Fatoração de Polinômios Bivariados

Autor: Guilherme Porto[1] **Orientador: Luiz Emilio Allem[2]**

1 Licenciando em Matemática, Instituto de Matemática Pura e Aplicada - UFRGS.
2 Professor Adjunto da UFRGS no Instituto de Matemática Pura e Aplicada.

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

1. Introdução

No XXIV Salão de Iniciação Científica da UFRGS apresentamos os métodos que estudamos para o desenvolvimento de um algoritmo que realiza a fatoração de polinômios bivariados sobre corpos finitos utilizando conhecimentos relacionados ao levantamento de Hensel e a fatoração polinomial univariada. Neste trabalho apresentaremos uma extensão do algoritmo que possibilita a fatoração de um número maior de polinômios utilizando conhecimentos relacionados a extensões algébricas.

Levantamento de Hensel:

O levantamento de Hensel é uma técnica que providencia um método prático e eficaz para a fatoração de polinômios sobre vários corpos. Utilizaremos ele para realizarmos a fatoração de polinômios bivariados.

Extensão Algébrica:

Realizamos a extensão algébrica de um corpo $\mathbb{F}_q$ visando gerar um novo corpo $\mathbb{F}_q[\alpha]$ com um número maior de elementos onde poderemos fatorar um polinômio que é irredutível em $\mathbb{F}_q$.

2. O Algoritmo Inicial

Trabalhamos com o seguinte modelo de polinômios bivariados:

Modelo $T(n,q)$:

Para um inteiro $n \geq 1$, denotamos $T(n,q)$ o conjunto de todos os polinômios em $\mathbb{F}_q[x,y]$ de grau total n, mônicos em x e com grau n em x

Nosso algoritmo inicial fatora polinômios do seguinte modelo:

Modelo $M(n,q)$:

Para um inteiro $n \geq 1$, temos que $M(n,q) \subseteq T(n,q)$ denota o subconjunto de todos os polinômios em $T(n,q)$ cuja redução módulo y é livre de quadrados.

Mostremos o algoritmo a seguir:

Algoritmo 1:

▶**Entrada:** Um polinômio $f = \sum_{k=0}^{n} f_k y^k \in M(n,q)$, onde $f_k \in F_q[x]$.
▶**Saída:** Todos os fatores mônicos de f com grau total entre 1 e $\lfloor n/2 \rfloor$.
▶**Passo 1.1:** Use um algoritmo para fatoração de polinômios univariados para fatorar $f_0 \equiv f \bmod y$, um polinômio livre de quadrados.
Se f_0 é irredutível então pare o algoritmo pois f é irredutível.
No entanto se f_0 é redutível. Liste todos os pares (g_0, h_0) dos fatores mônicos com $f_0 = g_0 h_0$ e $1 \leq grau(g_0) \leq grau(h_0)$. Para cada par (g_0, h_0), faça os passos de 1.2 até 1.4, onde $r = grau(g_0)$ para $1 \leq r \leq \lfloor n/2 \rfloor$.
▶**Passo 1.2:** Calcular polinômios u e v com $ug_0 + vh_0 = 1$ e grau$(u) <$ grau(h_0), $grau(v) < grau(g_0)$.
▶**Passo 1.3:** Para k de 1 à $\lfloor n/2 \rfloor$, calcular g_k e h_k utilizando as equações abaixo.

$$g_k = v(f_k - \sum_{i=1}^{k-1} g_i h_{k-i}) \bmod g_0 \quad (1)$$

$$h_k = u(f_k - \sum_{i=1}^{k-1} g_i h_{k-i}) \bmod h_0 \quad (2)$$

No caso em que $r \geq k$ verificar se $grau(g_k) \leq r - k$, e no caso de o que $k > r$ verificar se $g_k = 0$. Se uma destas duas condições não for satisfeita interromper o cálculo para este par.
▶**Passo 1.4:** Verifique se $g = \sum_{k \geq 0} g_k y^k$ divide f. Se sim, então fornecer g como saída.

3. Objetivo

- Implementar o processo de extensão algébrica no Algoritmo 1 para maximizar sua utilidade na fatoração de polinômios bivariados sobre corpos finitos.
- Realizar a fatoração de todos os polinômios bivariados do modelo $T(n,q)$.

4. Extensão Algébrica De Corpos Finitos

Dado um corpo $\mathbb{F}_q$ e um polinômio $p(x) \in \mathbb{F}_q[x]$ irredutível podemos realizar a adjunção de uma raiz $\alpha \in L$ de $p(x)$, com $\mathbb{F}_q \subset L$ e $\alpha \notin \mathbb{F}_q$, ao corpo finito $\mathbb{F}_q$ realizando sua extensão algébrica para um corpo maior $\mathbb{F}_q[\alpha]$ onde pode ser possível realizar a fatoração de $p(x) \in (\mathbb{F}_q[\alpha])[x]$.
Tomemos $p(x) \in \mathbb{F}_q[x]$ um polinômio irredutível com grau $p(x) = n$. Logo temos que o ideal $J = p(x)\mathbb{F}_q[x]$ é maximal.
Seja $\alpha \in L$ com $\mathbb{F}_q \subset L$ e $\alpha \notin \mathbb{F}_q$ com $p(\alpha) = 0$, ou seja, α é raíz de $p(x) \in \mathbb{F}_q$.
Logo pela Teorema dos Isomorfismos temos que:

$$\frac{\mathbb{F}_q[x]}{J} \simeq \mathbb{F}_q[\alpha]$$

Segue pelo Teorema dos Isomorfismo que $\mathbb{F}_q[\alpha]$ é um corpo da forma $\mathbb{F}_q[\alpha] = \{a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1} | a_i \in \mathbb{F}_q\}$.
Dizemos que $\mathbb{F}_q[\alpha]$ é uma extensão algébrica do corpo $\mathbb{F}_q$ e temos que $\mathbb{F}_q \subset \mathbb{F}_q[\alpha] \subset L$.
Com isso temos que $\#\mathbb{F}_q[\alpha] = q^n$ e portanto continua sendo um corpo finito.

