New Algorithms for Finding Irreducible Polynomials over Finite Fields

Victor Shoup
Computer Sciences Department
University of Wisconsin–Madison
Madison, WI 53706

January 31, 1989

Abstract. We present a new algorithm for finding an irreducible polynomial of specified degree over a finite field. Our algorithm is deterministic, and it runs in polynomial time for fields of small characteristic. We in fact prove the stronger result that the problem of finding irreducible polynomials of specified degree over a finite field is deterministic polynomial time reducible to the problem of factoring polynomials over the prime field.

1980 Mathematics Subject Classification (1985 revision). Primary 11T06.

This research was supported by National Science Foundation grants DCR-8504485 and DCR-8552596.

Appeared in *Mathematics of Computation* 54, pp. 435–447, 1990.

A preliminary version of this paper appeared in *Proceedings of the 29th Annual Symposium on Foundations of Computer Science,* October 1988.

1. Introduction

In this paper we present some new algorithms for finding irreducible polynomials over finite fields. Such polynomials are used to implement arithmetic in extension fields found in many applications, including coding theory (Berlekamp [1968]), cryptography (Chor and Rivest [1984]), multivariate polynomial factoring (von zur Gathen and Kaltofen [1985]), and parallel polynomial arithmetic (Eberly [1984]).

Let p be a prime number, F the finite field $\mathrm{GF}(p)$, and n a positive integer. Consider the deterministic complexity of finding an irreducible polynomial in $F[X]$ of degree n. Since encoding a polynomial in $F[X]$ of degree n requires about $n \log p$ bits, a polynomial time algorithm for finding irreducible polynomials in $F[X]$ of degree n should run in time bounded by a polynomial in n and $\log p$. There is no known deterministic polynomial time algorithm for this problem. However, in many applications p is small, and so an algorithm that ran in time polynomial in n and p would be of value. We present one here. Specifically, we present a deterministic algorithm that on input n and p generates an irreducible polynomial in $F[X]$ of degree n, and—ignoring powers of $\log n$ and $\log p$—runs in time $O(p^{1/2}n^4)$. Thus, if p is fixed, e.g. $p = 2$, then our algorithm runs in polynomial time.

Notation and terminology. Throughout this paper, $\log x$ denotes $\log_2 x$. In order to simplify the statements of running times, we use the expression x^ϵ to denote a fixed, but unspecified, polynomial in $\log x$. As a further simplification, running times will be stated in terms of operations in F, by which we mean one of $+, -, \times$, or $/$. To obtain bit complexities, we can multiply by $(\log p)^2$ if classical integer arithmetic algorithms are used, or $(\log p)^{1+\epsilon}$ if fast integer arithmetic algorithms are used.

Our approach to constructing irreducible polynomials is as follows. In section 2, we show that if we are given certain nonresidues in extension fields of F, then we can deterministically generate an irreducible polynomial over F of degree n in polynomial time:

Theorem 2.1. *Assume that for each prime $q \mid n, q \neq p$, we are given a splitting field K of $X^q - 1$ over F and a q-th nonresidue in K. Then we can find an irreducible polynomial over F of degree n deterministically with $O((\log p)n^{4+\epsilon} + (\log p)^2)$ operations in F.*

In section 3, we go on to show that given an oracle for factoring polynomials over F, these extension fields and nonresidues—and hence irreducible polynomials over F of degree n—can be constructed deterministically in polynomial time:

Theorem 3.1. *The problem of constructing an irreducible polynomial over F of degree n can be deterministically reduced in time bounded by a polynomial in n and $\log p$ to the problem of factoring polynomials over F.*

We obtain a deterministic algorithm for generating irreducible polynomials by replacing the oracle by any variant of Berlekamp's deterministic factoring algorithm (Berlekamp [1970]). Using the fast deterministic factoring algorithm in Shoup [1988], we obtain our main result:

Theorem 3.2. *We can deterministically construct an irreducible polynomial over F of degree n with $O(p^{1/2}(\log p)^3 n^{3+\epsilon} + (\log p)^2 n^{4+\epsilon})$ operations in F.*

Theorem 3.2 implies that if p is a fixed prime, then we can deterministically construct an irreducible polynomial of over F of degree n in time $O(n^{4+\epsilon})$.

Even for small values of p, previous algorithms for generating irreducible polynomials suffer from at least one of three drawbacks: they rely on *a source of randomness*, they rely on *unproven conjectures* in the proofs of their run times, or they generate polynomials of degree only *approximately* n. Rabin [1980] gives a randomized polynomial time algorithm. Adleman and Lenstra [1986] give a deterministic algorithm that runs in polynomial time assuming the Extended Riemann Hypothesis (ERH). They also give a deterministic polynomial time algorithm that generates an irreducible polynomial of degree only approximately n. Von zur Gathen [1986] gives several deterministic algorithms that are efficient in practice, but his proofs of their running times rely on unproven conjectures, and they generate irreducible polynomials of degree only approximately n.

