Título - Algoritmo de Berlekamp

ORIENTADORA – MARIA CRISTINA VARRIALE

Autor: Maikon Machado Toledo
Curso: Licenciatura Matemática
Universidade Federal do Rio Grande do Sul

Salão UFRGS 2013 – Conhecimento Formação Inovação
UFRGS PROPESQ XXV SIC Salão Iniciação Científica
CET - Ciências Exatas e da Terra

INTRODUÇÃO

O algoritmo de Berlekamp é um método bem conhecido para fatoração de polinômios sobre pequenos corpos finitos, foi inventado por Elwyn Berlekamp em 1967, foi o algoritmo dominante para resolver o problema até o surgimento de um algoritmo mais eficiente do Cantor-Zassenhaus de 1981. Com o auxílio do Teorema Chinês dos Restos e o Morfismo de Frobenius e baseado nas ferramentas da álgebra linear e o cálculo GCD's, o algoritmo lineariza o problema e obtém os fatores do polinômio. Neste trabalho vou dar uma ideia geral de como funciona o algoritmo de Berlekamp.

DESENVOLVIMENTO

O problema original consiste em dado um polinômio $f \in \mathbb{F}_p[x]$ expressá-lo da seguinte forma

$$f = {f_1}^{e_1} {f_2}^{e_2} \dots {f_k}^{e_k}$$

no qual $f_1, f_2, \dots, f_k$ são polinômios irredutíveis em $\mathbb{F}_p[x]$ e $e_1, e_2, \dots, e_k$ são inteiros positivos. Veremos a seguir que basta nos focarmos no caso em que $f \in \mathbb{F}_p[x]$ não possui fatores quadrados. Suponha que existe um polinômio $q \in \mathbb{F}_p[x]$, de grau ≥ 1, tal que q^2 divide f. Isto é, podemos escrever $f = q^2.r$, com $r \in \mathbb{F}_p[x]$. Então $f' = 2qr + r'q^2 = q(2r + qr')$. Portanto, grau de $MDC(f, f') \geq$ grau de $q \geq 1$. Assim, $MDC(f, f')$,é um candidato a fator não-trivial de f, mas pode acontecer de $MDC(f, f') = f$. Separemos em dois casos:

Se $MDC(f, f') = f$ então $f' = 0$, pois grau de f' <grau de f e f divide f'. Neste caso, é fácil verificar, todos os monômios que aparecem em f têm grau múltiplo de p, isto é, podemos escrever $f = \sum_{i=0}^{n} a_i x^{pi}$. Como, para cada i, $a_i = {a_i}^p$, obtemos $f = \left(\sum_{i=0}^{n} a_i x^i\right)^p$. Em particular, o polinômio $\sum_{i=0}^{n} a_i x^i$ é um fator não-trivial de f.

Se $MDC(f, f') \neq f$, o polinômio $MDC(f, f')$ é um fator não-trivial de f.

No caso em que $MDC(f, f')$ ainda tenha fatores repetidos, novamente aplicamos o processo descrito acima, por recorrência de até que o máximo divisor entre este fator e sua derivada seja igual a 1 , obtendo assim um fator não-trivial livre de quadrados. Assim, restringimos nossa atenção para polinômios sem fatores repetidos. O Algoritmo de Berlekamp toma como input um polinômio mônico $f = f_1.f_2 \dots f_k$ livre de quadrados e retorna como output os fatores irredutíveis do mesmo. Segue os teoremas cruciais.

Teorema 1: Se $f \in \mathbb{F}_q[x]$é mônico e $h \in \mathbb{F}_q[x]$ é tal que $h^q \equiv h \, mod \, f$, então

$$f(x) = \prod_{c \in \mathbb{F}_q} gcd(f(x), h(x) - c)$$

Teorema Chinês dos Restos: Dado um corpo F, polinômios não-nulos $f_1, f_2, \dots, f_k \in F[x]$ que dois a dois primos entre si, e polinômios arbitrários $g_1, g_2, \dots, g_k \in F[x]$, então as congruências simultâneas $h \equiv g_i \, mod \, f_i, i = 1,2, \dots, k$ tem uma única solução $h \in F[x]$ módulo $f = f_1.f_2 \dots f_k$.

Em particular, o Teorema Chinês dos Restos garante que dado um k-uplo qualquer $(c_1, c_2, \dots, c_k)$ de elementos de $\mathbb{F}_q$ existe um único $h \in \mathbb{F}_q[x]$ com $h(x) \equiv c_i \, mod \, f_i(x)$, $1 \leq i \leq k$ e $\deg(h) < \deg(f)$, ou seja, que os fatores de f dividem o polinômio $h(x) - c$ para algum $c \in \mathbb{F}_q$. O algoritmo consiste basicamente na construção destes $h's$ através de um sistema linear que é obtido através da equação $h^q \equiv h \, mod \, f$ quando substituímos h pela sua forma geral $h(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$. A base do espaço nulo associado sistema terá tantos vetores quanto o número de fatores irredutíveis de f, base esta que são justamente os $h's$ que estamos procurando. É possível mostrar com o auxílio do teorema Chinês dos Restos e com alguns cálculos que quaisquer dois fatores mônicos e irredutíveis de $f(x)$ são separados por algum $h_j(x)$ com $1 \leq j \leq k$, ou seja, $h_j(x) - c$ será divisível por $f_1(x)$, mas não por $f_2(x)$. Se $k = 1$, nós sabemos que f é irredutível sobre$\mathbb{F}_q[x]$ e o processo termina. No caso, as soluções são somente polinômios constantes, e o espaço nulo de $B - I$ contém somente vetores na forma $(c, 0, \dots, 0)$ com $c \in \mathbb{F}_q$. Se $k \geq 2$, nós pegamos as bases, ou seja, os $h's$ que são chamados de *f-reducing polynomials* $h_2(x)$ e calculamos o $gcd(f(x), h_2(x) - c)$ para todo $c \in \mathbb{F}_q$. O resultado será uma fatorização não-trivial de $f(x)$ fornecida pelo teorema 1. Se o uso $h_2(x)$ não dividirmos com sucesso f em k fatores, nós calculamos $gcd(g(x), h_3(x) - c)$ para todo $c \in \mathbb{F}_q$ e todos os fatores não triviais de $g(x)$ são encontrados rapidamente. Este processo segue até que os fatores de f sejam obtidos.

Seguem abaixo os passos do algoritmo:

1)Calcular as potências $x^{iq} rem f(x) = \sum_{j=0}^{n-1} b_{ij} x^j$ e $0 \leq i \leq n-1$.

2)Construir a matriz $nxn \; B = \left(b_{ij}\right), 0 \leq i, j \leq n-1$.

3)Obter a base do espaço nulo associado a matriz $B - I$ no qual, I é a matriz identidade.

4) Efetuar o cálculo dos GCD's.

Cabe ressaltar que a fatorização provido por este algoritmo depende do cálculo dos r máximo divisores comum, com $\mathrm{r} \geq q$, uma aplicação direta desta fórmula é praticável somente para pequenos corpos finitos $\mathbb{F}_q$

REFERÊNCIAS

- LIDL, Rudolf; NIEDERREITER, Harald. **Finite Fields.**

- GATHEN, Joachim Von Zur; GERHARD, Jurgen. **Modern Computer Algebra**.

25 anos
MODALIDADE DE BOLSA Iniciação Científica