УДК 519.16:004.02

М.Ю. Перминова, В.В. Кручинин, Д.В. Кручинин

Алгоритм декомпозиции полиномов, основанный на разбиениях

Рассмотрена задача представления полиномов в виде композиции. Предложен новый алгоритм декомпозиции полиномов, основанный на разбиениях. В основе предлагаемого алгоритма декомпозиции лежит формула нахождения коэффициентов композиции производящих функций, основанная на разбиении натурального числа.

Ключевые слова: декомпозиция полиномов, генерация разбиений, алгоритм.

В настоящее время при решении задач моделирования и математического анализа широко применяются системы компьютерной алгебры, относящиеся к классу систем символьных вычислений [1–3]. Одной из функций таких систем является представление полинома в виде композиции двух полиномов. Решение задачи представления полиномов в виде композиции двух полиномов имеет некоторую историю. Так, в 1976 г. американские ученые Д.Р. Бартон и Р.Е. Зиппель показали, что декомпозиция полиномов может упростить поиск корней в символьном виде. При этом они указали, что многие системы символьной алгебры поддерживают декомпозицию полиномов для таких целей [4]. В 1985 г. эти же ученые предложили два алгоритма декомпозиции полиномов [5]. Первый из них находил коэффициенты полиномов двух переменных, второй – полиномов одной переменной. Упрощенную версию второго алгоритма представили Алагар и Тан [9]. Их алгоритм был основан на дифференцировании исходного полинома.

В 1989 г. Д. Козен и С. Ландау предложили свой алгоритм декомпозиции полиномов в совместной статье [7]. По данному алгоритму находились коэффициенты внутреннего полинома. Затем для получения коэффициентов внешнего полинома решалась система уравнений, основанная на матрице коэффициентов внутреннего полинома. Далее проводилась проверка ранее найденных коэффициентов.

В 2003 г. корейские ученые Джун-Кюн Сон и Мен-Су Ким вместе с ученым из Израиля Г. Элбером предложили еще один алгоритм декомпозиции полиномов [8]. Он состоял из двух частей. По первой части алгоритма по исходному полиному вычислялся внутренний полином. Затем по второй части находился внешний полином.

В данной статье предложен новый алгоритм декомпозиции полиномов, основанный на использовании методов нахождения коэффициентов композиции производящих функций, развитый в работах [9, 10], и генерации разбиений [11].

Получение системы уравнений. Пусть дан полином $F(x)=\sum_{i=1}^{t} f_i x^i = f_1 x + f_2 x^2 + f_3 x^3 + \ldots + f_t x^t$.

Необходимо представить $F(x)$ в виде композиции двух полиномов $A(x)$ и $B(x)$, т.е. $F(x)=B\big(A(x)\big)$, методом, основанным на разбиениях. При этом:

$$A(x)=\sum_{i=1}^{m} a_i x^i = a_1 x + a_2 x^2 + a_3 x^3 + \ldots + a_m x^m, \quad B(x)=\sum_{i=1}^{s} b_i x^i = b_1 x + b_2 x^2 + b_3 x^3 + \ldots + b_s x^s,$$

где a_i и b_i – искомые коэффициенты; m и s – степени полиномов $A(x)$ и $B(x)$ соответственно ($t=m\cdot s$).

Данная задача имеет множество решений, так как полином композиции можно представить следующим образом:

$$F(x)=B_\alpha\big(A_\alpha(x)\big), \quad B_\alpha(x)=B(\alpha x), \quad A_\alpha(x)=A\left(\frac{x}{\alpha}\right), \text{ где } \alpha\neq 0.$$

Воспользуемся следующей формулой для нахождения композиции производящих функций [9]:

$$f_n=\sum_{k=1}^{n} A^{\Delta}(n,k)b_k, \qquad (1)$$

где коэффициенты $A^{\Delta}(n,k)$ представляются на основе композиций натурального числа n:

$$A^{\Delta}(n,k)=\sum_{\pi_k\in C_n} a_{\lambda_1}a_{\lambda_2}\ldots a_{\lambda_k}, \tag{2}$$

где C_n – множество всех композиций натурального числа n; π_k – композиция $\sum_{i=1}^{k}\lambda_i=n$, имеющая ровно k частей. Поскольку существует связь между композициями натурального числа и разбиениями, можно записать представление $A^{\Delta}(n,k)$ на основе разбиений

$$A^{\Delta}(n,k)=\sum_{\mu_k\in P_n}\binom{k}{j_1 j_2\ldots j_l}a_{r_1}^{j_1}a_{r_2}^{j_2}\ldots a_{r_l}^{j_l}, \tag{3}$$