We also mention two other results on constructing irreducible polynomials, of which our results were obtained independently. In a paper on factoring polynomials over finite fields, Evdokimov [1986] gives another proof that irreducible polynomials of specified degree can be constructed deterministically in polynomial time assuming the ERH. Evdokimov's method of constructing irreducible polynomials is similar to ours in that Evdokimov essentially reduces this problem to the problem of finding various nonresidues in extension fields of F; however, Evdokimov constructs these nonresidues by appealing to the ERH (making use of results of Huang [1985] and Lagarias, Montgomerey and Odlyzko [1979]), and does not address the problem of constructing these nonresidues without relying on the ERH. Varshamov [1984] describes a method for constructing irreducible polynomials of specified degree; however, in some cases the method either breaks down or appears to require time greater than a polynomial in n and p.

In sections 4 and 5, we prove some extensions and related results. In section 4, we show that our result on finding irreducible polynomials extends to nonprime finite fields:

Theorem 4.1. *Given an extension K over F of degree d, we can construct an irreducible polynomial over K of degree n deterministically with $O(p^{1/2}(\log p)^3 n^{3+\epsilon} + (\log p)^2 n^{4+\epsilon} + (\log p) n^{4+\epsilon} d^{2+\epsilon})$ operations in F.*

This result allows us to deterministically construct in polynomial time an irreducible polynomial of specified degree over a finite field of small characteristic. If p is fixed, then our algorithm runs in time $O(n^{4+\epsilon} d^{2+\epsilon})$. The proof of Theorem 4.1 reduces the problem of finding an irreducible polynomial over K of degree n to the problem of factoring polynomials over F via the problem of constructing, for each prime $q \mid n, q \neq p$, the splitting field of $X^q - 1$ over F, along with a q-th nonresidue in this field, or just a primitive q-th root of unity if q also happens to divide d.

In section 5, we give a new randomized algorithm for finding irreducible polynomials that makes particularly efficient use of randomness, failing with probability exponentially small in the number of random bits used:

Theorem 5.1. *For any constant $0 < c < 1/4$, there exists a randomized algorithm (depending on c) with the following properties. It uses $\lceil n \log p \rceil$ random bits, halts in time polynomial in n and $\log p$, and upon termination, it either outputs an irreducible polynomial over F of degree n, or reports failure. Furthermore, the probability that it fails is no more than $1/p^{cn}$.*

This result is of value in a setting where random bits are viewed as a scarce resource. See Shoup [1987], Bach [1987], Bach and Shoup [1988], Karloff and Raghavan [1988], and Krizanc, Peleg and Upfal [1988] for other work along these lines.

2. Reduction to Constructing Cyclotomic Extensions and Finding Nonresidues

This section is devoted to a proof of

Theorem 2.1. *Assume that for each prime $q \mid n, q \neq p$, we are given a splitting field K of $X^q - 1$ over F and a q-th nonresidue in K. Then we can find an irreducible polynomial over F of degree n deterministically with $O((\log p)n^{4+\epsilon} + (\log p)^2)$ operations in F.*

The splitting field of $X^q - 1$ is the smallest extension of F containing a primitive q-th root of unity. It is also the smallest extension of F containing q-th nonresidues. From group theory, we see that this is just $\mathrm{GF}(p^m)$ where m is the smallest positive integer such that q divides $p^m - 1$, the order of the group $\mathrm{GF}(p^m)^*$. That is, m is the order of p mod q. Note that $m \mid q-1$. The hypothesis of Theorem 2.1 means that we are given an irreducible polynomial f over F of degree m and a q-th nonresidue a in $F(\alpha)$ where α is a root of f.

We now describe our algorithm. Let $n = q_1^{e_1} \cdots q_r^{e_r}$ be the prime factorization of n. We first construct irreducible polynomials over F of degree $q_i^{e_i}$ for $i = 1, \ldots, r$. We then "combine" these polynomials to form an irreducible polynomial of degree n.

Step 1: Constructing Irreducible Polynomials of Prime Power Degree

Let $1 \leq i \leq r$ be fixed, and let $q = q_i, e = e_i$. We want to construct an irreducible polynomial in $F[X]$ of degree q^e. We break the problem down into three cases: (1) $q \neq 2, \neq p$, (2) $q = 2, \neq p$, and (3) $q = p$.

Case 1: $q \neq 2, \neq p$

Let m be the order of p mod q. By hypothesis, we are given an irreducible polynomial f of degree m over F, and a q-th nonresidue a in $K = F(\alpha)$ where α is a root of f.

We will make use of the following result from Lang [1984, p. 331, Theorem 9.1].

Lemma 2.2. *Let K be a field and d an integer ≥ 2. Let $a \in K, a \neq 0$. Assume that for all prime numbers t dividing d, we have $a \notin K^t$, and if $4 \mid d$ then $a \notin -4K^4$. Then $X^d - a$ is irreducible in $K[X]$.*

Note that K^t denotes the set of all t-th powers of elements in K. By Lemma 2.2, the polynomial $X^{q^e} - a \in K[X]$ is irreducible. We can represent the field $E = \mathrm{GF}(p^{mq^e})$ by $K(\beta)$, where β is a root of $X^{q^e} - a$. Now, $H = \mathrm{GF}(p^{q^e})$ is a subfield of E. We have the following picture:

$$\begin{tikzcd}
& E = K(\beta) \arrow[dl, dash, "q^e"'] \arrow[dr, dash, "m"] & \\
K = F(\alpha) \arrow[dr, dash, "m"'] & & H \arrow[dl, dash, "q^e"] \\
& F &
\end{tikzcd}$$

