УДК 519.688

ФАКТОРИЗАЦИЯ ПОЛИНОМОВ МНОГИХ ПЕРЕМЕННЫХ

© Д. С. Ивашов

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

Обсуждаются алгоритмы факторизации полиномов многих переменных.

1 Введение

Задача разложения полиномов на множители имеет долгую и выдающуюся историю. Одним из первых метод факторизации полиномов предложил Кронекер в 1882 г. С тех пор прошло более ста лет, и были получены современные, более быстрые алгоритмы разложения полиномов на множители. Д. Муссен, П. Ванг, Л. Ротшильд обобщили лемму Гензеля для получения алгоритма факторизации полиномов от нескольких переменных с целыми коэффициентами. Ван Хойя, основываясь на работах Калтофена и Шоупа предложил систему оценок, следуя которой выбирается определенная стратегия факторизации полиномов [1, 2]. В настоящее время появляются различные модификации известных алгоритмов, позволяющие ускорить процесс разложения на множители.

Настоящая работа продолжает исследования по факторизации полиномов многих переменных в среде ParCA. Здесь детализируется предварительный этап сведения задачи факторизации полиномов многих переменных к полиномам одной переменной [3]. Для факторизации полиномов одной переменной применяется алгоритм Берлекемпа в изложении Д. Кнута [4].

2 Выделение множителей, имеющих различные наборы переменных

Пусть $F(x_1, ..., x_n)$ – полином от n переменных $x_1, ..., x_n$. У такого полинома может быть не более 2^n сомножителей, которые имеют различные наборы переменных. При этом сомножителей, имеющих p различных переменных из n, может быть не более binomial $\{n, p\}$. Процедура выделения этих сомножителей состоит в следующем.

Предварительно находится НОД всех числовых коэффициентов и каждый коэффициент делится на него. Затем отделяется сомножитель, не содержащий переменную x_1. Для этого нужно записать полином F по степеням переменной x_1 и найти у полиномиальных коэффициентов НОД. После деления исходного полинома на этот НОД получим два полиномиальных сомножителя исходного полинома, один из которых не содержит переменную x_1.

Будем продолжать этот процесс для переменных x_2, x_3,..., x_s. Пусть уже выделены переменные, не содержащие все возможные наборы полиномов из x_2, ... , x_s. В каждом из этих полиномов можно попробовать выделить сомножитель, не содержащий переменную x_{s+1}. Для этого в каждом их этих полиномов найдем НОД полиномиальных коэффициентов при неизвестной x_{s+1} и разделим на него. Общее число полиномиальных сомножителей может при этом, в худшем случае, удвоится.

Таким образом, завершив этот процесс на последней переменной x_n, получим, в худшем случае, 2^n сомножителей.

Пример 1.

Разложим полином $F(x,y,z) = xyz^2 + 3yz^2 + x^2z^2 + 3xz^2 + 2xy^2z + 6y^2z + 3x^2yz + +9xyz + x^3z + 3x^2z + xy^3 + 3y^3 + 2x^2y^2 + 6xy^2 + x^3y + 3x^2y$. Найдем НОД полиномиальных коэффициентов относительно переменной x. Он равен $z + y$. Поэтому
$F(x,y,z) = (z+y) \cdot (xyz + 3yz + x^2z + 3xz + xy^2 + 3y^2 + 2x^2y + 6xy + x^3 + 3x^2)$. Обозначим $f_1 = z + y, f_2 = xyz + 3yz + x^2z + 3xz + xy^2 + 3y^2 + 2x^2y + 6xy + x^3 + 3x^2$. Для каждого из полученных сомножителей ищем НОД полиномиальных коэффициентов относительно переменной y. Для f_2 НОД будет равен $x + 3$, следовательно,
$f_2 = (x+3) \cdot (yz + xz + y^2 + 2xy + x^2)$. Обозначим $f_{2,1} = x+3, f_{2,2} = yz + xz + y^2 + 2xy + x^2$. Для каждого из полученных сомножителей ищем НОД полиномиальных коэффициентов относительно переменной z. Для полинома $f_{2,2}$ находим НОД коэффициентов $x + y$, следовательно, $f_{2,2} = (x + y) \cdot (x + y + z)$. Обозначим $f_{2,2,1} = x + y, f_{2,2,2} = x + y + z$. Следовательно, полином $F(x,y,z)$ раскладывается на множители следующим образом:
$F(x,y,z) = f_1 \cdot f_{2,1} \cdot f_{2,2,1} \cdot f_{2,2,2} = (z+y) \cdot (3+x) \cdot (x+y) \cdot (x+y+z)$.

