# О многомерной версии алгоритма Берлекэмпа—Месси

Пеленицын А. М.
ulysses4ever@gmail.com

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

30 октября 2009 г.

# Содержание

# Определение линейной рекуррентной последовательности

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

$u$ — 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. $u_{n+p} = u_n$, $n \geqslant r$. 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 $\{a_i\}$.*
   - *$\bar{u}_n = (u_n, u_{n+1}, \ldots, u_{n+k-1})$ — 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 $\bar{u}_0, \bar{u}_1, \ldots$ 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 $(m(x))$.*

# Минимальный многочлен II

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

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

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

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

# Удобные обозначения

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

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

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

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

# Индукция

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

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

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

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

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

# Степень $f'(x)$

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

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

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

## Следствие

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

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

## Следствие

*Если будет найден $h(x)$, такой что*

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

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

# «Формула Берлекэмпа»

позволяет построить $h(x)$, такой что

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

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

То есть

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

Уточним и завершим шаг индукции.

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

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

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

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

Возможные варианты:

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

# «Формула Берлекэмпа»

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

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 $g[u]_q \neq 0$;
- $d_p = f[u]_p$, $d_q = g[u]_q$;
- $r = \max(s, p - q + t)$.

# База индукции

Инициализация: $f = 1$.

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

# Степень $h(f,g)$ (связь $f$ и $g$)

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

где $r = \max(s, p-q+t)$.

**Вопрос**: $\deg(h) \stackrel{?}{=} \max(s, p-s+1)$.

1. $r = s$:

$$\deg(h) = \deg(f - x^{s-p+q-t}g) = \max(s, s-p+q) \stackrel{p \geq q}{=} s.$$

2. $r = p-q+t$:

$$\deg(h) = \deg(x^{p-q+t-s}f - g) = \max(p-q+t, t) =$$
$$\stackrel{p \geq q}{=} p-q+t \stackrel{*}{=} p-s+1,$$

(*) — по предположению индукции $s = q-t+1$.

# Основные определения

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

# Мономиальный порядок

Мономиальный порядок $<$ на множестве мономов $\mathrm{Mon}_n = \{x^{\boldsymbol{m}} \mid \boldsymbol{m} \in \mathbb{N}_0^n\}$ это бинарное отношение, обладающее свойствами:

1. $<$ — полный порядок (линейный порядок, при котором любое $M \subset \mathrm{Mon}_n$ имеет наименьший элемент),
2. для $u, v, w \in \mathrm{Mon}_n$ если $u < v$, то $uw < vw$.

Пример.

$$x^{\boldsymbol{m}} < x^{\boldsymbol{k}} \iff \Big( (\sum_i m_i < \sum_i k_i) \vee (\sum_i m_i = \sum_i k_i) \wedge (\exists j \forall i > j : (m_i = k_i) \wedge (m_j < k_j)) \Big)$$

Зафиксируем $<$. Тогда определена функция $\deg\colon \mathbb{F}_{\tilde{q}}[x] \to \mathbb{N}_0^n$,

$$\deg(f) = \max\nolimits_< \Gamma_f .$$

# Порядки на $\mathbb{N}_0^n$

Мономиальный порядок на $(\mathrm{Mon}_n, \cdot)$ индуцирует полный порядок на $(\mathbb{N}_0^n, +)$, согласованный с полугрупповой структурой. Если $\boldsymbol{n} \in \mathbb{N}_0^n$, обозначим через $\boldsymbol{n}' \in \mathbb{N}_0^n$ точку, непосредственно следующую за $\boldsymbol{n}$ относительно этого порядка.

Определим ещё частичный порядок $\leqslant_{\mathrm{P}}$ на $\mathbb{N}_0^n$:

$$\boldsymbol{m} \leqslant_{\mathrm{P}} \boldsymbol{k} \Leftrightarrow \forall i : m_i \leqslant k_i.$$

В терминах мономов $\leqslant_{\mathrm{P}}$ означает делимость: если $\boldsymbol{m} \leqslant_{\mathrm{P}} \boldsymbol{k}$, то корректно определён моном $x^{\boldsymbol{k}}/x^{\boldsymbol{m}} = x^{\boldsymbol{k}-\boldsymbol{m}}$ ($\boldsymbol{k} - \boldsymbol{m} \in \mathbb{N}_0^n$).

