A Note on Irreducible Polynomials and Identity Testing

Chandan Saha
Department of Computer Science and Engineering
Indian Institute of Technology Kanpur

Abstract

We show that, given a finite field F_q and an integer $d > 0$, there is a deterministic algorithm that finds an irreducible polynomial g over F_q in time polynomial in d and $\log q$ such that,

$$\frac{d}{c \log p} < deg(g) < \frac{d \log q}{\log p}$$

where c is a constant. This result follows easily from Adleman and Lenstra's result [AJ86] on irreducible polynomials over prime fields and Lenstra's result [Jr.91] on isomorphisms between finite fields. [1] As an application, we show that such construction of irreducible polynomials can be used to build a sample space of coprime polynomials for the Agrawal-Biswas [AB03] polynomial identity testing algorithm.

1 Introduction

The problem of finding irreducible polynomials over finite fields is an important problem in algorithmic algebra with many applications in coding theory, cryptography and complexity theory. In many such applications the primary use of irreducible polynomials is in the construction of larger finite fields. Although a random polynomial is irreducible with reasonable probability, there is no known deterministic polynomial time algorithm for contructing irreducible polynomial of a given degree. An efficient algorithm was designed by Adleman and Lenstra [AJ86] in case of prime fields under the assumption of the Extended Riemann Hypothesis. In the same paper they gave another result as stated by the following theorem.

Theorem 1.1 *There is a deterministic algorithm that on input a prime p and an integer $d > 0$, outputs an irreducible polynomial $g \in F_p[x]$ such that*

$$\frac{d}{c \log p} < deg(g) < d$$

where c is a constant. The algorithm takes $(d \log p)^{O(1)}$ time.

We show that this result can be extended to any finite field as stated by the following theorem.

Theorem 1.2 *Let F_q be a finite field, with $q = p^u$ and p prime, that is explicitly given by an irreducible polynomial $f \in F_p[x]$ of degree u i.e. $F_q = \frac{F_p[x]}{(f)}$. Given an integer $d > 0$, there is a deterministic algorithm that outputs an irreducible polynomial $g \in F_q[x]$ such that,*

$$\frac{d}{c \log p} < deg(g) < \frac{d \log q}{\log p}$$

where c is a constant. The algorithm takes $(d \log q)^{O(1)}$ time.

[1] Hendrik W. Lenstra Jr. pointed out that a stronger result follows from [AJ86] and [Jr.91] i.e. it is possible to find a degree d irreducible polynomial over F_q from a degree d irreducible polynomial over F_p.

Our proof is fairly straightforward and it makes use of Theorem 1.1 and a result by Lensta [Jr.91] on isomorphism between finite fields,

Theorem 1.3 *There is an algorithm that, given a finite field F, a positive integer u, and two field extensions F_1, F_2 of F of degree u, constructs an F-isomophism $F_1 \rightarrow F_2$ in time $(\log \mid F_1 \mid)^{O(1)}$.*

In the absence of an efficient deterministic algorithm for finding irreducible polynomial of a given degree, partial result like Theorem 1.2 could be useful as there are applications where an irreducible polynomial of roughly the desired degree is just as good. We have chosen one such application from complexity theory - the problem of testing whether a polynomial, given as a circuit, is identically zero.

We show that Theorem 1.2 is useful in the construction of a sample space of polynomials used by Agrawal and Biswas's algorithm [AB03] to check if an input polynomial is identically zero. In their paper [AB03], Agrawal and Biswas showed an elegant way of constructing a small space of *almost* coprime low degree polynomials. Their algorithm works by randomly selecting a polynomial from the sample space and computing the output of the circuit modulo the chosen polynomial. The input polynomial is declared as identically zero if and only if the output of the circuit is evaluated to zero. An important feature of their algorithm is that it achieves the time-error tradeoff with a running time that is only polynomial in the size of the circuit and the error parameter.