3 Освобождение от квадратов

После отделения сомножителей с разными наборами коэффициентов можно в каждом из сомножителей освободиться от квадратов. То есть попытаться представить полином в виде произведения сомножителей, каждый из которых входит в произведение со степенью, которая отличается от степеней других сомножителей:

$$F(x_1, ..., x_n) = \prod_{i=1}^{r} f_i(x_1, ..., x_n)^{s_i},$$

где s_i – различные натуральные числа, $s_i \neq s_j$, при $i \neq j$. При этом если f_i раскладывается дальше на сомножители, то каждый из них входит в f_i в первой степени.

Выделение таких сомножителей можно производить последовательным дифференцированием и вычислением НОД полинома и его производной.

Пример 2. Разложим полином $p(x,y,z) = (z^3 + 5yz^2 + 8y^2z + 4y^3)$ на множители. Найдем $p'_z = 3z^2 + 10yz + 8y^2$. Вычислим $(p, p'_z) = z + 2y$. Следовательно, $p = (z + 2y)^2 \cdot (z + y)$.

4 Проблема старшего коэффициента полинома многих переменных

Теперь наступает самая трудная часть процедуры факторизации. Если еще существует дальнейшее разложение на множители, то каждый из множителей будет иметь один и тот же набор переменных и входить в произведение в первой степени. При этом если коэффициент при старшей переменной равен 1, то это облегчает дальнейшие поиски сомножителей. Перейти к такому случаю можно домножением полинома на степень старшего коэффициента и заменой переменных.

Пусть $F(x_1,...,x_n) = \sum\limits_{i=0}^{k} a_i \cdot x_n^i$ – полином n переменных $x_1,...,x_n$, x_n – старшая переменная, $a_i = a_i(x_1,...,x_{n-1})$ – коэффициенты при старшей переменной, которые представляют собой полиномы от остальных переменных. Можно перейти к многочлену со старшим коэффициентом равным одному, если домножить полином на старший коэффициент a_k в степени $k-1$. В результате замены переменной x_n на $y = x_n a_k$ придем к полиному, у которого старшая переменная y имеет старший коэффициент равный 1.

Требует дополнительного исследования вопрос о том, в каких случаях такое действие является оправданным и "облегчает" задачу факторизации. Конкретные рекомендации по этому вопросу неизвестны.

5 Факторизация нормированного, свободного от квадратов полинома

Рассмотрим теперь полином от n переменных $f(x_1,...,x_n)$, у которого нет кратных сомножителей и который раскладывается на взаимно простые множители: $f(x_1,...,x_n) = \prod\limits_j f_j(x_1,...,x_n)$. Сомножители $f_j(x_1,...,x_n)$ требуется найти. Будем полагать, что нам известен способ факторизации полиномов от одной переменной. Пусть Y_i $(i = 1,...,n-1)$ конечные подмножества Q, такие что $\mid Y_i \mid = k_i + 1$, где $k_i = deg_{x_i} f(x_1,...,x_n)$. В каждом из этих множеств все элементы различные. Введем обозначение элементов Y_i: $Y_i = \{t_i^0,...,t_i^{k_i}\}$. Обозначим через $\varphi_{v_1,...,v_{n-1}}(x_n) = f(t_1^{v_1},...,t_{n-1}^{v_{n-1}}, x_n)$ 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 отображенииgiven and $Q[x_1,...,x_n] \to Q[x_1,...,x_n]/\rho_{v_1,...,v_{n-1}} Q[x_1,...,x_n]$. Перейдем к восстановлению искомых функции $f_j(x_1,...,x_n)$.

Первый шаг.

Отметим, что $\varphi_{j,v_1,...,v_{n-1}}(t_n^{v_n}) = f_j(t_1^{v_1},...,t_n^{v_n})$ $\forall v_1 \in [0,...,k_1],...,v_n \in [0,...,k_n]$. Введем 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:

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