где P_n – множество всех разбиений натурального числа n; μ_k – разбиение, имеющее ровно k частей; r_i – не повторяющиеся части разбиения μ_k; l – число не повторяющихся частей; j_i – число повторений частей r_i в разбиении. Здесь в разбиении в отличие от композиции не учитывается порядок частей, поэтому в выражении (3) мультиномиальный коэффициент показывает, сколько существует вариантов композиций, состоящих из тех же частей разбиения. При этом справедлива следующая система уравнений

$$\begin{cases} j_1+j_2+\ldots+j_l=k, \\ r_1 j_1+r_2 j_2+\ldots+r_l j_l=n, \end{cases} \tag{4}$$

где $l\le k$.

Решение системы уравнений (4) есть все разбиения числа n, в которых ровно k частей [12].

Подставив (3) в (1), получаем систему из n уравнений:

$$\sum_{k=1}^{n}\sum_{\mu_k\in P_n}\binom{k}{j_1 j_2\ldots j_l}a_{r_1}^{j_1}a_{r_2}^{j_2}\ldots a_{r_l}^{j_l}b_k=f_n. \tag{5}$$

Для получения системы уравнений (5) степени полиномов композиции должны быть известны. Для дальнейшего изложения будем предполагать, что m и s нам известны.

Учитывая, что степени полиномов ограничены, части разбиения r_i не должны превышать m, т.е. $r_i\le m$. Также коэффициенты b_k ограничены степенью s полинома $B(x)$, т.е. $k\le s$. Степень p исходного полинома $F(x)$ ограничивает значения n, т.е. $n\le t$.

Анализ формулы (5) показал, что для получения системы уравнений необходимо получить все разбиения (m,s,n), где n – число, представляемое разбиением; s – число частей разбиения, каждая из которых не превосходит m. Такие разбиения исследовал Г. Эндрюс. Он получил следующую рекуррентную формулу для числа разбиений $p(m,s,n)$ [13]:

$$p(m,s,n)=p(m,s-1,n)+p(m-1,s,n-s).$$

Используя эту формулу и метод построения алгоритма комбинаторной генерации [12, 14, 15], авторами разработаны оригинальные алгоритмы генерации и нумерации таких разбиений [11].

Свойства системы уравнений. На основе подхода построения системы уравнений, основанной на генерации разбиений, исследуем её свойства. Для этого рассмотрим композиционную формулу (1), на которой основаны уравнения в системе. Коэффициенты $A^{\Delta}(n,k)$ можно представить в виде треугольной матрицы

$$\begin{array}{ccccc} A_{1,1}^{\Delta} & & & & \\ A_{2,1}^{\Delta} & A_{2,2}^{\Delta} & & & \\ A_{3,1}^{\Delta} & A_{3,2}^{\Delta} & A_{3,3}^{\Delta} & & \\ \ldots & \ldots & \ldots & \ldots & \\ A_{n,1}^{\Delta} & A_{n,2}^{\Delta} & A_{n,3}^{\Delta} & \ldots & A_{n,n}^{\Delta} \end{array}$$

В первом столбце данной матрицы записаны коэффициенты производящей функции $A(x)$,…, в k-м столбце матрицы – коэффициенты производящей функции $[A(x)]^k$ [12]. Так как степень m полинома $A(x)$ известна, значит, число коэффициентов производящей функции $A(x)$ равно m. По-

этому, основываясь на свойствах треугольной матрицы [12], можно сделать вывод о том, что в первом столбце будет m элементов, не равных нулю. Во втором столбце нули начнутся на $(m+1)$-й позиции, в третьем – на $(2m+1)$-й, в четвертом – на $(3m+1)$-й, …, в $(k-1)$-м – на $\big((k-2)m+1\big)$-й позиции, а в k-м – на $\big((k-1)m+1\big)$-й позиции. Таким образом, формула для подсчета ненулевых коэффициентов в k-м столбце треугольной матрицы имеет вид $(km-k+1)$. Наглядно это можно представить следующим образом (для $m=2$):

$$
\begin{array}{ccccccc}
A^{\Delta}_{1,1} & & & & & & \\
A^{\Delta}_{2,1} & A^{\Delta}_{2,2} & & & & & \\
0 & A^{\Delta}_{3,2} & A^{\Delta}_{3,3} & & & & \\
0 & A^{\Delta}_{4,2} & A^{\Delta}_{4,3} & A^{\Delta}_{4,4} & & & \\
0 & 0 & A^{\Delta}_{5,3} & A^{\Delta}_{5,4} & A^{\Delta}_{5,5} & & \\
0 & 0 & A^{\Delta}_{6,3} & A^{\Delta}_{6,4} & A^{\Delta}_{6,5} & A^{\Delta}_{6,6} & \\
. & . & . & . & . & . & .
\end{array}
$$