For the sake of theoretical interest, it is natural to ask if one can get a similar result using a sample space of mutually coprime polynomials instead of almost coprime polynomials. We answer this question affirmatively. The time-error tradeoff property of the algorithm is also preserved. A slight advantage of using coprime polynomials over almost coprime polynomials is that the degree of each polynomial in the sample space can be chosen to be smaller than the polynomials in the sample space of almost coprime polynomials. This makes modulo operations less costly which gives a slightly better running time of the algorithm for large enough circuits.

2 Finding Irreducible Polynomials

In this section we prove Theorem 1.2.

Theorem 2.1 *Let F_q be a finite field, with $q = p^u$ and p prime, that is explicitly given by an irreducible polynomial $f \in F_p[z]$ of degree u i.e. $F_q = \frac{F_p[z]}{(f)}$. Given an integer $d > 0$, there is a deterministic algorithm that outputs an irreducible polynomial $g \in F_q[y]$ such that,*

$$\frac{d}{c \log p} < deg(g) < \frac{d \log q}{\log p}$$

where c is a constant. The algorithm takes $(d \log q)^{O(1)}$ time.

Proof: The field F_q denotes the explicitly given field $\frac{F_p[z]}{(f)}$. The outline of the proof is as follows.

1. Construct a sufficiently large field E that contains F'_q, an isomorphic copy of F_q. The extension degree $[E : F'_q]$ should be sufficiently large so that step 2 is feasible.
2. Construct an irreducible polynomial $g' \in F'_q[y]$ such that

$$\frac{d}{c \log p} < deg(g') < \frac{d \log q}{\log p}.$$

3. Use an isomorphism to find an irreducible polynomial $g \in F_q[y]$ such that $deg(g) = deg(g')$.

The rest of the proof shows how to perform each of these steps.

Step 1: Construct a sufficiently large field.

Finding a sufficiently large extension of F_p is made easy by Theorem 1.1, but the only complication being that this extended field might not contain an isomorphic copy of F_q. This is because Theorem 1.1 does not provide a handle on the exact value of the extension degree. The following discussion shows how to circumvent this problem.

Using Theorem 1.1 first find an irreducible polynomial $h \in F_p[x]$ of degree m such that,

$$\frac{ud}{c \log p} < m < ud.$$

The field $F_{p^m} = \frac{F_p[x]}{(h)}$ may not contain an isomorphic copy F_q (as u may not divide m). Therefore, we intend to construct the field $F_{p^{m'}}$ where $m' = lcm(m, u)$. To do this first find the prime factorizations of m and u and find $m' = lcm(m, u)$. Suppose v be a prime such that $v^k || m'$ (v^k exactly divides m'). Then v^k exactly divides m or u. Assume without loss of generality that $v^k || m$. Let $F = F_{p^m}$ and $K = F_{p^{v^k}}$. The idea is to find an element that generates K over F_p. For this we make use of the trace function.

Recall that, if $M = F_{q^k}$ is an extension field of $N = F_q$ then the function $Tr_{M|N} : M \to N$ is defined as the sum,

$$Tr_{M|N}(\alpha) = \alpha^{q^{m-1}} + \alpha^{q^{m-2}} + \ldots + \alpha^q + \alpha, \quad \text{for every } \alpha \in M.$$

Function $Tr_{M|N}$ is a linear map from M onto N.

Consider taking trace of the elements, $X, \ldots, X^{m-1}$, of F over K,

$$Tr_{F|K}\left(X^i\right) \quad \text{for } 0 < i < m,$$

where $X = x \mod h$. Since the elements $1, X, \ldots, X^{m-1}$ form the basis of F over F_p and v is prime, there must exist an i, $0 < i < m$, such that,

$$K = F_{p^{v^k}} = F_p(Tr_{F|K}\left(X^i\right)).$$

Otherwise the fact that $Tr_{F|K}$ maps F onto K is contradicted. If $\alpha_v = Tr_{F|K}\left(X^i\right)$ is the generator of K over F_p, then the minimal polynomial of α_v over F_p is an irreducible polynomial h_v of degree v^k. The task of finding α_v and h_v is efficient because finding minimal polynomial and testing for irreducibility can be done in deterministic polynomial time.

