

О многомерной версии алгоритма Берлекэмп—Месси

Пеленицын А. М.
ulysses4ever@gmail.com

Кафедра алгебры и дискретной математики
Факультет математики, механики и компьютерных наук
Южный федеральный университет

16 октября 2009 г.

1 Одномерный случай

- Линейные рекуррентные последовательности
- Задача
- Алгоритм

2 Многомерный случай

- Последовательности и полиномы
- Задача
- Алгоритм

3 Приложения

Определение линейной рекуррентной последовательности

(Одномерная) Последовательность: $u: \mathbb{N}_0 \rightarrow \mathbb{F}_{\tilde{q}}$ ($\mathbb{N}_0 = \{0, 1, \dots\}$).

u — линейная рекуррентная последовательность (ЛРП), если существуют $\{a_i\}_{i=0}^{k-1}$, такие что:

$$u_{n+k} = \sum_{i=0}^{k-1} a_i u_{i+n}, \quad n \in \mathbb{N}_0.$$

Тогда

- k — порядок ЛРП u ,
- $\{a_i\}_{i=0}^{k-1}$ — закон рекурсии ЛРП u .

Всем известный пример:

$$f_{n+2} = f_n + f_{n+1}$$

Закон рекурсии: $a_0 = 1$, $a_1 = 1$, порядок — 2.


Описание класса ЛРП

Теорема

Класс ЛРП совпадает с классом периодических последовательностей.

Доказательство

- 1 Пусть u — периодическая. Существуют p и r , т. ч. $u_{n+p} = u_n$, $n \geq r$. Значит u — ЛРП с законом рекурсии $a_r = 1$ и $a_i = 0$, где $i \in [0, p-1]_{\mathbb{N}_0} \setminus \{r\}$, порядка $p+r$.
- 2 Пусть u — ЛРП порядка k с законом рекурсии $\{a_i\}$.
 - $\bar{u}_n = (u_n, u_{n+1}, \dots, u_{n+k-1})$ — **вектор n -го состояния**, он вполне определяет всю последовательность; в частности, если $\bar{u}_i = \bar{u}_j$, то $\bar{u}_{i+1} = \bar{u}_{j+1}$.
 - В последовательности $\bar{u}_0, \bar{u}_1, \dots$ лишь конечное число различных элементов, потому она периодическая.

Значит, и u периодическая. 

Минимальный многочлен I

Для ЛРП u существует более одного закона рекурсии. Есть ли между ними связь? — **Да**, её можно описать в алгебраических терминах.

Пусть $\{a_i\}_{i=0}^{k-1}$ — закон рекурсии u . Назовём **характеристическим многочленом** u нормированный многочлен:

$$f(x) = x^k - \sum_{i=0}^{k-1} a_i x^i.$$

Теорема

Пусть u — ЛРП, тогда существует единственный нормированный многочлен $m(x)$, такой что любой характеристический многочлен $f(x)$ ЛРП u делится на $m(x)$.

Следствие

Множество характеристических многочленов ЛРП u составляет все нормированные многочлены **идеала** $(m(x))$.

Степень $m(x)$ называется **линейной сложностью** ЛРП u .

Как найти $m(x)$?

От теории к практике

На практике нет возможности работать с бесконечными последовательностями.

На практике **задача такова**: для данных $\{u_i\}_{i=0}^m$ найти $f(x)$ минимальной степени (обозначим её k), такой что

$$\sum_{i=0}^k f_i u_{i+n-k} = 0, \quad n \in [k, m]_{\mathbb{N}_0}. \quad (1)$$

$$(f(x) = \sum_{i=0}^k f_i x^i.)$$

Похоже на СЛАУ?

Решение этой задачи — $f(x)$ — это минимальный полином ЛРП u , первые m членов которой совпадают с заданными $\{u_i\}_{i=0}^m$.

Закон рекурсии u : $\{-\frac{f_i}{f_k}\}_{i=0}^{k-1}$.

Для $f(x)$ степени k , последовательности u и $n \geq k$ введём обозначение:

$$f[u]_n \stackrel{\text{def}}{=} \sum_{i=0}^k f_i u_{i+n-k} \quad (\in \mathbb{F}_{\tilde{q}}).$$

На практике **задача такова**: для данных $\{u_i\}_{i=0}^m$ найти $f(x)$ минимальной степени (обозначим её k), такой что

$$f[u]_n = 0, \quad n \in [k, m]_{\mathbb{N}_0}.$$

Будем рассуждать **индуктивно**.