Коэффициенты b_k ограничены степенью s полинома $B(x)$. Ниже показан вид коэффициентов b_k при $s=3$:

$$
\begin{array}{cccccc}
b_1 & & & & & \\
b_1 & b_2 & & & & \\
b_1 & b_2 & b_3 & & & \\
b_1 & b_2 & b_3 & 0 & & \\
b_1 & b_2 & b_3 & 0 & 0 & \\
. & . & . & . & . & . \\
b_1 & b_2 & b_3 & 0 & \ldots & 0
\end{array}
$$

Далее рассмотрим вид системы уравнений (5). Он зависит от соотношения параметров m и s. Например, для $m \le s$ (при $m=2,\ s=3$) система уравнений имеет вид

$$
\begin{array}{cccccccccc}
A^{\Delta}_{1,1}b_1 & & & & & & & & & = f_1 \\
A^{\Delta}_{2,1}b_1 & A^{\Delta}_{2,2}b_2 & & & & & & & & = f_2 \\
0 & A^{\Delta}_{3,2}b_2 & A^{\Delta}_{3,3}b_3 & & & & & & & = f_3 \\
0 & A^{\Delta}_{4,2}b_2 & A^{\Delta}_{4,3}b_3 & 0 & & & & & & = f_4 \\
0 & 0 & A^{\Delta}_{5,3}b_3 & 0 & 0 & & & & & = f_5 \\
0 & 0 & A^{\Delta}_{6,3}b_3 & 0 & 0 & 0 & & & & = f_6 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & & & = f_7 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & & = f_8 \\
. & . & . & . & . & . & . & . & . & .
\end{array}
$$

для $m > s$ ($m=3,\ s=2$):

$$
\begin{array}{ccccccccc}
A^{\Delta}_{1,1}b_1 & & & & & & & & = f_1 \\
A^{\Delta}_{2,1}b_1 & A^{\Delta}_{2,2}b_2 & & & & & & & = f_2 \\
A^{\Delta}_{3,1}b_1 & A^{\Delta}_{3,2}b_2 & 0 & & & & & & = f_3 \\
0 & A^{\Delta}_{4,2}b_2 & 0 & 0 & & & & & = f_4 \\
0 & A^{\Delta}_{5,2}b_2 & 0 & 0 & 0 & & & & = f_5 \\
0 & A^{\Delta}_{6,2}b_2 & 0 & 0 & 0 & 0 & & & = f_6 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & & = f_7 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & = f_8 \\
. & . & . & . & . & . & . & . & .
\end{array}
\qquad (6)
$$

Для дальнейшего удобства каждому уравнению в системе присвоим номер в соответствии с индексом коэффициента f. Например, уравнения из (6) будут иметь следующие номера:

$$A^{\Delta}_{1,1}b_1 = f_1 - \text{ номер 1},$$

$$A^{\Delta}_{2,1}b_1 + A^{\Delta}_{2,2}b_2 = f_2 - \text{ номер 2},$$

$$A^{\Delta}_{3,1}b_1 + A^{\Delta}_{3,2}b_2 = f_3 - \text{ номер 3},$$

$$A^{\Delta}_{4,2}b_2 = f_4 - \text{ номер 4},$$

$$A^{\Delta}_{5,2}b_2 = f_5 - \text{ номер 5},$$

$$A^{\Delta}_{6,2}b_2 = f_6 - \text{ номер 6}.$$

Полученная таким образом система состоит из t уравнений, при этом число неизвестных переменных равно $m+s$ (m неизвестных коэффициентов полинома $A(x)$, так как m – это степень полинома $A(x)$, s неизвестных коэффициентов полинома $B(x)$). При этом $t = ms \geq m+s$, поэтому достаточно решить $m+s$ уравнений из полученной системы.

Система уравнений имеет множество решений, так как представить полином в виде композиции можно бесконечным числом вариантов (см. разд. Получение системы уравнений). Для исключения такой ситуации одному из коэффициентов присвоим фиксированное значение 1. Таким коэффициентом будет a_m, т.е. $a_m = 1$.

Найденное решение необходимо проверить на существование композиции.

Таким образом, множество всех уравнений системы делим на два подмножества:

- $m+s-1$ уравнений – это уравнения, которые решаются для нахождения коэффициентов a_i и b_i. При получении решения данных уравнений нельзя сказать, существует композиция или нет;
- оставшиеся $t-(m+s-1)$ уравнений – это уравнения, с помощью которых проверяется наличие композиции при найденных значениях коэффициентов a_i и b_i.