By repeating the above process for other prime factors of m', we can find all irreducible polynomials of degree w^ℓ such that $w^\ell || m'$ and w is a prime. Suppose $h_v(x)$ and $h_w(y)$ be two irreducible polynomials of relatively coprime degrees v^k and w^ℓ respectively. Let $F_p(X) = \frac{F_p[x]}{(h_v)}$ and $F_p(Y) = \frac{F_p[y]}{(h_w)}$ where $X = x \mod h_v$ and $Y = y \mod h_w$. Then it is not difficult to verify that $F_p(X, Y) = F_p(X + Y) = F_{p^{v^k w^\ell}}$. This is because any maximal proper subfield of $F_{p^{v^k w^\ell}}$ must contain either X or Y and hence cannot contain $X + Y$. Therefore, the minimal polynomial of $X + Y$ over F_p yields an irreducible polynomial of degree $v^k w^\ell$. Repeat this process

till we get an irreducible polynomial of degree m' over F_p. Let this polynomial be h'. The field $E = \frac{F_p[x]}{(h')} = F_{p^{m'}}$ thus contains an isomorphic copy of F_q which we denote by F'_q.

Step 2: Constructing irreducible polynomial over F'_q.

As before, assume that $E = \frac{F_p[x]}{(h')}$ and $X = x \mod h'$. The minimal polynomial of $X \in E$ over F'_q is an irreducible polynomial of degree $\frac{m'}{u}$ over F'_q. The process of finding a monic polynomial of degree $\frac{m'}{u}$ with coefficients taken from F'_q reduces to solving a bunch of linear equations over F_p. To see this reduction assume that X satisfies the monic polynomial $g'(y) \in F'_q[y]$,

$$g'(y) = \sum_{i=0}^{m'/u} \beta_i y^i \quad \text{where } \beta_i \in F'_q \text{ and } \beta_{\frac{m'}{u}} = 1.$$

Take each $\beta_i \in E$ to be,

$$\beta_i = \sum_{j=0}^{m'-1} b_{ij} x^j \quad \text{where } b_{ij}\text{'s are unknowns in } F_p.$$

We can ensure that each β_i belongs to F'_q using the equation $\beta_i^q = \beta_i$, which in turn reduces to linear equations in b_{ij}'s. Further, since X is a root of $g'(y)$,

$$g'(X) = \sum_{i=0}^{m'/u} \beta_i x^i \mod h' = 0$$

which yields more linear equations in b_{ij}'s. By solving the equations for b_{ij}'s we get the unique irreducible polynomial $g'(y) \in F'_q[y]$ of degree $\frac{m'}{u}$.

Step 3: Finding an irreducible polynomial over F_q through an isomorphism.

Suppose that v is a prime factor of u such that $v^k || u$ and let $K = F_{p^{v^k}}$. As argued before, there exists an i $(0 \le i < m')$ such that for $\alpha = Tr_{E|K}(X^i)$, $K = F_p(\alpha)$. Moreover, if $F_{p^{v^k}} = F_p(\alpha)$ and $F_{p^{w^\ell}} = F_p(\beta)$ where v and w are distinct prime divisors of u then $F_{p^{v^k w^\ell}} = F_p(\alpha + \beta)$. This way we can find an element $\gamma \in E$ such that $F'_q = F_p(\gamma)$. Let $f'(y) \in F_p[y]$ be the minimal polynomial of γ over F_p. Using Theorem 1.3 find an isomorphism $\sigma(z)$ from $\frac{F_p[z]}{(f')}$ to $F_q = \frac{F_p[z]}{(f)}$. This means that the element z in $\frac{F_p[z]}{(f')}$ maps to the element $\sigma(z)$ in $F_q = \frac{F_p[z]}{(f)}$. Since $g'(y)$ belongs to $F'_q[y]$, we can express each coefficient of $g'(y)$ as an F_p-linear combinations of the basis elements $\{\gamma^j\}_{1 \le j < u}$. This is done by solving linear equations over F_p. Thus if $\beta = \sum_{i=0}^{u-1} b_i \gamma^i$ is an element in F'_q then $\sum_{i=0}^{u-1} b_i \sigma(z)^i \mod f(z)$ is the image of β in F_q (by identifying γ with the element z in $\frac{F_p[z]}{(f')}$). This isomorphism when applied to the coefficients of $g'(y)$ yields an irreducible polynomial $g(y) \in F_q[y]$ of degree $\frac{m'}{u}$. Since,