It will suffice to find an element γ in E of degree q^e over F. We can then construct its minimum polynomial over F by computing $(X-\gamma)(X-\gamma^p)\cdots(X-\gamma^{p^{q^e-1}})$. This will be an irreducible polynomial of degree q^e over F. But finding an element in E of degree q^e over F is easy. Let T be the trace from E down to H; that is, for any x in E, $T(x) = x + x^\sigma + \cdots + x^{\sigma^{m-1}}$, where σ is the generator of the Galois group of E over H given by $x \mapsto x^{p^{q^e}}$. Then we claim that $\gamma = T(\beta)$ has degree q^e over F.

To prove this claim, suppose to the contrary that γ has degree q^t over F, where $t < e$. Then it is easy to see that γ has degree q^t over K. Now, $[K(\beta) : K(\beta^q)] = q$, and so in particular, γ lies in $K(\beta^q)$. For $i = 0, \ldots, m-1$, let $p^{iq^e} = x_i q + y_i$, where $0 < y_i < q$. It is easily seen that the y_i's are distinct, since p (which is $\equiv p^{q^e} \pmod q$) has order m mod q. This gives us an equation

$$(\beta^q)^{x_0}\beta^{y_0} + \cdots + (\beta^q)^{x_{m-1}}\beta^{y_{m-1}} - \gamma = 0.$$

Thus, β is a root of a nonzero polynomial over $K(\beta^q)$ of degree less than q. But this contradicts the fact that β has degree q over $K(\beta^q)$, and so the claim is proved.

Case 2: $q = 2, \neq p$

We want to find an irreducible polynomial of degree 2^e. In this case, as in case 1, we make use of Lemma 2.2. Since p is odd, $p \equiv \pm 1 \pmod 4$. Suppose $p \equiv 1 \pmod 4$. Then $(-1)^{(p-1)/2} = 1$, and so -1 has a square root in F. Therefore, if we have an element $a \in F$ that is not a square, then we certainly cannot have $a = -4b^4$, since $-4b^4$ is a square. Thus, the hypotheses of Lemma 2.2 are already satisfied, and so $X^{2^e} - a$ is irreducible.

Now suppose $p \equiv -1 \pmod 4$. In this case, we can quickly find an irreducible polynomial of degree 2^e deterministically. We have $(-1)^{(p-1)/2} = -1$, so -1 does not have a square root in F, and therefore

X^2+1 is irreducible. If $e=1$, we are done. Otherwise, we can proceed as follows. We construct the field $F(i)$ where $i=\sqrt{-1}$. Since -1 has a square root in $F(i)$, if we find an $a \in F(i)$ that is not a square, then $X^{2^{e-1}}-a$ is an irreducible polynomial in $F(i)[X]$ (by reasoning identical to that in the previous paragraph). Let $E=F(i,\alpha)$ where α is a root of $X^{2^{e-1}}-a$. It is easy to see that $E=F(\alpha)$ (since $[F(i,\alpha):F]=\mathrm{lcm}([F(i):F],[F(\alpha):F])$, and so it will suffice to compute the minimum polynomial of α over F, which has degree 2^e. Let σ be the automorphism on $F(i)$ defined by $i\mapsto -i$. Then the minimum polynomial for α over F is just $(X^{2^{e-1}}-a)(X^{2^{e-1}}-a^\sigma)$.

So we have reduced the problem to finding a quadratic nonresidue in $F(i)$. This is easily done as follows. $F(i)^*$ is a cyclic group of order p^2-1. Write $p^2-1=l2^k$, l odd. If we take $k-2$ successive square roots of i, we will obtain a primitive 2^k-th root of unity in $F(i)$. This must be a quadratic nonresidue; otherwise, its square root would be an element of order 2^{k+1} in $F(i)^*$, which is impossible by Lagrange's theorem.

So we have reduced the problem to taking square roots in $F(i)$. But this can easily be done using the formula

$$\sqrt{\alpha}=(1+\alpha^{(p-1)/2})^{(p-1)/2}\cdot\alpha^{(p+1)/4},$$

which holds for every quadratic residue α in $F(i)$, except if $\alpha^{(p-1)/2}=-1$, in which case $\sqrt{\alpha}=i\alpha^{(p+1)/4}$.

Case 3: $q=p$

We want to construct an irreducible polynomial of degree p^e. Our approach in this case follows Adleman and Lenstra [1986]. We will show how to inductively construct a sequence of irreducible polynomials $f_1,f_2,\ldots,f_e$ over F of degrees $p,p^2,\ldots,p^e$.