Для $\boldsymbol{p}, \boldsymbol{q} \in \mathbb{N}_0^n$ введём обозначения для множеств точек:

$$\Sigma_{\boldsymbol{q}} = \{\boldsymbol{m} \in \mathbb{N}_0^n \mid \boldsymbol{q} \leqslant_{\mathrm{P}} \boldsymbol{m}\},$$
$$\Sigma_{\boldsymbol{q}}^{\boldsymbol{p}} = \{\boldsymbol{m} \in \mathbb{N}_0^n \mid \boldsymbol{q} \leqslant_{\mathrm{P}} \boldsymbol{m} < \boldsymbol{p}\},$$
$$\Gamma_{\boldsymbol{p}} = \{\boldsymbol{m} \in \mathbb{N}_0^n \mid \boldsymbol{m} \leqslant_{\mathrm{P}} \boldsymbol{p}\}.$$

# Линейные рекуррентные последовательности

$u$ называется линейной рекуррентной последовательностью, если существуют $\{f_{\boldsymbol{i}}\}_{\boldsymbol{i}\in\Gamma}$ ($\Gamma \subset \mathbb{N}_0^n$, $|\Gamma| < \infty$, $\boldsymbol{s} = \max_< \Gamma$), такие что:

$$\sum_{\boldsymbol{i}\in\Gamma} f_{\boldsymbol{i}} u_{\boldsymbol{m}+\boldsymbol{i}-\boldsymbol{s}} = 0 \quad \forall \boldsymbol{m} \in \Sigma_{\boldsymbol{s}}.$$

Как и прежде, определяется характеристический полином $f(x) = \sum_{\boldsymbol{i}\in\Gamma} f_{\boldsymbol{i}} x^{\boldsymbol{i}}$ для ЛРП $u$ и вводится обозначение:

$$f[u]_{\boldsymbol{m}} \stackrel{\text{def}}{=} \sum_{\boldsymbol{i}} f_{\boldsymbol{i}} u_{\boldsymbol{i}+\boldsymbol{m}-\boldsymbol{s}} \quad \forall \boldsymbol{m} \in \Sigma_{\boldsymbol{s}},$$

где $\boldsymbol{s} = \deg f$.

**Теорема**

*Множество $I(u)$ характеристических полиномов ЛРП $u$ является идеалом в $\mathbb{F}_{\tilde{q}}[x]$.*

- идеалы в $\mathbb{F}_{\tilde{q}}[x]$ не являются главными;
- однако справедлива

**Теорема («Гильберта о базисе»)**

*Любой идеал $I \subset \mathbb{F}_{\tilde{q}}[x]$ конечнопорождён, т. е. существуют $\{f_i(x)\}_{i=1}^{k}$, такие что*

$$I = \{f_1 g_1 + \ldots + f_k g_k \mid g_1(x), \ldots, g_k(x) \in \mathbb{F}_{\tilde{q}}[x]\} \stackrel{\text{def}}{=} \langle f_1, \ldots, f_k \rangle.$$

# Базовые сведения о $\mathbb{F}_{\tilde{q}}[x]$-идеалах II [CLO'S00]

- базис существенно неединственен (в частности, разные базисы могут содержать разное количество элементов);
- однако существуют «хорошие» базисы: базисы Грёбнера

