МАТЕМАТИКА

УДК 512.622

А.Э. МАЕВСКИЙ

АЛГОРИТМ ПОИСКА КОРНЕЙ МНОГОЧЛЕНОВ С КОЭФФИЦИЕНТАМИ ИЗ КОЛЬЦА $\mathbf{k}[x,y]$

Построен детерминированный алгоритм поиска корней многочленов одной переменной с коэффициентами из кольца $\mathbf{k}[x,y]$, *где* $\mathbf{k}$ *– произвольное поле. Алгоритм имеет полиномиальные временную и емкостную сложности и может рассматриваться как распространение алгоритма Рота-Рукенштейна [2] поиска корней многочленов с коэффициентами из кольца* $\mathbf{k}[x]$ *на случай многочленов с коэффициентами из* $\mathbf{k}[x,y]$.
Ключевые слова: *корни многочленов, алгоритм Рота-Рукенштейна, факторизация многочленов, линейные делители, конечные поля.*

Введение и постановка задачи. Пусть $\mathbf{k}$ – поле произвольной характеристики, $\mathbf{k}[x,y]$ – кольцо многочленов от переменных x, y с коэффициентами из $\mathbf{k}$, $\mathbf{k}[x,y][T]$ ($\cong\mathbf{k}[x,y,T]$) – кольцо многочленов от переменной T с коэффициентами из $\mathbf{k}[x,y]$. Под *полной степенью* $\deg(f(x,y))$ многочлена $f(x,y)$ ($\in\mathbf{k}[x,y]$) будем понимать максимальную из степеней мономов, входящих в $f(x,y)$, а под *степенью* (*T-степенью*) многочлена $Q(x,y,T)$ ($\in\mathbf{k}[x,y][T]$) – максимальный показатель степени переменной T, с которым она входит в $Q(x,y,T)$. Многочлен $f(x,y)$ ($\in\mathbf{k}[x,y]$) будем называть *T-корнем* многочлена $Q(x,y,T)$, если многочлен $Q(x,y,f(x,y))$ нулевой.

Рассмотрим следующую задачу: для заданного многочлена $Q(x,y,T)$ ($\in\mathbf{k}[x,y][T]$) и заданного целого числа d (>0) найти все T-корни $Q(x,y,T)$ полной степени не выше d. Эта задача возникает во многих областях современной математики, например, в теории помехоустойчивого кодирования при решении задач списочного декодирования [1], [2], [5]. Легко показать, что множество

$$\Omega_Q(d) = \{\, f(x,y)\in\mathbf{k}[x,y] \mid \deg(f(x,y)) \le d,\ Q(x,y,f(x,y)) \equiv 0 \,\}$$

всех T-корней $Q(x,y,T)$ полной степени не выше d находится во взаимно однозначном соответствии с множеством делителей $Q(x,y,T)$ вида $(T - f(x,y))$, где $\deg(f(x,y)) \le d$. Поэтому исходная задача эквивалентна задаче поиска всех линейных делителей многочлена $Q(x,y,T)$ вида $(T - f(x,y))$, $\deg(f(x,y)) \le d$.

Существует несколько подходов к решению поставленной задачи. Например, можно использовать общие алгоритмы факторизации многочленов от нескольких переменных [3], [4], и выделить все искомые линейные делители специального вида. Однако вычислительная сложность при этом может оказаться слишком высокой, так как почти все алгоритмы факторизации многочленов от нескольких переменных вероятностные, а многочлен $Q(x,y,T)$ может иметь большое количество ненужных нам линейных делителей вида $(g(x,y)T+f(x,y))$. В работе [5] предложен алгоритм поиска T-корней многочленов с коэффициентами из поля рациональных функций $\mathbf{k}(x_1,\dots,x_m)$. Так как $\mathbf{k}[x_1,x_2]\subset\mathbf{k}(x_1,\dots,x_m)$ при $m\ge 2$, этот алгоритм может быть применен и для построения множества $\Omega_Q(d)$. Однако он использует нетри-