Lemma 2.3. *The polynomial X^p-X-1 is irreducible in $F[X]$. Furthermore, if K is an extension of F, and $a\in K$, and the polynomial X^p-X-a is irreducible in $K[X]$, and $E=K(\alpha)$ where α is a root of X^p-X-a, then the polynomial $X^p-X-a\alpha^{p-1}$ is irreducible in $E[X]$.*

Proof. According to Artin-Schreier theory (see, e.g., Lang [1984, p. 325, Theorem 6.4]), over any field of characteristic p, the polynomial X^p-X-a is either irreducible or splits completely. The first statement of the lemma follows immediately from this. To prove the second statement, suppose that $X^p-X-a\alpha^{p-1}$ is not irreducible in $E[X]$. Then it has a root β in E, which we can write as $\beta=\sum_{i=0}^{p-1}b_i\alpha^i$ where the b_i's are in K. Substituting this expression for β into the equation $\beta^p-\beta-a\alpha^{p-1}=0$, and replacing α^p by $\alpha+a$, we obtain an equation

$$\sum_{i=0}^{p-1}b_i^p(\alpha+a)^i-\sum_{i=0}^{p-1}b_i\alpha^i-a\alpha^{p-1}=0.$$

In the expansion of the left hand side of this equation, the coefficient of α^{p-1} is $b_{p-1}^p-b_{p-1}-a$, which is nonzero by virtue of the fact that X^p-X-a is irreducible over K. Thus, α is a root a polynomial of degree $p-1$ over K, which is impossible, and so the lemma is proved. ■

Let $f_1 = X^p - X - 1$. Suppose that we have computed f_t, $t \geq 1$. Let $K = F(\alpha)$ where α is a root of f_t. If $t = 1$, let $a = \alpha^{p-1}$; otherwise, let $a = \alpha^{2p-1} - \alpha^p$. The polynomial $X^p - X - a$ is irreducible over K. Let $E = K(\beta)$, where β is a root of $X^p - X - a$. It is easy to see that $E = F(\beta)$ (since $[F(\alpha, \beta) : F] = \mathrm{lcm}([F(\alpha) : F], [F(\beta) : F])$. Let f_{t+1} be the minimum polynomial of β over F, which we compute as $\prod_{i=0}^{p^t-1}(X^p - X - a^{p^i})$. Observe that the polynomial $X^p - X - a\beta^{p-1} = X^p - X - (\beta^{2p-1} - \beta^p)$ is irreducible over E.

Step 2: "Combining" Irreducible Polynomials of Prime Power Degree

Suppose we have constructed irreducible polynomials over F of degrees $q_1^{e_1}, \ldots, q_r^{e_r}$. We will show how to inductively construct a sequence of irreducible polynomials over F of degrees $q_1^{e_1}, q_1^{e_1}q_2^{e_2}, \ldots, q_1^{e_1} \cdots q_r^{e_r} = n$. It will suffice to solve the following problem: given two irreducible polynomials $f, g \in F[X]$ of degrees a and b, where $\gcd(a, b) = 1$, find an irreducible polynomial of degree ab.

Lemma 2.4. *Let $\alpha, \beta \in \bar{F}$, where $\bar{F}$ is the algebraic closure of F. Suppose that $[F(\alpha) : F] = a$, $[F(\beta) : F] = b$, and $\gcd(a, b) = 1$. Then $[F(\alpha, \beta) : F] = [F(\alpha + \beta) : F] = ab$.*

Proof. We have $[F(\alpha, \beta) : F] = \mathrm{lcm}([F(\alpha) : F], [F(\beta) : F]) = ab$. Any maximal proper subfield of $F(\alpha, \beta)$ (i.e., $\mathrm{GF}(p^{ab/r})$ where r is prime) must contain either α or β, but not both, and hence cannot contain $\alpha + \beta$. Therefore, $F(\alpha + \beta) = F(\alpha, \beta)$. ∎

Suppose that f and g are given as described above. Lemma 2.4 allows us to construct a tower of fields $F \subset F(\alpha) \subset F(\alpha, \beta)$ where α is a root of f and β is a root of g. The degree of the first step in the tower is a and the degree of the second is b. We can construct the minimal polynomial of $\alpha + \beta$ over F by computing $(X - (\alpha + \beta))(X - (\alpha + \beta)^p) \cdots (X - (\alpha + \beta)^{p^{ab-1}})$. This is an irreducible polynomial over F of degree ab.

Counting Operations

Our step count analysis uses fast algorithms for polynomial arithmetic based on the Fast Fourier Transform (Schönhage [1977], Aho, Hopcroft and Ullman [1974]). These algorithms allow us to multiply and perform the division algorithm on polynomials of degree d over a field K using $O(d^{1+\epsilon})$ operations in K. Raising a field element to the p-th power is done using the method of repeated squaring. The following is a breakdown of the complexity of our algorithm in terms of operations in F:

Step 1	Case 1	$O((\log p)(mq^e)^{2+\epsilon})$
	Case 2	$O(2^e + (\log p)^2)$
	Case 3	$O((p^{2e-1})^{1+\epsilon})$
Step 2		$O((\log p)n^{2+\epsilon})$

3. Reduction to Factoring

In this section, we prove

Theorem 3.1. *The problem of constructing an irreducible polynomial over F of degree n can be deterministically reduced in time bounded by a polynomial in n and $\log p$ to the problem of factoring polynomials over F.*

Let q be a prime, $q \mid n, q \neq p$. Let m be the order of p mod q. By Theorem 2.1, it will suffice to find an irreducible polynomial f of degree m, and a q-th nonresidue in $F(\alpha)$ where α is a root of f.