Свойство 1. При наличии композиции все оставшиеся уравнения решаются.

Свойство 2. При отсутствии композиции хотя бы одно уравнение из множества оставшихся не имеет решения.

$m+s-1$ уравнений для решения выбираются следующим образом. В системе уравнений (5) число членов в уравнениях с номерами $t-m \leq i \leq t$ меньше числа членов в уравнениях с номерами $1 \leq i \leq s-1$, а наибольшее число членов содержится в уравнениях, которые имеют номера, близкие к $t/2$. Поэтому берем уравнения, которые имеют номера $1 \leq i \leq s-1$ и $t-m \leq i \leq t$. Решить выбранные уравнения можно последовательно, начиная с последнего уравнения системы. В последнем уравнении вычисляется значение b_s. И далее методом подстановки в последующих уравнениях рассчитываются значения оставшихся переменных. При подстановке в последующие уравнения значений известных коэффициентов уравнения принимают линейный вид.

Решение выбранных уравнений является коэффициентами a_i и b_i полиномов $A(x)$ и $B(x)$.

Алгоритм декомпозиции полиномов, основанный на разбиениях. Рассмотренные выше свойства систем уравнений (5) позволяют построить оригинальный алгоритм, основанный на генерации разбиений. На вход алгоритма подается исходный полином $F(x)$, на выходе получаются два полинома, композиция которых представляет собой полином $F(x)$. Основными элементами алгоритма являются:

- $F(x)$ – исходный полином;
- D – список известных коэффициентов a_i и b_i полиномов композиции $A(x)$ и $B(x)$ соответственно. Изначально $D = \{a_m = 1\}$;
- T – список номеров уравнений системы (5), $\#T$ – мощность множества T;
- *GetT*(m,s) формирует список T, согласно критериям выбора уравнений (см. разд. Свойства системы уравнений): из системы уравнений берем уравнения с номерами $1 \leq i \leq s-1$ и $t-m \leq i \leq t$;
- *Poly* – полином, из которого формируется уравнение *Eq*;

• L – путь в дереве разбиений;

• *First*(m,s,n) находит путь от корня (m,s,n) к самому левому листу дерева разбиений. Здесь m – степень полинома $A(x)$, s – степень полинома $B(x)$;

• *Next*(m,s,n) находит следующий путь в поддереве дерева разбиений;

• *GetMonom*(*P*) формирует моном по разбиению *P* (см. разд. Получение системы уравнений);

• *GetEquation*(*Poly*) формирует уравнение, приравнивая полином к соответствующему коэффициенту f_i, т. е. получаемое уравнение *Eq* имеет вид: $Poly_i = f_i$ см. формулу (5).

На рис. 1 представлен сам алгоритм.

```
GetDecomposition(F(x)) :=
D = { a_m = 1 },
T = GetT(m, s),
// для каждого уравнения
for ( j = 1, j ≠ #T + 1, j++ ) do
        Poly = { },
        // получаем моном и решаем уравнение
        for ( L = First(m,s, T_j ), L ≠ null, L = Next(m,s, T_j ) ) do
                P = GetPartition(L), // получаем разбиение P числа T_j
                M = GetMonom(P), // получаем моном M для T_j , k
                Poly = Poly + M, // добавляем моном M в полином Poly
                // получаем уравнение Eq,
                // подставляем в него значения известных коэффициентов из D
                Eq = GetEquation(Poly)
        end
        S = Solve(Eq), // получаем решение S линейного уравнения Eq
        D = D + S // добавляем S в список D
end
```

Рис. 1. Алгоритм декомпозиции полиномов, основанный на разбиениях

Кратко опишем работу алгоритма. В список коэффициентов D записываем заданное значение коэффициента a_m, т.е. $D = \{a_m = 1\}$. Формируем список номеров уравнений T функцией *GetT*. Затем для каждого уравнения из списка T генерируется список разбиений P, по P получается список мономов M. Далее из мономов составляется уравнение Eq и находится его решение S. Найденные коэффициенты добавляются в список известных коэффициентов D.

Анализ решения. Найденные коэффициенты полиномов $A(x)$ и $B(x)$ необходимо проверить на существование композиции. Возможны следующие варианты проверки найденного решения:

1) подставить найденные коэффициенты во все оставшиеся уравнения и решить их. Если все эти уравнения решаются, то композиция существует, иначе композиции нет;

2) проверить значения в заданных точках x_i. То есть взять некоторые точки x_i и подставить их в исходный полином и полиномы композиции с найденными коэффициентами. Если композиция существует, то будут выполняться равенства $F(x_i) = A(B(x_i))$;

3) из оставшихся уравнений каким-либо способом выбрать несколько уравнений, подставить в них найденные коэффициенты и с определенной вероятностью сделать вывод о существовании или отсутствии композиции.