5. Aplicação da Extensão Algébrica

Para fatorar um polinômio $f \in T(n,q)$ devemos inicialmente verificar se $f \in M(n,q)$, para isso realizamos o rebaixamento de f para um polinômio $f_0 \in \mathbb{F}_q[x]$ e verificamos se é livre de quadrados.
Para realizar o rebaixamento de $f \in T(n,q)$ tomamos $y = \beta$, com $\beta \in \mathbb{F}_q$ e assim obtemos $f(x,\beta) \in \mathbb{F}_q[x]$. Caso $f(x,\beta)$ não seja livre de quadrados para todo $\beta \in \mathbb{F}_q$ temos que $f \notin M(n,q)$ e portanto, o Algoritmo 1 não pode fatorar f.
Neste caso passamos ao processo de extensão algébrica do corpo $\mathbb{F}_q$ onde adjuntamos uma raiz $\alpha \in L$ com $\mathbb{F}_q \subset L$ e $\alpha \notin \mathbb{F}_q$ para gerar o corpo $\mathbb{F}_q[\alpha]$. Como $\#\mathbb{F}_q[\alpha] > \#\mathbb{F}_q$ temos mais possibilidades para obtermos $f(x,\beta)$ livre de quadrados para algum $\beta \in \mathbb{F}_q[\alpha]$.
Se existir $\beta \in \mathbb{F}_q[\alpha]$ tal que $f(x,\beta)$ seja livre de quadrados poderemos aplicar o Algotirmo 1 e fatorar f.
Caso contrário descartamos essa extensão algébrica e realizamos uma diferente buscando encontrar um corpo $\mathbb{F}_q[\gamma]$ onde exista $\beta \in \mathbb{F}_q[\gamma]$ tal que $f(x,\beta)$ seja livre de quadrados e com isso poderemos utilizar o Algoritmo 1 para fatorar f.

6. O Novo Algoritmo

Nesta versão do algoritmo realizaremos a fatoração de um polinômio $f \in T(n,q)$.
Mostremos o algoritmo a seguir:

Algoritmo 2:

▶**Entrada:** Um polinômio $f = \sum_{k=0}^{n} f_k y^k \in T(n,q)$, onde $f_k \in F_q[x]$.
▶**Saída:** Todos os fatores mônicos de f com grau total entre 1 e $\lfloor n/2 \rfloor$.
▶**Passo 2.1:** Use um algoritmo para fatoração de polinômios univariados para fatorar $f(x,\beta) \in \mathbb{F}_q[x]$ para todo $\beta \in \mathbb{F}_q$.
Se $f(x,\beta)$ é livre de quadrados para algum $\beta \in \mathbb{F}_q$ tome $f_0 = f(x,\beta) \in \mathbb{F}_q[x]$ e vá para o Passo 2.3.
Se $f(x,\beta)$ não é livre de quadrados para todo $\beta \in \mathbb{F}_q$ vá para o Passo 2.2.
Se $f(x,\beta)$ é irredutível para todo $\beta \in \mathbb{F}_q$ então pare o algoritmo pois f é irredutível.
▶**Passo 2.2:** Tome um polinômio $p(x) \in \mathbb{F}_q[x]$ irredutível com $p(\alpha) = 0$, sendo $\alpha \in L$, $\mathbb{F}_q \subset L$ e $\alpha \notin \mathbb{F}_q$. Usando este $p(x)$ construa o corpo $\mathbb{F}_q[\alpha]$.
Use um algoritmo para fatoração de polinômios univariados para fatorar $f(x,\gamma) \in (\mathbb{F}_q[\alpha])[x]$ para todo $\gamma \in \mathbb{F}_q[\alpha]$.
Se $f(x,\gamma)$ é livre de quadrados para algum $\gamma \in \mathbb{F}_q[\alpha]$ tome $f_0 = f(x,\gamma) \in (\mathbb{F}_q[\gamma])[x]$ e vá para o Passo 2.3.
Se $f(x,\gamma)$ não é livre de quadrados para todo $\gamma \in \mathbb{F}_q[\alpha]$ repita o Passo 2.2 utilizando outro polinômio $p(x) \in \mathbb{F}_q[x]$ irredutível.
▶**Passo 2.3:** Liste todos os pares (g_0, h_0) dos fatores mônicos com $f_0 = g_0 h_0$ e $1 \leq grau(g_0) \leq grau(h_0)$. Para cada par (g_0, h_0), vá para o passo 2.4, tomando $r = grau(g_0)$ para $1 \leq r \leq \lfloor n/2 \rfloor$.
▶**Passo 2.4:** Realizar do Passo 1.2 ao Passo 1.4 do Algoritmo 1.

Referências

▶Shuhong Gao and Alan G.B. Lauder, "Hensel lifting and polynomial factorisation," Mathematics of Computation 71 (2002), 1663-1676.
▶Gathen, Joachim von zur; Gerhard, Jürgen. "Modern Computer Algebra".
▶Stewart, Ian. "Galois Theory-3rd. edition".

25 anos
MODALIDADE DE BOLSA **PIBIC CNPq-UFRGS**