The basic idea is to factor the cyclotomic polynomial $\Phi_q = X^{q-1} + \cdots + 1$, obtaining an irreducible polynomial of degree m. This gives us $\mathrm{GF}(p^m)$ and a primitive q-th root of unity ξ in $\mathrm{GF}(p^m)$. Now, $\mathrm{GF}(p^m)^*$ is a cyclic group of order $p^m - 1$. Write $p^m - 1 = lq^k$ where $\gcd(l, q) = 1$. If we take $k-1$ successive q-th roots of ξ, we obtain a primitive q^k-th root of unity in $\mathrm{GF}(p^m)$. This must be a q-th nonresidue; otherwise, its q-th root would be an element of order q^{k+1} in $\mathrm{GF}(p^m)^*$, which is impossible by Lagrange's theorem. So we have reduced the problem to finding roots of polynomials of the form $X^q - c$ over $\mathrm{GF}(p^m)$. Berlekamp [1970] gives a reduction from factoring in $\mathrm{GF}(p^m)[X]$ to factoring in $\mathrm{GF}(p)[X]$. We give an explicit construction, tailoring Berlekamp's reduction to our particular application.

We inductively define a sequence of irreducible polynomials $f^{(1)}, \ldots, f^{(k)}$ in $F[X]$ of degree m where the roots of $f^{(i)}$ are primitive q^i-th roots of unity. We define $f^{(1)}$ to be any irreducible factor of Φ_q. It is clear that the roots of $f^{(1)}$ are primitive q-th roots of unity. For $i = 2, \ldots, k$, we define $f^{(i)}$ to be any irreducible factor of $f^{(i-1)}(X^q)$. Since the roots of $f^{(i-1)}$ are primitive q^{i-1}-th roots of unity, the roots of $f^{(i)}$ must be primitive q^i-th roots of unity.

Computing the sequence $f^{(1)}, \ldots, f^{(k)}$ requires us to factor one polynomial of degree $q-1$ and $k-1 < m \log p$ polynomials of degree mq. Each of these polynomials is the product of distinct irreducible polynomials of degree m. We then put $f = f^{(k)}$. Any root α of f is a q-th nonresidue in $F(\alpha)$. This completes the proof of Theorem 3.1.

Berlekamp's deterministic factoring algorithm runs in time bounded by p times a polynomial in the degree of the polynomial to be factored and $\log p$. Therefore, Theorem 3.1 implies that we can deterministically construct an irreducible polynomial over F of degree n in time bounded by p times a polynomial in n and $\log p$.

Improvements to Berlekamp's factoring algorithm described in Shoup [1988] allow us to extract an irreducible factor of a polynomial over F that is the product of k distinct irreducible polynomials of degree l using $O((\log p) l^{2+\epsilon} k^{1+\epsilon} + p^{1/2} (\log p)^2 l^{1+\epsilon} k^{1+\epsilon})$ operations in F. Using this improved factoring algorithm and the running time bounds stated in Theorem 2.1, we obtain

Theorem 3.2. *We can deterministically construct an irreducible polynomial over F of degree n with $O(p^{1/2} (\log p)^3 n^{3+\epsilon} + (\log p)^2 n^{4+\epsilon})$ operations in F.*

4. Irreducible Polynomials over Extension Fields

In this section, we prove

Theorem 4.1. *Given an extension K over F of degree d, we can construct an irreducible polynomial over K of degree n deterministically with $O(p^{1/2}(\log p)^3 n^{3+\epsilon} + (\log p)^2 n^{4+\epsilon} + (\log p) n^{4+\epsilon} d^{2+\epsilon})$ operations in F.*

The hypothesis of this theorem means that $K = F(\theta)$ where θ is a root of a given irreducible polynomial over F of degree d. The algorithm described in sections 2 and 3 could be adapted to this situation in a fairly straightforward manner. However, we will describe a slightly more complicated, but more efficient, algorithm.

Implicit in our algorithm is a reduction to the problem of factoring polynomials over F via the problem of constructing, for each prime $q \mid n, q \neq p$, the splitting field of $X^q - 1$ over F, along with a q-th nonresidue in this field, or just a primitive q-th root of unity if q also happens to divide d.

A straightforward implementation of our algorithm, making use of FFT polynomial arithmetic and the polynomial factoring algorithm in Shoup [1988], will achieve the stated running time bound. The details are left to the reader.

We now describe our algorithm. As in section 2, it will suffice to construct irreducible polynomials over K of prime power degree q^e, and then combine these to obtain an irreducible polynomial over K of degree n. We consider two possibilities: either q does not divide d, or it does.

In the first case, it will suffice to construct an irreducible polynomial over F of degree q^e, for this polynomial will remain irreducible over the larger field K. The algorithm in sections 2 and 3 can be used for this.

