New Algorithms for Finding Irreducible Polynomials over Finite Fields

by

Victor Shoup

Computer Sciences Technical Report #763

April 1988

New Algorithms for Finding Irreducible Polynomials over Finite Fields

Victor Shoup

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

April 1, 1988

Abstract. Let p be a prime number, F be the finite field with p elements, and n be a positive integer. We present new algorithms for finding irreducible polynomials in $F[X]$ of degree n. We show that in time polynomial in n and $\log p$ we can reduce the problem of finding an irreducible polynomial over F of degree n to the problem of factoring polynomials over F. Combining this with Berlekamp's deterministic factoring algorithm, we obtain a deterministic algorithm for finding irreducible polynomials that runs in time polynomial in n and p. This is useful when p is small. Unlike earlier results in this area, ours does not rely on any unproven hypotheses, such as the Extended Riemann Hypothesis. We also present a new randomized algorithm for finding irreducible polynomials that runs in time polynomial in n and $\log p$ and makes particularly efficient use of randomness. It uses $n \log p$ random bits, and fails with probability less than $1/p^{\alpha n}$ where α is a constant between 0 and 1/4. This result is interesting in a setting where random bits are viewed as a scarce resource.

This research was sponsored by the National Science Foundation, via grants DCR-8504485 and DCR-8552596.

1. Introduction

Let p be a prime number, F the finite field GF(p), and n a positive integer. Consider the problem of finding an irreducible polynomial in $F[X]$ of degree n. Irreducible polynomials in $F[X]$ are used to implement arithmetic in field extensions of F. They have applications in coding theory, cryptography, and complexity. Rabin has given a randomized algorithm for finding an irreducible polynomial over F of degree n that runs in time polynomial in n and $\log p$ [Rabin]. Adleman and Lenstra have given a deterministic algorithm that runs in time polynomial in n and $\log p$ assuming the Extended Riemann Hypothesis [Adleman/Lenstra]. Von zur Gathen has also given several deterministic algorithms that run quickly assuming some unproven conjectures [von zur Gathen].

In this paper, we show that in time polynomial in n and $\log p$ we can reduce the problem of finding an irreducible polynomial over F of degree n to the problem of factoring polynomials over F. Combining this with Berlekamp's deterministic factoring algorithm [Berlekamp], we obtain a new algorithm that runs in in time polynomial in n and p. Our algorithm is completely deterministic and does not rely on any unproven hypotheses. It is useful in the important special case where p is small. We also give a new randomized algorithm that makes particularly efficient use of randomness, failing with probability exponentially small in the number of random bits used.

In section 2, we shall prove

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 in time polynomial in n and $\log p$.

The splitting field K of $X^q - 1$ is the smallest extension of F containing a primitive q-th root of unity. This is just GF(p^m) where m is the order of p mod q. The hypothesis of theorem 2.1 means that we are given an irreducible polynomial f over F of degree m and that $K = F(\alpha)$ where α is a root of f. Note that all of the irreducible factors of the cyclotomic polynomial $\Phi_q = X^{q-1} + \cdots + 1$ are of degree m.

The problems of factoring Φ_q and finding q-th nonresidues in GF(p^m) are discussed in [Huang]. Huang's analysis, however, assumes the Extended Riemann Hypothesis.

In section 3 we prove

Theorem 3.1. Given an oracle for factoring polynomials over F, we can construct an irreducible polynomial over F of degree n in time polynomial in n and $\log p$.

Using Berlekamp's deterministic factoring algorithm, we immediately obtain

Corollary 3.2. We can construct an irreducible polynomial over F of degree n deterministically in time polynomial in n and p.

In section 4, we present a new randomized algorithm for finding irreducible polynomials. The problem that originally motivated this research was to find a randomized algorithm for finding irreducible polynomials that used fewer random bits than Rabin's algorithm. This problem is interesting in a setting where random bits are viewed as a scarce resource. In this setting, a "random bit efficient" algorithm fails with probability exponentially small in the number of random bits used. That is, for some constant α, the failure probability is no more than $2^{-\alpha b}$ where b random bits are used. See [Shoup, Bach, Bach/Shoup] for other work along these lines.

Rabin's algorithm uses about $n \log p$ random bits to generate a monic polynomial of degree n over F, and then tests it for irreducibility. The probability of success is about $1/n$. Obviously, Rabin's algorithm is not random bit efficient.

We present a new, random bit efficient algorithm for finding irreducible polynomials. We shall prove

Theorem 4.1. For any constant $0 < \alpha < 1/4$, there exists a randomized algorithm (depending on α) with the following properties. It uses about $n \log p$ 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 $1/p^{\alpha n}$.

2. Reduction to Constructing Cyclotomic Extensions and Finding Nonresidues

Let $F = \mathrm{GF}(p)$. We want to construct an irreducible polynomial of degree n over F. 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 in time polynomial in n and $\log p$.

The splitting field K of $X^q - 1$ is the smallest extension of F containing a primitive q-th root of unity. This is just $\mathrm{GF}(p^m)$ where m is the order of p mod q. In particular, $m \mid q - 1$. Since $q \mid p^m - 1$, the set of q-th residues form a proper subgroup of K^*. We assume that we are given an irreducible polynomial f over F of degree m and that $K = F(\alpha)$ where α is a root of f.

