Malaschonok G.I., Smirnov R.A. About composition of functions and a machine forms. The form of the function compositions for computer algebra system are discussed. The problem of calculation of limits and derivations of a composition of functions is considered.

Key words: canonical form, function compositions, machine forms of functions.

Поступила в редакцию 20 ноября 2009г.

УДК 004.421

ОБ АЛГОРИТМЕ ФАКТОРИЗАЦИИ ПОЛИНОМОВ МНОГИХ ПЕРЕМЕННЫХ[1]

© Г. И. Малашонок, Д. С. Ивашов

Ключевые слова: факторизация полиномов, полиномы многих переменных, компьютерная алгебра.

Приводится алгоритм факторизации полиномов многих переменных. Алгоритм опирается на алгоритм факторизации полиномов одной переменной и на методы гомоморфных образов в кольцах полиномов.

Одной из очень важных задач компьютерной алгебры является задача факторизации полиномов многих переменных над рациональными числами.

Для факторизации полиномов одной переменной известно много замечательных алгоритмов. С обзором работ по факторизации можно познакомиться по учебнику Е.В. Панкратьева [1]. Будем полагать, что имеется некоторый алгоритм разложения на множители полиномов одной переменной. Требуется построить алгоритм факторизации для полиномов многих переменных. Рассмотрим сначала случай двух переменных.

Пусть $F(x,y)$ раскладывается на взаимнопростые множители $f_i(x,y)$: $F(x,y) = \prod_{i=0}^{s} f_i(x,y)^{n_i}$, $n_0 < n_1 < ... < n_s$. Тогда это разложение можно получить вычисляя НОД $F(x,y)$ и $F'(x,y)$ необходимое количество раз.

Пусть $f(x,y)$ — полином от двух переменных, у которого нет кратных сомножителей и который раскладывается на взаимнопростые множители: $f(x,y) = \prod_{j}^{s} f_j(x,y)$. Сомножители $f_j(x,y)$ требуется найти. Обозначим $S_x = deg_x f(x,y)$. Возьмём множество разных точек $Y \subseteq \mathbb{Q}$, такое что $|Y| = S_x + 1 = k$. Обозначим $\varphi_i(y) = f(x_i,y)\ \forall x_i \in Y$.

[1]Работа выполнена при поддержке программы «Развитие потенциала высшей школы» (проект 2.1.1/1853).

Разложим $\varphi_i(y)$ на множители: $\varphi_i(y) = \prod\limits_s \varphi_{si}(y)$. Воспользуемся китайской теоремой об остатках для полиномов. Тогда полином $f_j(x,y)$ можно восстановить по его k образам: $\varphi_{j1}(y), ..., \varphi_{jk}(y)$, поднимая каждый коэффициент при степени y в полином степени $k-1$ от x по его k числовым значениям. Таким образом мы восстановим все множители $f_j(x,y)$ полинома $f(x,y)$.

Рассмотрим $f(x_1, ..., x_n)$ — полином от n переменных, у которого нет кратных сомножителей и который раскладывается на взаимнопростые множители: $f(x_1, ..., x_n) = \prod\limits_j f_j(x_1, ..., x_n)$. Сомножители $f_j(x_1, ..., x_n)$ требуется найти. Пусть Y_i $(i = 1, ..., n-1)$ конечные подмножества $\mathbb{Q}$, такие что $|Y_i| = k_i + 1$, где $k_i = deg_{x_i} f(x_1, ..., x_n)$. В каждом из этих множеств все элементы различные. Введём обозначение элементов Y_i: $Y_i = \{t_i^0, ..., t_i^{k_i}\}$. Обозначим $\varphi_{v_1,...,v_{n-1}}(x_n) = f(t_1^{v_1}, ..., t_{n-1}^{v_{n-1}}, x_n)$ полином, который получается подстановкой вместо переменных x_i чисел $t_i^{v_i}$ $(i = 1, ..., n-1;\ v_i \in [0, ..., k_i])$. Разложим каждый из $\varphi_{v_1,...,v_{n-1}}(x_n)$ на множители: $\varphi_{v_1,...,v_{n-1}}(x_n) = \prod\limits_j \varphi_{j,v_1,...,v_{n-1}}(x_n)$. Обозначим $\rho_{v_1,...,v_{n-1}} = \prod\limits_{i=1}^{n-1}(x_i - t_i^{v_i})$. Отметим, что $\varphi_{j,v_1,...,v_{n-1}}(x_n)$ является образом $f_j(x_1, ..., x_n)$ при отображении $\mathbb{Q}[x_1, ..., x_n] \to \mathbb{Q}[x_1, ..., x_n]/\rho_{v_1,...,v_{n-1}}\mathbb{Q}[x_1, ..., x_n]$. Перейдём к восстановлению искомых функции $f_j(x_1, ..., x_n)$.

Шаг 1.

