CS 681: Computational Number Theory and Algebra **Lecture 9**

Polynomial factorization over Finite Fields

Lecturer: Manindra Agrawal **Scribe: Sudeepa Roy**

August 19, 2005

1 Introduction

In the last lecture we studied the tool automorphism over finite rings. In this lecture we will discuss how to use automorphism to factorize a polynomial over finite fields.
Let $f(x)$ be a polynomial of degree d over field F_q.

Definition 1.1 *f is **square free** if g^2 does not divide for any g.*

2 Factorization algorithms for different types of polynomials

2.1 Case I : f is not square free

In this case $g^2 \mid f$ for some g.
Let $\frac{df}{dx} = f'$.
Then $g \mid gcd(f, f')$.
This produces a factor of f.

2.2 Case II : f is square free

Let $f \;=\; f_1 f_2 \cdots f_k$
where each f_i is irreducible and let $\deg f_i \;=\; d_i$ with

$$d_1 \leq d_2 \leq \cdots \leq d_k$$

Let $R = F_q[X]/(f(X))$
$= \oplus_{i=1}^{k} F_q[X]/(f_i(X))$
[by Chinese Remaindering, as all the f_i s are distinct and irreducible, so are prime to each other].

Let
$\quad \psi(y) \;=\; y^q$

Observation 2.1 *ψ is an automorphism of $F_q[X]/(f_i(X))$ and $\psi^j = id$ in $F_q[X]/(f_i(X))$ iff $j \;=\; d_i$.*

2.2.1 Case II.1 : There is an i such that $d_i > d_1$

Then ψ^{d_1} is trivial in $F_q[X]/(f_1(X))$ but not in $F_q[X]/(f_i(X))$.
In other words,

$\psi^{d_1}(X) - X = 0$ in $F_q[X]/(f_1(X))$ but not in $F_q[X]/(f_i(X))$
$\Rightarrow f_1(x) \mid \psi^{d_1}(x) - x$ but ***not*** $f_i(x) \mid \psi^{d_1}(x) - x$

Algorithm

$for\ i = 1\ to\ d-1\ do$
compute $gcd(\psi^i(x) - x,\ f(x))$

Time Complexity

Observation 2.2 $gcd(\psi^i(x) - x,\ f(x)) = gcd((\psi^i(x) - x) \mod f(x),\ f(x))$

Hence in each step of the algorithm we will perform $= gcd(x^{q^i} \mod f(x) - x,\ f(x))$ so that the degree of both the terms are bounded above by $\deg f(x) = d$.

To compute x^{q^i} we will follow repeated squaring method, where we will compute the sequence $x, x^2, x^4, \cdots, x^{2^j}$ [each modulo f] unless $2^j > q^i$.
Here no. of squaring required $= \log q^i = i \log q \leq d \log q$ as $i \leq d$.

Using FFT, complexity of polynomial multiplication = complexity of polynomial division $= O(d \log d)$ where degree of each polynomial is bounded by d. So at each step of the above sequence computation, multiplication and taking modulo f needs $O(d \log d)$ operations. As each element of the field F_q is $\log q$ bits long, so complexity of multiplication of coefficients of f using FFT is $O(\log q\ \log\log q\ \log\log\log q)$, or ignoring sublogarithmic factors $\tilde{O}(\log q)$.

Hence time complexity to compute x^{q^i}
$= \tilde{O}(d \log q.\ d \log d.\ \log q)$
$= \tilde{O}(d^2\ (\log q)^2\ \log d)$
$= \tilde{O}(d^2 \log^2 q)$ [ignoring $\log d$ factor]

To compute $gcd(\psi^i(x) - x,\ f(x))$
$= \tilde{O}(d^3 \log^2 q)$ [as we may have to iterate at most d times to get the gcd].

Hence to iterate the procedure $d - 1$ times, time complexity of the algorithm $= \tilde{O}(d^4 \log^2 q)$.
[Using more intelligent gcd algorithm the time complexity can be reduced by a factor of d].

2.2.2 Case II.2 : $d_1 = d_2 = \cdots = d_k = \frac{d}{k}$

In this case, $gcd(\psi^i(x) - x,\ f(x)) = 1$ for $i < \frac{d}{k}$ and $gcd(\psi^{\frac{d}{k}}(x) - x,\ f(x)) = f(x)$. Hence we can obtain no. of factors of the polynomial f, if we note down the point $i = t$ such that the value of the gcd changes from 1, then $\frac{d}{t} = k =$ no. of factors of f.

The first step will be to reduce the problem to finding roots [finding roots is equivalent to find the linear factors of f, so it is no harder than factorization problem].

$R = \oplus_{i=1}^{k} F_q[X]/(f_i(X))$ [by Chinese Remaindering, as all the f_is are distinct and irreducible]
Let $S = \{e(X) \mid e(X) \in R \ \& \ \psi(e(X)) = e(X)\}$
Each $e(X)$ can be viewed as a k-tuple.

Observation 2.3 *Each component of $e(X) \in S$ represented as a k-tuple $\in F_q$.*

Hence,
$|S| = q^k > q = |F_q|$ if $k > 1$.
[We have k tuples and q elements in each tuple, and by Chinese Remaindering Theorem all are distinct elements of R]
$\Rightarrow$ There is an $e(X) \in S - F_q$

[To be continued in the next lecture].