2-4]. Общим характерным признаком этих методов