

# Алгоритм Берлекэмпса разложения на множители многочленов от одной переменной над конечным полем

Плешаков Алексей, М3439

15.10.2020

## 1 Постановка задачи

Пусть  $f(x) = x^d a_d + x^{d-1} a_{d-1} + \dots + a_0$  — многочлен от одной переменной,  $a_i \in GF(q = p^n)$ ,  $d = \deg(f(x)) \geq 2$ . Требуется разложить  $f(x)$  на множители в соответствующем конечном поле.

## 2 Подготовка

Если  $a, b$  — многочлены в кольце вычетов по модулю  $p$ ,  $p$  — простое, то  $(a + b)^p \equiv a^p + b^p \pmod{p}$ .

*Доказательство.* Распишем выражение с помощью бинома Ньютона:

$$(a + b)^p = a^p + \binom{p}{1} a^{p-1} b + \dots + \binom{p}{p-1} a b^{p-1} + b^p \equiv a^p + b^p \pmod{p}$$

□

Пусть  $a(x)$  — многочлен, тогда  $a(x^p) \equiv a(x)^p \pmod{p}$ .

*Доказательство.* Докажем утверждение индукцией по  $\deg(a(x))$ . Предположение верно при  $\deg(a(x)) = 0$ . В общем случае же  $a(x) = b(x) + a_n x^n$ ,  $\deg(b(x)) < \deg(a(x))$ , и  $a(x)$  можно выразить следующим образом:

$$a(x) = (b(x) + a_n x^n)^p = a(x)^p + (a_n x^n)^p = b(x^p) + a_n x_{np} = a(x^p)$$

□

## 3 Переход к задаче попроще

Пусть

$$f(x) = f_1(x)_1^{e_1} f_2(x)_2^{e_2} \dots f_k(x)_k^{e_k}$$

где  $f_i$  — неприводимые многочлены, входящие в разложение со степенями  $e_i$ . Покажем, что нахождение разложения  $\prod_0^n f_i(x)^{e_i}$  сводится к нахождению разложения многочлена

$$g(x) = g_1(x) g_2(x) \dots g_k(x)$$

не имеющего кратных неприводимых множителей. В самом деле, если будет найдено разложение  $g(x)$ , то, при условии, что возможно декомпозировать  $f(x)$  на совокупность различных  $g_j(x)_{j=0}^t$ , можно будет получить степени  $f_i(x)$ . Рассмотрим метод, позволяющий декомпозировать  $f(x)$ .

### 3.1 Square-free decomposition

Предположим, что  $f(x)$  представлен в виде произведения линейных множителей:

$$f(x) = \prod_{i=1}^n (x - a_i)^{n_i}$$

В таком случае производная  $f'$ , посчитанная чисто алгебраическим методом по коэффициентам  $f$ , равна

$$f' = \sum_{i=1}^n n_i (x - a_i)^{n_i-1} \prod_{i \neq j, j=1}^n (x - a_j)^{n_j}$$

Заметим, что, для любого  $i$ ,  $(x - a_i)^{n_i-1}$  делит  $f$  и  $f'$ . Более того, каждый многочлен, делящий  $f$ , является произведением  $(x - a_i)$  в степенях, не превосходящих соответствующие  $n_i$ . Таким образом, наибольший общий делитель  $g = \gcd(f, f')$  почти определен: это произведение  $(x - a_i)$  в степенях  $n_i$  или  $n_i - 1$ . Но эта степень не может быть равной  $n_i$ , так как в таком случае ровно одно слагаемое  $f'$  не будет делиться на  $g$ , а, значит, и  $f'$  не будет делиться на  $g$ . Таким образом,

$$\gcd(f, f') = \prod_{i=1}^n (x - a_i)^{n_i-1}$$

Значит,  $\frac{f}{\gcd(f, f')} = \prod_{i=1}^n (x - a_i)$ . Обозначим эту величину как  $q$ . Далее,

$$\gcd(q, \gcd(f, f')) = \prod_{i=1, n_i > 1}^n (x - a_i)$$

, и, соответственно,

$$\frac{q}{\gcd(q, \gcd(f, f'))} = \prod_{i=1, n_i=1}^n (x - a_i) = g(x)$$

Заметим, что рассуждения выше не работают для многочленов с нулевой производной. Обработаем эти случаи следующим образом:

Пусть  $\gcd(f, f') = f$ , тогда  $f' = 0$ . Такое равенство может выполняться лишь в том случае, когда каждый моном  $f$  является точной  $p$ -й степенью (так как  $p$  является характеристикой конечного поля). Тогда  $f = g(x)^p$ , и для вычисления декомпозиции мы должны рекурсивно применить алгоритм к  $g$ .