**Определение**

*Набор полиномов $\{f_i(x)\}_{i=1}^{k} \subset I$ называется базисом Грёбнера идеала $I$, если:*

$$\forall g \in I\ \exists i : \deg f_i \leqslant_P \deg g .$$

*В этом случае $I = \langle f_1, \ldots, f_k \rangle$.*

**Определение**

*Нормированный базис Грёбнера $\{f_i(x)\}_{i=1}^{k}$ идеала $I$ называется минимальным базисом Грёбнера, если:*

$$\forall i \forall j \neq i : \deg f_i \nleqslant_P \deg f_j .$$

# Задача

Рассмотрим отрезок последовательности $u^{\mathbf{r}}: \Sigma_{\mathbf{0}}^{\mathbf{r}} \to \mathbb{F}_{\tilde{q}}$. Для любого $f \in \mathbb{F}_{\tilde{q}}[x]$ условие

$$\forall \boldsymbol{m} \in \Sigma_{\deg f}^{\mathbf{r}}: f[u]_{\boldsymbol{m}} = 0$$

будем записывать просто $f[u^{\mathbf{r}}] = 0$ или кратко: $f[u] = 0$.

## Определение

*Множество нормированных полиномов $F = \{f_i(x)\}_{i=1}^{k}$ называется минимальным множеством для отрезка последовательности $u^{\mathbf{r}}: \Sigma_{\mathbf{0}}^{\mathbf{r}} \to \mathbb{F}_{\tilde{q}}$, если выполнены условия:*

1. $\forall i: f_i[u] = 0;$
2. $\forall g(x): (g[u] = 0) \to (\exists i: \deg f_i \leqslant_P \deg g);$
3. $\forall i\, \forall j \neq i: \deg f_i \nleqslant_P \deg f_j.$

**Как найти минимальное множество для отрезка $u^{\mathbf{r}}$?**

# Класс минимальных множеств

Множество минимальных множеств отрезка последовательности $u^{\mathbf{r}} : \Sigma_{\mathbf{0}}^{\mathbf{r}} \to \mathbb{F}_{\tilde{q}}$ обозначим $\mathscr{F}(u^{\mathbf{r}})$.

# Как выглядит $\deg(\{f(x) \mid f[u] = 0\})$?

Пусть $F \in \mathscr{F}(u^{\boldsymbol{r}})$. Обозначим:

$$\Sigma(u^{\boldsymbol{r}}) \stackrel{\text{def}}{=} \bigcup_{f \in F} \Sigma_{\deg f},$$

$$\Delta(u^{\boldsymbol{r}}) \stackrel{\text{def}}{=} \Sigma_{\boldsymbol{0}} \setminus \Sigma.$$

Для краткости можно писать $\Sigma(\boldsymbol{r})$, $\Delta(\boldsymbol{r})$.

# Индукция

Будем рассуждать индуктивно.

Пусть $\boldsymbol{p} < \boldsymbol{r}$, $F \in \mathscr{F}(u^{\boldsymbol{p}})$, $G \subset \mathbb{F}_{\tilde{q}}[x]$ $(|G| < \infty)$.

Необходимо найти $F' \in \mathscr{F}(u^{\boldsymbol{p}'})$, $G' \subset \mathbb{F}_{\tilde{q}}[x]$ $(|G'| < \infty)$.

Для каждого $f \in F$ есть две возможности:

1. $f[u]_{\boldsymbol{p}} = 0$ — тогда $f \in F'$.
2. $f[u]_{\boldsymbol{p}} \neq 0$ — ...

# Связь $F$ и $G$

$\forall g \in G \; \exists \boldsymbol{q} : g \in F(u^{\boldsymbol{q}}) \wedge g[u]_{\boldsymbol{q}} \neq 0.$

**Требование**: $\{\boldsymbol{q} - \deg g | g \in G\} = \max_{\leqslant_{\mathrm{P}}} \Delta(u^r).$

# Лемма о границе для степени $f'(x) \in F'$

Обозначим $F_{\mathrm{fail}} = \{f \in F \mid f[u]_{\boldsymbol{p}} \neq 0\}$.

**Лемма**

*Пусть* $f(x) \in F_{\mathrm{fail}}$, *тогда не существует* $f'(x) \in F'$, *такого что:*

$$\deg f' \leqslant_P (\boldsymbol{p} - \deg f).$$

*То есть* $\deg f' \in \Sigma_{\mathbf{0}} \setminus \Gamma_{\boldsymbol{p} - \deg f}$.

