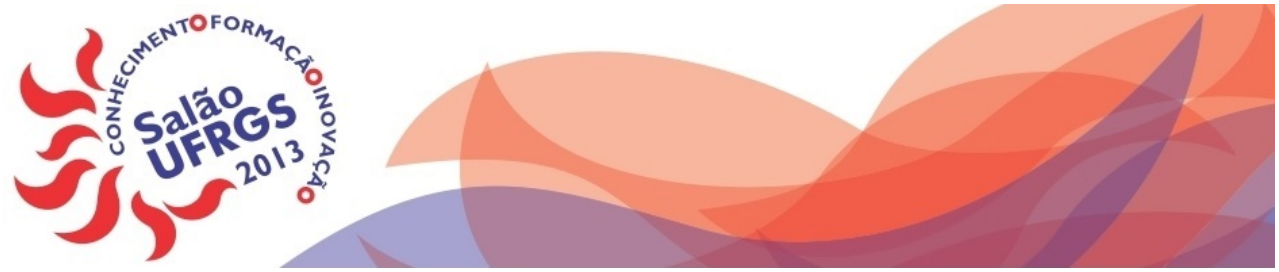

Evento	Salão UFRGS 2013: SIC - XXV SALÃO DE INICIAÇÃO CIENTÍFICA DA UFRGS
Ano	2013
Local	Porto Alegre - RS
Título	Fatoração de Polinômios Bivariados
Autor	GUILHERME PORTO DA SILVA
Orientador	LUIZ EMILIO ALLEM

No Salão de Iniciação científica da UFRGS de 2012 apresentamos os métodos que estudamos para o desenvolvimento de um algoritmo para a fatoração de polinômios bivariados sobre corpos finitos utilizando conhecimentos relacionados ao levantamento de Hensel e a fatoração polinomial. Para este ano apresentamos uma extensão deste algoritmo que faz com que um número maior de polinômios possam ser fatorados aumentando sua eficácia.

Para nos guiar por esse estudo utilizamos o artigo Hensel Lifting and Bivariate Polynomial Factorisation Over Finite Fields escrito por Shuhong Gao e Alan G. B. Lauder, o livro Galois Theory escrito por Ian Stewart e o livro Introdução a Álgebra escrito por Adilson Gonçalves.

Começamos nossos estudos tratando de tópicos relacionados à teoria de anéis, teoria de ideais e teoria de corpos onde nosso objetivo era compreender como são às relações de isomorfismo entre anéis quocientes e corpos e o processo de adjunção de raízes a corpos para então podermos construir extensões algébricas visando fatorar polinômios em corpos que possuem uma quantidade maior de elementos.

Tomamos como motivação para realizar o estudo de extensões algébricas fazer com que nosso algoritmo consiga realizar a fatoração de uma quantidade maior de polinômios. Implementando este processo ao nosso algoritmo podemos maximizar sua utilidade na fatoração de polinômios bivariados sobre corpos finitos.

Em nosso algoritmo anterior tínhamos que dado um polinômio $f(x,y) \in \mathbb{F}_q[x,y]$ inicialmente realizamos o rebaixamento desse polinômio para o anel $\mathbb{F}_q[x]$, para isto tomamos $y = \beta$, com $\beta \in \mathbb{F}_q$ e assim obtemos $f(x,\beta) \in \mathbb{F}_q[x]$.

Caso $f(x,\beta)$ seja livre de quadrados para algum $\beta \in \mathbb{F}_q$ o algoritmo consegue realizar a fatoração. Caso $f(x,\beta)$ não seja livre de quadrados para todo $\beta \in \mathbb{F}_q$ o algoritmo não pode realizar a fatoração de $f(x,y) \in \mathbb{F}_q[x,y]$.

Para prosseguirmos no caso onde $f(x,\beta)$ não é livre de quadrados passamos ao processo de adjunção de raízes visando adicionar uma raiz $\alpha \in L$ ao corpo $\mathbb{F}_q$, com $\mathbb{F}_q \subset L$ e $\alpha \notin \mathbb{F}_q$, para criarmos a extensão algébrica $\mathbb{F}_q[\alpha]$ de modo que tenhamos $f(x,\alpha) \in (F_q[\alpha])[x]$ livre de quadrados e possamos fatorá-lo.

Para isso tomamos $g(x) \in \mathbb{F}_q[x]$ irredutível e $\alpha \in L$ com $\mathbb{F}_q \subset L$ e $\alpha \notin \mathbb{F}_q$ de modo que $g(\alpha) = 0$ e assim construímos o corpo $\mathbb{F}_q[\alpha]$.

Agora realizamos o rebaixamento do polinômio $f(x,y)$ para o anel $(\mathbb{F}_q[\alpha])[x]$, para isto tomaremos $y = \beta$ com $\beta \in (\mathbb{F}_q[\alpha])$ e assim obtemos $f(x,\beta) \in (\mathbb{F}_q[\alpha])[x]$, no entanto note que a quantidade de elementos em $\mathbb{F}_q[\alpha]$ é maior do que a quantidade de elementos em $\mathbb{F}_q$ e portanto temos mais possibilidades para obtermos $f(x,\beta)$ livre de quadrados para algum $\beta \in \mathbb{F}_q[\alpha]$.

Caso consigamos encontrar um $\beta \in \mathbb{F}_q[\alpha]$ tal que $f(x,\beta)$ seja livre de quadrados aplicamos o algoritmo e fatoramos $f(x,y) \in \mathbb{F}_q[x,y]$.

Caso não consigamos encontrar $\beta \in \mathbb{F}_q[\alpha]$ tal que $f(x,\beta)$ seja livre de quadrados descartamos essa extensão e realizamos uma diferente buscando encontrar corpo $\mathbb{F}_q[\gamma]$ onde exista $\beta \in \mathbb{F}_q[\gamma]$ tal que $f(x,\beta)$ seja livre de quadrados e possamos fatorá-lo.

Podemos introduzir o processo acima como uma nova etapa em nosso algoritmo alterando sua estrutura de modo a fornecer um aumento significativo da utilidade do algoritmo, uma vez que obtemos capacidade para realizar a fatoração de uma quantidade maior de polinômios bivariados sobre corpos finitos.