In the second case, let $d = q^k l$ where $\gcd(q, l) = 1$. It will then suffice to find a polynomial of degree q^e over $F(\vartheta)$, where ϑ is an element in K of degree q^k over F, for this polynomial will remain irreducible over K. To facilitate efficient computation in $F(\vartheta)$, we construct the minimum polynomial of ϑ over F by computing $(X - \vartheta)(X - \vartheta^p) \cdots (X - \vartheta^{p^{q^k-1}})$. We can find such an element ϑ quickly in the following way. Construct the minimum polynomial of θ over $\mathrm{GF}(p^{q^k})$ by computing $(X - \theta)(X - \theta^\sigma) \cdots (X - \theta^{\sigma^{l-1}})$, where σ generates the Galois group of K over $\mathrm{GF}(p^{q^k})$. Suppose this polynomial is $\vartheta_0 + \vartheta_1 X + \cdots + \vartheta_{l-1} X^{l-1} + X^l$. Then it is easy to see that $[F(\vartheta_0, \ldots, \vartheta_{l-1}) : F] = q^k$, and so one of the ϑ_i's must have degree q^k over F. We can examine each ϑ_i until we find one such that $\vartheta_i^{p^{q^{k-1}}} \neq \vartheta_i$. Now let $\vartheta = \vartheta_i$. This has degree q^k over F.

To construct an irreducible polynomial of degree q^e over $F(\vartheta)$, as in section 2, we break the problem into three cases: (1) $q \neq 2, \neq p$, (2) $q = 2, \neq p$, and (3) $q = p$.

Case 1: $q \neq 2, \neq p$

We assume that we have the field $F(\xi)$, where ξ is a primitive q-th root of unity, which we can obtain by factoring the q-th cyclotomic polynomial. Let $m = [F(\xi) : F]$, i.e., m is the order of p mod q. Since m and q are relatively prime, we can construct the tower of fields $F \subset F(\vartheta) \subset F(\vartheta, \xi)$ where the degree of the first step in the tower is q^k and the degree of the second is m.

We proceed to find a q-th nonresidue a in $F(\vartheta, \xi)$ as follows. Let L be the subfield $\mathrm{GF}(p^{mq^{k-1}})$ of

$F(\vartheta, \xi)$, and let σ generate the Galois group of $F(\vartheta, \xi)$ over L. We compute the Lagrange resolvents

$$(\vartheta^i) + \xi(\vartheta^i)^\sigma + \cdots + \xi^{q-1}(\vartheta^i)^{\sigma^{q-1}}$$

for $i = 1, \ldots, q-1$. One can show that one of these resolvents, call it a, must be nonzero, and that a^q is a q-th nonresidue in L (see page 179 of van der Waerden [1970]). It follows easily from Lemma 2.2 that a is a q-th nonresidue in $F(\vartheta, \xi)$.

By Lemma 2.2, the polynomial $X^{q^e} - a$ is irreducible over $F(\vartheta, \xi)$, so if we adjoin a root β of this polynomial to $F(\vartheta, \xi)$, we obtain the tower of fields $F \subset F(\vartheta) \subset F(\vartheta, \xi) \subset F(\vartheta, \xi, \beta)$. We can now compute $\gamma = T(\beta)$ where T is the trace from $F(\vartheta, \xi, \beta)$ down to $\mathrm{GF}(p^{q^{k+e}})$. By reasoning almost identical to that in section 2, we can prove that γ has degree q^e over $F(\vartheta)$, and hence we can compute the minimum polynomial of γ over $F(\vartheta)$ to obtain an irreducible polynomial of degree q^e over $F(\vartheta)$.

Case 2: $q = 2, \neq p$

Let L be the subfield $\mathrm{GF}(p^{2^{k-1}})$ of $F(\vartheta)$, and let σ generate the Galois group of $F(\vartheta)$ over L. Compute the Lagrange resolvent $a = \vartheta - \vartheta^\sigma$. Then a^2 is a quadratic nonresidue in L. If $k > 1$ or $p \equiv 1 \pmod 4$, then a is a quadratic nonresidue in $F(\vartheta)$ and the polynomial $X^{2^e} - a$ is irreducible over $F(\vartheta)$. Otherwise, let $p^2 - 1 = 2^s t$, and take $s-2$ successive square roots of a in $F(\vartheta)$ using the formula in section 2, obtaining a 2^{s-2}-th root b of a. Then b is a quadratic nonresidue in $F(\vartheta)$, and so $X^{2^e} - b$ is irreducible over $F(\vartheta)$.

Case 3: $q = p$

As in section 2, we inductively construct a sequence of irreducible polynomials over $F(\vartheta)$ of degrees $p, p^2, \ldots, p^e$. Everything is essentially the same as in section 2, except to get this inductive process started, we need to find an element a in $F(\vartheta)$ such that $X^p - X - a$ is irreducible. A nice way to do this is as follows. Suppose the minimum polynomial of ϑ over F is $X^{p^k} + a_1 X^{p^k - 1} + \cdots + a_{p^k}$. Let i be the least positive integer smaller than p^k such that $i \not\equiv 0 \pmod p$ and $a_i \neq 0$. We claim that such an i exists, and that $X^p - X - \vartheta^i$ is irreducible over $F(\vartheta)$.