Пусть $f(x)$ — полином минимальной степени (обозначим её k), такой что

$$f[u]_n = 0, \quad k \leq n \leq p.$$

Как получить полином минимальной степени $f'(x)$ (обозначим её k'), такой что

$$f'[u]_n = 0, \quad k' \leq n \leq p+1?$$

- ❶ $f[u]_{p+1} = 0$ — нам повезло: $f'(x) \stackrel{\text{def}}{=} f(x)$.
- ❷ $f[u]_{p+1} \neq 0$ — придётся потрудиться.

Степень $f'(x)$

Лемма (о нижней границе для степени $f'(x)$)

Для степени k' полинома $f'(x)$ выполнено:

$$k' \geq p - k + 1.$$

Следствие

Для степени k' полинома $f'(x)$ выполнено

$$k' \geq \max(p - k + 1, k).$$

Следствие

Если будет найден $h(x)$, такой что

- ① $h[u]_n = 0, \quad n \leq p + 1,$
- ② $\deg h = \max(p - k + 1, k),$

то $f'(x) \stackrel{\text{def}}{=} h(x).$

«Формула Берлекэмпа»

позволяет построить $h(x)$, такой что

- ❶ $h[u]_n = 0, \quad n \leq p + 1,$
- ❷ $\deg h = \max(p - k + 1, k),$

на основе имеющегося $f(x)$ и некоторого полинома $g(x)$.

То есть

$$\begin{aligned} h(x) &= h(f, g), \\ f'(x) &\stackrel{\text{def}}{=} h(x). \end{aligned}$$

Уточним и завершим шаг индукции.

Пусть $f(x)$ — полином минимальной степени, такой что

$$f[u]_n = 0, \quad n \leq p,$$

и $g(x)$ подходящий для формулы Берлекэмпа полином.

Как получить $f'(x)$, $g'(x)$, такие что...?

Возможные варианты:

- ❶ $f[u]_{p+1} = 0$ — тогда $f'(x) \stackrel{\text{def}}{=} f(x)$, $g'(x) \stackrel{\text{def}}{=} g(x)$.
- ❷ $f[u]_{p+1} \neq 0$ — тогда $f'(x) = h(f, g)$, и
если $k' = k$, то $g'(x) \stackrel{\text{def}}{=} g(x)$, иначе $g'(x) \stackrel{\text{def}}{=} f(x)$.

$$h(f, g) = x^{r-s} f(x) - \frac{d_p}{d_q} x^{r-p+q-t} g(x).$$

Обозначения. $s, t, p, q, r \in \mathbb{N}_0$, $d_p, d_q \in \mathbb{F}_{\tilde{q}}$.

- $s = \deg f$, $t = \deg g$;
- p — текущий шаг, q — таков, что $\forall m < q: g[u]_m = 0$ и $g[u]_q \neq 0$;
- $d_p = f[u]_p$, $d_q = g[u]_q$;
- $r = \max(s, p - q + t)$.

Инициализация: $f = 1$.

$$h_0 = x^{p+1} - \frac{u_{p+1}}{u_p}, \text{ если } p < m,$$

$$h_0 = x^{m+1} \text{ иначе.}$$

- n -мерная последовательность u : $u: \mathbb{N}_0^n \rightarrow \mathbb{F}_{\tilde{q}}$.
- Если $\mathbf{m} \in \mathbb{N}_0^n$, то $x^{\mathbf{m}} = x_1^{m_1} x_2^{m_2} \dots x_n^{m_n}$.
- Полином $f(x)$ от n переменных: $f(x) = \sum_{i \in \Gamma_f} f_i x^i$.
Конечное множество $\Gamma_f (\subset \mathbb{N}_0^n)$ — «носитель» f . $f_i \in \mathbb{F}_{\tilde{q}}$.

Степень $f(x)$?

- [Blahut86] *Блейхут Р.* Теория и практика кодов, контролирующих ошибки: Пер. с англ. / М.: Мир, 1986.
- [LN88] *Лидл Р., Нидеррайтер Г.* Конечные поля: В 2-х т. / М.: Мир, 1988. 822 стр.
- [KKMN94] *V. L. Kurakin, A. S. Kuzmin, A. V. Mikhalev, A. A. Nechaev.* Linear recurring sequences over rings and modules. // I. of Math. Science. Contemporary Math. and it's Appl. Thematic surveys, vol. 10, 1994.
- [Sakata88] *Sakata S.* Finding a minimal set of linear recurring relations capable of generating a given finite two-dimensional array // J. Symb. Comp. 1988. Vol. 5. Pp. 321–337.
- [Sakata09] *Sakata S.* The BMS Algorithm // Chapter in Gröbner Bases, Coding, and Cryptography, Springer, 2009.
- [CLO'S00] *Кокс Д., Литтл Дж., О'Ши Д.* Идеалы, многообразия и алгоритмы. Введение в вычислительные аспекты алгебраической геометрии и коммутативной алгебры. / М.: Мир, 2000.