Отметим, что $\varphi_{j,v_1,...,v_{n-1}}(t_n^{v_n}) = f_j(t_1^{v_1}, ..., t_n^{v_n})$ $\forall v_1 \in [0, ..., k_1], ..., v_n \in [0, ..., k_n]$. Введём обозначения для коэффициентов полиномов $\varphi_{j,v_1,...,v_{n-2},g}(x_n)$. Пусть

$$\varphi_{j,v_1,...,v_{n-2},g}(x_n) = \sum_{g_n=0}^{k_n} \alpha^0_{j,v_1,...,v_{n-2},g,g_n} x_n^{g_n}, \qquad g = 0, ..., k_{n-1}.$$

Восстановим полином степени k_{n-1} по его значениям: $\alpha^0_{j,v_1,...,v_{n-2},0,g_n}, ...,\ \alpha^0_{j,v_1,...,v_{n-2},k_{n-1},g_n}$ в точках $t_{n-1}^0, ..., t_{n-1}^{k_{n-1}}$ по формуле Лагранжа:

$$f_{j,v_1,...,v_{n-2},g_n} = \sum_{g=0}^{k_{n-1}} \alpha^0_{j,v_1,...,v_{n-2},g,g_n} \frac{(x_{n-1} - t_{n-1}^0)...(x_{n-1} - t_{n-1}^{g-1})(x_{n-1} - t_{n-1}^{g+1})...(x_{n-1} - t_{n-1}^{k_{n-1}})}{(t_{n-1}^g - t_{n-1}^0)...(t_{n-1}^g - t_{n-1}^{g-1})(t_{n-1}^g - t_{n-1}^{g+1})...(t_{n-1}^g - t_{n-1}^{k_{n-1}})}.$$

Сгруппируем коэффициенты при неизвестных:

$$f_{j,v_1,...,v_{n-2},g_n} = \sum_{s=0}^{k_{n-1}} \alpha^1_{j,v_1,...,v_{n-2},g_n,s} x_{n-1}^s.$$

Составим полином от двух переменных:

$$\varphi_{j,v_1,...,v_{n-2}}(x_{n-1}, x_n) = \sum_{g_{n-1}=0}^{k_{n-1}} \sum_{g_n=0}^{k_n} \alpha^1_{j,v_1,...,v_{n-2},g_{n-1},g_n} x_{n-1}^{g_{n-1}} x_n^{g_n},$$

который в точках $t_{n-1}^{v_{n-1}}, t_n^{v_n}$ равен значению полинома $f_j(t_1^{v_1}, ..., t_{n-2}^{v_{n-2}}, x_{n-1}, x_n)$:

$$\varphi_{j,v_1,...,v_{n-2}}(t_{n-1}^{v_{n-1}}, t_n^{v_n}) = f_j(t_1^{v_1}, ..., t_n^{v_n}).$$

Шаг r.

Пусть уже получено $(k_1+1)...(k_{r-1}+1)$ полиномов:

$$\varphi_{j,v_1,...,v_{r-1},g}(x_{r+1},...,x_n)=\sum_{g_{r+1}=0}^{k_{r+1}}...\sum_{g_n=0}^{k_n}\alpha^{n-1-r}_{j,v_1,...,v_{r-1},g,g_{r+1},...,g_n}x_{r+1}^{g_{r+1}}...x_n^{g_n},$$

$g=0,...,k_r; v_1\in[0,...,k_1],...,v_{r-1}\in[0,...,k_{r-1}]$.

Будем восстанавливать полином степени k_r по его значениям: $\alpha^{n-1-r}_{j,v_1,...,v_{r-1},0,g_{r+1},...,g_n}$,..., $\alpha^{n-1-r}_{j,v_1,...,v_{r-1},k_r,g_{r+1},...,g_n}$ в точках $t_r^0,...,t_r^{k_r}$ по формуле Лагранжа:

$$f_{j,v_1,...,v_{r-1},g_{r+1},...,g_n}=\sum_{g=0}^{k_r}\alpha^{n-1-r}_{j,v_1,...,v_{r-1},g,g_{r+1},...,g_n}\frac{(x_r-t_r^0)...(x_r-t_r^{g-1})(x_r-t_r^{g+1})...(x_r-t_r^{k_r})}{(t_r^g-t_r^0)...(t_r^g-t_r^{g-1})(t_r^g-t_r^{g+1})...(t_r^g-t_r^{k_r})}.$$

Сгруппируем коэффициенты при неизвестных:

$$f_{j,v_1,...,v_{r-1},g_{r+1},...,g_n}=\sum_{s=0}^{k_r}\alpha^{n-r}_{j,v_1,...,v_{r-1},g_{r+1},...,g_n,s}x_r^s.$$

Составим полином от $n-r+1$ переменной:

$$\varphi_{j,v_1,...,v_{r-1}}(x_r,...,x_n)=\sum_{g_r=0}^{k_r}\sum_{g_{r+1}=0}^{k_{r+1}}...\sum_{g_n=0}^{k_n}\alpha^{n-r}_{j,v_1,...,v_{r-1},g_r,g_{r+1},...,g_n}x_r^{g_r}x_{r+1}^{g_{r+1}}...x_n^{g_n},$$

который в точках $t_r^{v_r},...,t_n^{v_n}$ равен значению полинома $f_j(t_1^{v_1},...,t_{r-1}^{v_{r-1}},x_r,...,x_n)$:

$$\varphi_{j,v_1,...,v_{r-1}}(t_r^{v_r},...,t_n^{v_n})=f_j(t_1^{v_1},...,t_n^{v_n}).$$

Шаг $n-1$.