To prove this claim, we first observe that such an i must exist, since otherwise the minimum polynomial of ϑ over F would be a perfect p-th power. Second, one can show that the polynomial $X^p - X - a$ is irreducible over $F(\vartheta)$ if and only if $T(a) \neq 0$ where T is the trace from $F(\vartheta)$ down to F (this follows from Hilbert's Theorem 90, and the Artin-Schreier Theorem on p. 325 of Lang [1984]). But using Newton's formulas for sums of powers of the roots of a polynomial (Uspensky [1948, p. 261]), we have the following recurrence relation

$$T(\vartheta^i) + a_1 T(\vartheta^{i-1}) + \cdots + a_{i-1} T(\vartheta) + i a_i = 0 \qquad (i = 1, \ldots, p^k),$$

from which the claim now follows directly.

5. A New Randomized Algorithm

This section is devoted to a proof of

Theorem 5.1. *For any constant $0 < c < 1/4$, there exists a randomized algorithm (depending on c) with the following properties. It uses $\lceil n \log p \rceil$ random bits, halts in time polynomial in n and $\log p$, and upon termination, it either outputs an irreducible polynomial over F of degree n, or reports failure. Furthermore, the probability that it fails is no more than $1/p^{cn}$.*

Let q be a prime, $q \mid n, q \neq p$. Let m be the order of p mod q. By Theorem 2.1, it will suffice to find an irreducible polynomial f of degree m and a q-th nonresidue in $F(\alpha)$ where α is a root of f, for each such q.

We obtain an irreducible polynomial f of degree m by factoring the cyclotomic polynomial $\Phi_q = X^{q-1} + \cdots + 1$. Using $\lceil n \log p \rceil$ random bits, we can construct a list ρ of n numbers between 0 and $p-1$ with an almost-uniform distribution (see Bach and Shoup [1988, section 4] for details). Let $0 < \delta < 1$ be a constant. Algorithms in Bach and Shoup [1988] will completely factor Φ_q with failure probability $\leq 1/p^{(1-\delta)n/4}$ using n random field elements in $(n \log p)^{O(1)}$ steps. We can use our list ρ as the source of random field elements.

Having obtained f, we construct the field $K = \mathrm{GF}(p^m)$. Now we need to find a q-th nonresidue in K. We could do this by factoring more polynomials, as in section 3; however, we can proceed much more straightforwardly using

Lemma 5.2. *Let $K = \mathrm{GF}(s)$ and let $d \mid s-1$, $d \neq 1$. Let $k = \lceil (\log_d s)/2 \rceil$. Suppose $c_1, \ldots, c_k \in K$ are distinct constants. Then if $x \in K$ is chosen at random, the probability that $x + c_1, x + c_2, \ldots, x + c_k$ are all in K^d is at most*

$$\frac{(\log_d s)/2 + 2}{s^{1/2}}.$$

Proof. Let τ be the probability that $x + c_1, \ldots, x + c_k$ are all d-th powers. Consider the system of equations

$$\begin{aligned} x + c_1 &= y_1^d \\ &\vdots \\ x + c_k &= y_k^d \end{aligned} \qquad (*)$$

Let N be the number of tuples $(x, y_1, \ldots, y_k)$ satisfying $(*)$. We want to get an upper bound on N. Let χ be a character of order d on K. For fixed $a \in K$, the number of solutions to the equation $y^d = a$ is $1 + \chi(a) + \cdots + \chi^{d-1}(a)$. Therefore,

$$\begin{aligned} N &= \sum_{x \in K} \prod_{i=1}^{k} (1 + \chi(x + c_i) + \cdots + \chi^{d-1}(x + c_i)) \\ &= \sum_{0 \leq e_1, \ldots, e_k \leq d-1} \sum_{x \in K} \chi((x + c_1)^{e_1} \cdots (x + c_k)^{e_k}) \end{aligned}$$

In this last expression, the term corresponding to $e_1 = \cdots = e_k = 0$ is s. For the other terms, we can bound the magnitude of each character sum by $(k-1)s^{1/2}$ (see Schmidt [1976, p. 43, Theorem 2C′]). Since there are $d^k - 1$ such terms, we have

$$N \leq s + d^k(k-1)s^{1/2}.$$

Dividing this by d^k, we get a bound on the number of $x \in K$ for which there exist nonzero $y_1, \ldots, y_k$ satisfying $(*)$. Divide again by s to get the probability τ' that $x + c_1, \ldots, x + c_k$ are all nonzero d-th powers. So we have $\tau' \leq 1/d^k + (k-1)/s^{1/2}$. Since $\tau \leq k/s + \tau'$, we have $\tau \leq k/s + 1/d^k + (k-1)/s^{1/2}$. Plugging in $k = \lceil(\log_d s)/2\rceil$, and observing that $k \leq s^{1/2}$, gives the desired result. ■

Let $s = p^m$. Then using m random elements of F we can construct a random element of K. Using this random element, we can find a q-th nonresidue with failure probability $\leq (((\log_q s)/2+2)^2/s)^{1/2}$. There is constant M (that depends on δ) such that for $s > M$, we have $((\log_q s)/2+2)^2 < s^\delta$. Therefore, if $s \leq M$, we can find a q-th nonresidue by brute force search; otherwise, we can find a q-th nonresidue with failure probability $\leq 1/p^{(1-\delta)m/2}$.

Let $u = \lfloor n/m \rfloor$. Using ρ, we can perform u independent searches for a q-th nonresidue, obtaining a failure probability bound of $1/p^{(1-\delta)mu/2} \leq 1/p^{(1-\delta)n/4}$, this last inequality following from the fact that $mu > n/2$.