$$\frac{ud}{c \log p} < m < ud \quad \text{and} \quad m \le m' \le mu,$$

hence,

$$\frac{d}{c \log p} < deg(g) < \frac{d \log q}{\log p}.$$

■

3 Constructing the sample space for Identity Testing

Let $\mathcal{C}$ be a circuit of size s that computes the polynomial $P(x_1, \ldots, x_n) \in F_q[x_1, \ldots, x_n]$. The task is to check whether the polynomial is identically zero. Assume that the degree in each variable is bounded by $d-1$. As in [AB03], first convert the multivariate polynomial to an univariate polynomial $P(x)$ by substituting x_i by $x^{d^{i-1}}$ (this is also known as *Kronecker substitution*). This substitution has the property that $P(x_1, \ldots, x_n)$ is a zero polynomial if and only if $P(x)$ is a zero polynomial. Note that the degree of polynomial $P(x)$ could be as high as $d^n - 1$.

The number of coprime polynomials of degree t that divides $P(x)$ is at most $\frac{d^n}{t}$. Suppose that we have a sample space of 2^r coprime polynomials of degree t, then the probability that a random polynomial from the sample space divides $P(x)$ is at most $\frac{d^n}{t \cdot 2^r}$. Thus if our sample space is large enough i.e. $2^r > d^n$ then the error probability is bounded by $\frac{1}{t}$. Constructing such a sample space is made easy by Theorem 1.2. First extend the field F_q to another field $F_{q'}$ using an appropriate irreducible polynomial such that $q' > d^n$. Since the field $F_{q'}$ is explicitly given by an irreducible polynomial over F_q, we can define a natural ordering among the elements in $F_{q'}$ using the ordering of elements in F_p. Thus with every $a \in F_{q'}$ we can associate a non-negative integer $index(a) < q'$. Also note that given an integer $i < d^n$ we can uniquely compute the element $a \in F_{q'}$ such that $index(a) = i$. Now define the sample space of polynomials as,

$$S = \{X^t + a : a \in F_{q'} \text{ and } index(a) < d^n\}$$

Such a sample space can be defined using only $r = \lceil n \log d \rceil$ random bits.

The time taken for evaluating *Kronecker substitutions* modulo a polynomial $(X^t + a)$ is $\tilde{O}(n^2 \log d \log \frac{q}{\epsilon})$, where $t = \frac{1}{\epsilon}$ and ϵ is the error parameter. The total time taken for modular operations in the circuit is $\tilde{O}(s \cdot \frac{1}{\epsilon} \cdot n \log d \cdot \log q)$, where s is the size of the circuit. In addition the time taken for extending the field is $(n \log d)^c$ for a constant c. Thus, when s is greater than $(n \log d)^c$, the total running time is $\tilde{O}(s \cdot \frac{1}{\epsilon} \cdot n \log d \cdot \log q)$. This is slightly better than the running time of $\tilde{O}((s + n^2 \log d) \cdot (n \log d)^2 \cdot (n \log d + \frac{1}{\epsilon}) \cdot (\log q)^2)$ given in [AB03].

4 Remarks

The arguments used to prove Theorem 1.2 can also be used to extend Aldleman and Lensta's [AJ86] other result on finding irreducible polynomial of a given degree over a prime field to any finite field, under the assumption of the Extended Riemann Hypothesis. It would be nice to find other applications of Theorem 1.2.

References

[AB03] Manindra Agrawal and Somenath Biswas. Primality and Identity Testing via Chinese Remaindering. *Journal of the ACM*, 50(4):429–443, 2003.

[AJ86] Leonard M. Adleman and Hendrik W. Lenstra Jr. Finding Irreducible Polynomials over Finite Fields. *STOC*, 1986.

[Jr.91] Hendrik W. Lenstra Jr. Finding Isomorphisms Between Finite Fields. *Mathematics of Computation*, 56(193):329–347, 1991.