Пусть уже получено k_1+1 полиномов:

$$\varphi_{j,g}(x_2,...,x_n)=\sum_{g_2=0}^{k_2}...\sum_{g_n=0}^{k_n}\alpha^{n-2}_{j,g,g_2,...,g_n}x_2^{g_2}...x_n^{g_n},\qquad g=0,...,k_1.$$

Восстановим полином степени k_1 по его значениям: $\alpha^{n-2}_{j,0,g_2,...,g_n}$,..., $\alpha^{n-2}_{j,k_1,g_2,...,g_n}$ в точках $t_1^0,...,t_1^{k_1}$ по формуле Лагранжа:

$$f_{j,g_2,...,g_n}=\sum_{g=0}^{k_1}\alpha^{n-2}_{j,g,g_2,...,g_n}\frac{(x_1-t_1^0)...(x_1-t_1^{g-1})(x_1-t_1^{g+1})...(x_1-t_1^{k_1})}{(t_1^g-t_1^0)...(t_1^g-t_1^{g-1})(t_1^g-t_1^{g+1})...(t_1^g-t_1^{k_1})}.$$

Сгруппируем коэффициенты при неизвестных:

$$f_{j,g_2,...,g_n}=\sum_{s=0}^{k_1}\alpha^{n-1}_{j,g_2,...,g_n,s}x_1^s.$$

Составим полином от n переменных:

$$\varphi_j(x_1,...,x_n)=\sum_{g_1=0}^{k_1}\sum_{g_2=0}^{k_2}...\sum_{g_n=0}^{k_n}\alpha^{n-1}_{j,g_1,g_2,...,g_n,}x_1^{g_1}...x_n^{g_n},$$

который в точках $t_1^{v_1}, ..., t_n^{v_n}$ равен значению полинома $f_j(t_1^{v_1}, ..., t_n^{v_n})$:

$$\varphi_j(t_1^{v_1}, ..., t_n^{v_n}) = f_j(t_1^{v_1}, ..., t_n^{v_n}).$$

Получен искомый полином $f_j(x_1, ..., x_n)$. Вычисляя последовательно все полиномы $f_j(x_1, ..., x_n)$, $i = 0, 1, .., s$, получим искомое разложение: $f(x_1, ..., x_n) = \prod_j f_j(x_1, ..., x_n)$.

ЛИТЕРАТУРА

1. *Панкратьев Е.Г.* Элементы компьютерной алгебры. Учебное пособие. М. Интернет-университет информационных технологий; БИНОМ. Лаборатория знаний, 2007.

Malaschonok G.I., Ivashov D.S. An algorithm of factorization of polynomials of several variables.

Key words: factorization of polynomials, computer algebra.

Поступила в редакцию 20 ноября 2009г.

УДК 004.421

О ПАРАЛЛЕЛЬНОМ ВЫЧИСЛЕНИИ ДИСКРЕТНОГО ПРЕОБРАЗОВАНИЯ ФУРЬЕ И ПРОВЕДЁННЫХ ЭКСПЕРИМЕНТАХ[1]

© **А. О. Лапаев**

Ключевые слова: параллельная компьютерная алгебра, дискретное преобразование Фурье, быстрое преобразование Фурье, полиномиальные алгоритмы.
Предлагается алгоритм параллельного вычисления многомерного дискретного преобразования Фурье полинома нескольких переменных в простом поле. Приводятся результаты экспериментов на кластере МСЦ РАН.

1 Введение

Пусть $f \in \mathbb{Z}_p[x_1, x_2, \ldots, x_d]$, p — простое число. Пусть наибольшая степень переменной x_i в полиноме f равна $n_i - 1$, $n_i = 2^{N_i}$. Обозначим $n = n_1 n_2 \ldots n_d$. Тогда полином f можно записать в виде:

$$f = \sum_{i_1=0}^{n_1-1} \sum_{i_2=0}^{n_2-1} \cdots \sum_{i_d=0}^{n_d-1} f_{i_1 i_2 \ldots i_n} x_1^{i_1} x_2^{i_2} \ldots x_d^{i_d}.$$

[1]Работа выполнена при поддержке программы «Развитие потенциала высшей школы» (проект 2.1.1/1853).