We now consider the failure probability for constructing an irreducible polynomial of degree n. We can reuse ρ for each of the randomized steps, of which there are at most $2\log n$ (two for each q). So the failure probability is no more than $2\log n/p^{(1-\delta)n/4}$. For sufficiently large p^n, this is no more than $1/p^{(1-\delta)^2 n/4}$. For small p^n we can use brute force search. Now choose δ so that $(1-\delta)^2/4$ is smaller than the given value of c. This proves the theorem.

Acknowledgments

Thanks to Harold Niederreiter for pointing out Varshamov's work, and to Joachim von zur Gathen for pointing out Evdokimov's work. Thanks also to the referee for many improvements to the original version of this paper, especially the method for constructing an element of degree q^e in Section 2, Case 1. Finally, thanks to Eric Bach for many encouraging and helpful discussions.

References

L. Adleman and H. Lenstra [1986]. "Finding irreducible polynomials over finite fields," in *Proc. 18th Annual ACM Symp. on Theory of Computing*, pp. 350-355.

A. Aho, J. Hopcroft and J. Ullman [1974]. *The Design and Analysis of Computer Algorithms,* Addison-Wesley.

E. Bach [1987]. "Realistic analysis of some randomized algorithms," in *Proc. 19th Annual ACM Symp. on Theory of Computing*, pp. 453-461.

E. Bach and V. Shoup [1988]. "Factoring polynomials using fewer random bits," Computer Sciences Technical Report No. 757, University of Wisconsin–Madison.

E. Berlekamp [1968]. *Algebraic Coding Theory,* McGraw-Hill.

E. Berlekamp [1970]. "Factoring polynomials over large finite fields," *Mathematics of Computation*, vol. 24, pp. 713-735.

P. Camion [1983]. "Improving an algorithm for factoring polynomials over a finite field and constructing large irreducible polynomials," *IEEE Transactions on Information Theory,* vol. 29, no. 3, pp. 378-385.

B. Chor and R. Rivest [1984]. "A knapsack type public key cryptosystem based on arithmetic in finite fields," in *Advances in Cryptology: Proceedings of Crypto 84*, Springer-Verlag Lecture Notes in Computer Science No. 144, pp. 54-65.

W. Eberly [1984]. "Very fast parallel matrix and polynomial arithmetic," in *Proc. 25th Annual Symp. on Foundations of Computer Science*, pp. 21-30.

S. Evdokimov [1986]. "Efficient factorization of polynomials over finite fields and generalized Riemann hypothesis," preprint, Leningrad Institute for Informatics and Automatization, USSR Academy of Sciences.

J. von zur Gathen [1986]. "Irreducible polynomials over finite fields," Computer Sciences Technical Report No. 188/86, University of Toronto.

J. von zur Gathen [1987]. "Factoring polynomials and primitive elements for special primes," *Theoretical Computer Science,* vol. 52, pp. 77-89.

J. von zur Gathen and E. Kaltofen [1985]. "Factorization of multivariate polynomials over finite fields," *Mathematics of Computation,* vol. 45, no. 171, pp. 251-261.

M. Huang [1985]. "Riemann Hypothesis and finding roots over finite fields," in *Proc. 17th Annual ACM Symp. on Theory of Computing*, pp. 121-130.

H. Karloff and P. Raghaven [1988]. "Randomized algorithms and pseudorandom numbers," in *Proc. 20th Annual ACM Symp. on Theory of Computing*, pp. 310-321.

D. Krizanc, D. Peleg and E. Upfal [1988]. "A time-randomness tradeoff for oblivious routing," in *Proc. 20th Annual ACM Symp. on Theory of Computing*, pp. 93-102.

J. Lagarias, H. Montgomery and A. Odlyzko [1979]. "A bound for the least prime ideal in the Chebotarev density theorem," *Inv. Math.*, Vol. 54, pp. 271-296.

S. Lang [1984]. *Algebra (2nd edition),* Addison-Wesley.

M. Rabin [1980]. "Probabilistic algorithms in finite fields," *SIAM Journal on Computing,* vol. 9, no. 2, pp. 273-280.

W. Schmidt [1976]. *Equations over Finite Fields,* Springer-Verlag Lecture Notes in Mathematics No. 536.

A. Schönhage [1977]. "Schnelle Multiplikation von Polynomen über Körpern der Charakteristik 2," *Acta Informatica,* vol. 7, pp. 395-398.

V. Shoup [1987]. "Finding witnesses using fewer random bits," Computer Sciences Technical Report No. 725, University of Wisconsin–Madison.

V. Shoup [1988]. "On the deterministic complexity of factoring polynomials over finite fields," Computer Sciences Technical Report No. 782, University of Wisconsin–Madison.

J. Uspensky [1948]. *Theory of Equations,* McGraw-Hill.

R. Varshamov [1984]. "A general method of synthesizing irreducible polynomials over Galois fields," *Soviet Mathematics Doklady,* vol. 29, no. 2, pp. 334-336.

B. van der Waerden [1970]. *Algebra, Volume 1 (7th edition),* Ungar.