Вышеприведенным образом оказывается возможно вычислить  $g(x)$ , являющийся произведением всех множителей, входящих в  $f(x)$  в первой степени. Более того, было получено значение  $\gcd(f, f')$ , которое имеет все те же множители, что и  $f$ , но с уменьшенными на единицу показателями степеней. Если примененный к  $f$  алгоритм применить к  $\gcd(f, f')$ , можно получить значение  $g$ , являющееся произведением всех множителей  $f$  второй степени. Действуя по аналогии, можно представить  $f$  в виде  $\prod g_i^i$ , где  $g_i$  — произведение всех множителей  $f$  степени  $i$ . Каждый из  $g_i$  при этом не имеет множителей степеней более первой, и все  $g_i$  взаимно просты. Такое разложение  $f$  называется **square free decomposition**. Вышеприведенное сведение можно выполнить за  $\mathcal{O}(d^3 \log d) \subset \mathcal{O}(qrd^2)$ , где  $r$  — количество неприводимых сомножителей  $f$ .

## 4 Основной случай

Пусть

$$f(x) = f_1(x)f_2(x) \dots f_k(x)$$

где  $f_i$  — неприводимые многочлены. Необходимо найти разложение  $\{f_1(x), f_2(x), \dots, f_k(x)\}$ . Примем во внимание факт, что  $f_i$  взаимно просты.

Пусть  $s_1, s_2, \dots, s_k$  — некоторые элементы поля  $GF(q)$ . По китайской теореме об остатках, существует полином

$$v \equiv s_i \pmod{f_i(x)} \quad (1)$$

. Степень  $v$  при этом не превосходит произведение  $f_i$ , то есть  $f$ . Такой полином может нам пригодиться, так как если  $s_i \neq s_j$ , то  $\gcd(f, v - s_i)$  делится на  $f_i$ , при этом не делясь на  $f_j$ , и поэтому декомпозирует  $f$ . Выполняется следующее соотношение:

$$v(x)^q \equiv s_j^q \equiv s_j \equiv v(x) \pmod{f_j, q}$$

, и, по китайской теореме об остатках,

$$v(x)^q \equiv v(x) \pmod{f(x), q} \quad (2)$$

. Также, подставив в вышестоящее равенство  $x = v(x)$ , получим соотношение

$$v(x)^q - v(x) \equiv (v(x) - 0)(v(x) - 1) \dots (v(x) - (q - 1)) \pmod{q} \quad (3)$$

Таким образом, если  $v(x)$  удовлетворяет равенству (2),  $f(x)$  делит левую часть (3), и каждый из неприводимых сомножителей  $f_i$  является делителем одного полинома правой части (3). Это, в свою очередь, иллюстрирует то, что  $v$  эквивалентен элементу из поля  $GF(q)$ , а, значит, решения уравнения (1) совпадают с решениями уравнения (2).

Уточним, как алгоритмически получить решения (1). Рассмотрим матрицу

$$Q = \begin{pmatrix} q_{0,0} & q_{0,1} & \dots & q_{0,d-1} \\ q_{1,0} & q_{1,1} & \dots & q_{1,d-1} \\ \vdots & \vdots & & \vdots \\ q_{d-1,0} & q_{d-1,1} & \dots & q_{d-1,d-1} \end{pmatrix}$$

, где  $x^{qk} \equiv q_{k,d-1}x^{d-1} + \dots + q_{k,1}x + q_{k,0} \pmod{f(x), q}$ . Рассмотрим полином как вектор его коэффициентов; тогда умножение на  $Q$  будет соответствовать возведению этого полинома в степень  $q$ . Таким образом, решения (2) будут являться собственными векторами  $Q$  для собственного числа 1. Наконец, алгоритм Берлекэмпса будет выглядеть следующим образом:

1. Привести  $f(x)$  к соответствующему многочлену, не имеющему кратных неприводимых сомножителей.
2. Вычислить матрицу  $Q$ .
3. Найти собственные векторы  $Q$  для собственного значения 1. Одним из них всегда является вектор  $[1, 0, \dots, 0]$ , так как целые числа всегда являются решениями (2). Размер базиса собственных векторов соответствует количеству многочленов в разложении  $f(x)$ .
4. Вычислить  $\gcd(f, v_i - s)$  для каждого целого числа  $s$  по модулю  $q$ , где  $v_i$  — многочлены, соответствующие собственным векторам  $Q$ . С помощью этих вычислений получить разложение  $f(x)$ .

5. Если преобразование шага 1 оказалось нетривиальным, восстановить разложение исходного полинома по имеющемуся.

Асимптотикой алгоритма будет являться  $\mathcal{O}(d^3 + qrd^2)$ , где  $r$  — количество множителей в разложении.