Заключение. Дан обзор современных методов решения задачи декомпозиции полиномов. На основе метода определения композиции производящей функции получен алгоритм построения систем уравнений, основанных на разбиениях. Показано, что система уравнений разбивается на две части: одна часть – для нахождения коэффициентов полиномов; вторая – для проверки полученного решения. Разработан оригинальный алгоритм нахождения декомпозиции полинома.

Литература

1. Бухбергер Б., Калме Ж., Калтофен Э. и др. Компьютерная алгебра. Символьные и алгебраические вычисления / пер. с англ. – М.: Мир, 1986. – 392 с.

2. Мысовских В.И. Системы компьютерной алгебры и символьные вычисления // Записки научных семинаров ПОМИ РАН. – 2001. – Т. 281. – С. 227–236.

3. Кулябов Д.С., Кокотчикова М.Г. Аналитический обзор систем символьных вычислений // Вестник РУДН. Сер. «Математика. Информатика. Физика». – 2007. – № 1, 2. – С. 38–45.

4. Barton D.R. Polynomial decomposition / D.R. Barton, R.E. Zippel // Proceedings of Symposium on Symbolic and Algebraic Manipulation. – 1976. – P. 356–358.

5. Barton D.R. Polynomial decomposition algorithms / D.R. Barton, R.E. Zippel // Journal of Symbolic Computation. – 1985. – Vol. 1, № 2. – P. 159–168.

6. Alagar V.S. Fast polynomial decomposition algorithms / V.S. Alagar, M. Thanh // Proceedings of European Conference on Computer Algebra. – 1985. – P. 150–153.

7. Kozen D. Polynomial decomposition algorithms / D. Kozen, S. Landau // Journal of Symbolic Computation. – 1989. – № 7. – P. 445–456.

8. Seong J.-K., Elber G., Kim M.-S. Polynomial Decomposition and Its Applications [Электронный ресурс]. – Режим доступа: http://www.cs.utah.edu/~seong/decomposition.pdf, свободный (дата обращения: 09.07.2015).

9. Кручинин В.В. Степени производящих функций и их применение / В.В. Кручинин, Д.В. Кручинин. – Томск: ТУСУР, 2013. – 234 с.

10. Kruchinin D.V. Application of a composition of generating functions for obtaining explicit formulas of polynomials / D.V. Kruchinin, V.V. Kruchinin // Journal of Mathematical Analysis and Applications. – 2013. – Vol. 404, № 1. – P. 161–171.

11. Перминова М.Ю. Алгоритмы рекурсивной генерации ограниченных разбиений натурального числа / М.Ю. Перминова, В.В. Кручинин // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2014. – № 4(34). – С. 89–94.

12. Кручинин В.В. Комбинаторика композиций и ее приложения / В.В. Кручинин. – Томск: В-Спектр, 2010. – 156 с.

13. Эндрюс Г. Теория разбиений / пер. с англ. – М.: Наука. Главная редакция физико-математической литературы, 1982. – 256 с.

14. Кручинин В.В. Рекурсивные композиции деревьев и их свойства / В.В. Кручинин // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2007. – № 2(16). – С. 75–80.

15. Кручинин В.В. Алгоритмы генерации и нумерации композиций и разбиений натурального числа n / В.В. Кручинин // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2008. – № 2(17). – С. 113–119.

Перминова Мария Юрьевна
Аспирант каф. промышленной электроники (ПрЭ) ТУСУРа
Тел.: +7 (382-2) 70-15-53
Эл. почта: pmy@2i.tusur.ru

Кручинин Владимир Викторович
Д-р техн. наук, профессор каф. ПрЭ
Тел.: +7 (382-2) 70-15-54
Эл. почта: kru@ie.tusur.ru

Кручинин Дмитрий Владимирович
Мл. науч. сотрудник каф. комплексной информационной безопасности электронно-вычислительных систем ТУСУРа
Тел.: +7 (382-2) 70-15-54
Эл. почта: kdv@keva.tusur.ru

Perminova M.Yu., Kruchinin V.V., Kruchinin D.V.

Algorithm for decomposition of polynomials based on partitions

In this paper we consider a problem of polynomials decomposition. We solve that problem by developing a special algorithm which relies on the formula that allows to find composition coefficients of generating functions. That formula is based on partition of a natural number.

Keywords: decomposition of polynomials, generation of partitions, algorithm.