**Следствие**

*Пусть* $\Gamma = \bigcup_{f \in F_{\mathrm{fail}}} \Gamma_{\boldsymbol{p} - \deg f}$, *тогда*

$$\deg(F') \subset (\Sigma(u^{\boldsymbol{p}}) \setminus \Gamma).$$

# Степень $f \in F_{\mathrm{fail}}$ и формула Берлекэмпа

1. Если $\boldsymbol{p} - \deg f \in \Delta(u^{\boldsymbol{p}})$, то на степень $f'$ нет дополнительных ограничений и формула Берлекэмпа $h(f, g)$ позволяет построить $f'$: $\deg f' = \deg f$.
   В качестве $g$ нужно взять такой элемент $G$, что $\boldsymbol{p} - \deg f \leqslant_{\mathrm{P}} \boldsymbol{q} - \deg g$.

$$h(f, g) = f - \frac{d_{\boldsymbol{p}}}{d_{\boldsymbol{q}}} x^{\boldsymbol{q} - \deg g - (\boldsymbol{p} - \deg f)} g.$$

2. Если $\boldsymbol{p} - \deg f \notin \Delta(u^{\boldsymbol{p}})$, ...

# $F_{\text{fall}}$

Остались нерассмотренными $f \in F_{\text{fail}}$, такие что $\boldsymbol{p} - \deg f \notin \Delta(u^{\boldsymbol{p}})$, обозначим их $F_{\text{fall}}$.

Для каждой пары $(f, g)$, где $f \in F_{\text{fall}}$, $g \in G$,

- если $\boldsymbol{s}' = \max(\deg f, \boldsymbol{p} - \boldsymbol{q} + \deg g)$ минимальна по $\leqslant_{\mathrm{P}}$ в $S' = \{\max(\deg f, \boldsymbol{p} - \boldsymbol{q} + \deg g) \mid f \in F_{\text{fall}}, g \in G\}$,
- то полином:
$$h(f, g) = x^{\boldsymbol{s}' - \deg f} f - \frac{d_{\boldsymbol{p}}}{d_{\boldsymbol{q}}} g$$
добавляется в $F'$.

# Вырожденный случай

Пусть $\hat{S}$ множество минимальных по $\leqslant_{\mathrm{P}}$ элементов в $\Sigma(u^{\boldsymbol{p}}) \setminus \Gamma_{\boldsymbol{p}}$.

Для каждого $\hat{\boldsymbol{s}} \in \hat{S}$, если не найдётся такого $\boldsymbol{s}' \in S'$, что $\boldsymbol{s}' \leqslant_{\mathrm{P}} \hat{\boldsymbol{s}}$, тогда для каждого $f \in F_{\mathrm{fall}}$, такого что $\deg f \leqslant_{\mathrm{P}} \hat{\boldsymbol{s}}$, полином

$$h(f) = x^{\boldsymbol{s}' - \deg f} f$$

добавляется в $F'$.

# Библиография


[Blahut86] *Блейхут Р.* Теория и практика кодов, контролирующих ошибки: Пер. с англ. / М.: Мир, 1986.

[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.

[KKMN94] *Kurakin V. L., Kuzmin A. S., Mikhalev A. V., Nechaev A. A.* Linear recurring sequences over rings and modules. // I. of Math. Science. Contemporary Math. and it's Appl. Thematic surveys, vol. 10, 1994.

[LN88] *Лидл Р., Нидеррайтер Г.* Конечные поля: В 2-х т. / М.: Мир, 1988. 822 стр.

[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. 1988. Pp. 321–337.

[Sakata90] *Sakata S.* Extension of the Berlekamp–Massey algorithm to N dimensions. // Inform. and Comput. 84, no. 2. 1990. Pp. 207–239.

[Sakata09] *Sakata S.* The BMS Algorithm // Chapter in Gröbner Bases, Coding, and Cryptography, Springer, 2009.