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

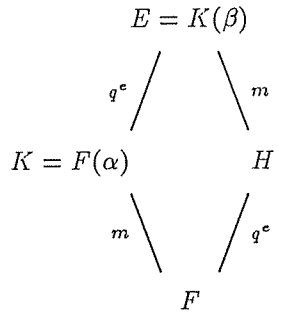
Let $1 \leq i \leq r$ be fixed, and let $q = q_i, e = e_i$. We want to construct an irreducible polynomial in $F[X]$ of degree q^e. We break the problem down into three cases: (1) $q \neq 2, \neq p$, (2) $q = 2, \neq p$, and (3) $q = p$.

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

We will make use of the following very general theorem from [Lang, p. 331, theorem 9.1].

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

Let m be the order of p mod q. We assume that we have an irreducible polynomial f of degree m. Let $K = F(\alpha)$ where α is a root of f. Then $\{1, \alpha, \ldots, \alpha^{m-1}\}$ is a basis for K as a vector space over F. We are also given $a \in K$ that is a q-th nonresidue. 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 $X^{q^e} - a$. Then $\{1, \beta, \ldots, \beta^{q^e-1}\}$ is a basis for E as a vector space over K. Therefore, $B = \{\alpha^i \beta^j : i = 0, \ldots, m-1; j = 0, \ldots, q^e - 1\}$ is is a basis for E as a vector space over F. Now, $H = \mathrm{GF}(p^{q^e})$ is a subfield of E. We have the following picture:



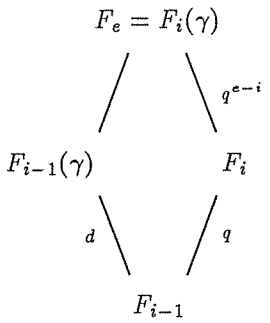
We will make use of the trace map. The trace T from $\mathrm{GF}(s^d)$ to $\mathrm{GF}(s)$ is given by $T(x) = x + x^s + x^{s^2} + \cdots + x^{s^{d-1}}$. The main fact we need to know about T is that it is a $\mathrm{GF}(s)$-linear map from $\mathrm{GF}(s^d)$ onto $\mathrm{GF}(s)$ (see [Ireland/Rosen, p. 158, proposition 11.2.1]).

Let T be the trace from E to H. If we apply T to the basis set B, we get a set $T(B)$ that spans H as a vector space over F. In particular, H is generated as a field by $T(B)$, i.e. $H = F(T(B))$. We claim that there is a single element $\gamma \in T(B)$ such that $H = F(\gamma)$. To prove this, observe that the intermediate fields between H and F form a tower $F = F_0 \subset F_1 \subset \cdots \subset F_{e-1} \subset F_e = H$, where $[F_{i+1} : F_i] = q$. Now, since $H = F(T(B))$, it is clear that $H = F_{e-1}(T(B))$, and so if we pick γ to be any element in $T(B)$ that is not in F_{e-1}, then we must have $H = F_{e-1}(\gamma)$. The following lemma establishes the claim.

Lemma 2.3. Let F_0 be a finite field. Consider a tower of fields $F_0 \subset F_1 \subset \cdots \subset F_e$ where $[F_{i+1} : F_i] = q$ and q is prime. Suppose that for some $0 \leq i < e$ and $\gamma \in F_e$, we have $F_e = F_i(\gamma)$. Then $F_e = F_0(\gamma)$.

Proof. If $i = 0$, the assertion is trivial. Assume $i > 0$. Let $d = [F_{i-1}(\gamma) : F_{i-1}]$. Consider the following

diagram.



Now, we know that $d = q^{e-i}$ or $d = q^{e-i+1}$ [Lang p. 305, corollary 1.13]. In either case, $F_{i-1}(\gamma)$ must contain F_i as a subfield, by the uniqueness of intermediate fields of a given degree. But then $F_e \supset F_{i-1}(\gamma) \supset F_i(\gamma) = F_e$. Therefore, $F_e = F_{i-1}(\gamma)$. The proof is finished by induction. ■

So we now have a primitive element γ for H over F. The minimum polynomial g for γ over F is of degree q^e. We can compute g by multiplying together conjugates, obtaining $g = (X - \gamma)(X - \gamma^p) \cdots (X - \gamma^{p^{q^e-1}})$.

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. Let $i = \sqrt{-1}$, and represent $\mathrm{GF}(p^2)$ as $K = F(i)$. Since -1 has a square root in K, if we find an $a \in K$ that is not a square, then $X^{2^{e-1}} - a$ is an irreducible polynomial in $K[X]$ (by reasoning identical to that in the previous paragraph). Let α be a root of $X^{2^{e-1}} - a$ and $E = K(\alpha)$. By lemma 2.3, $E = F(\alpha)$, and so it will suffice to compute the minimum polynomial of α over K, 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 are left to solve equations of the form $(x + yi)^2 = a + bi$ where $b \neq 0$. Expanding the left hand side and equating coefficients, we have a system of equations

$$x^2 - y^2 = a \qquad 2xy = b.$$

We must have $x \neq 0$, since $x = 0$ implies $b = 0$. Substitute $y = b/(2x)$ into the first equation, set $z = x^2$, and we obtain $z^2 - az - \frac{b^2}{4} = 0$. To solve this we need to compute the $\sqrt{a^2 + b^2}$, and then compute $x = \sqrt{z}$.

So we have reduced the problem to finding square roots in F. But since $p \equiv -1 \pmod 4$, this is easy to do. The group of quadratic residues in F has order $(p-1)/2$; therefore, if u is a quadratic residue, $\left(u^{(p+1)/4}\right)^2 = u^{(p+1)/2} = u$. So we can compute $\sqrt{u}$ directly as $u^{(p+1)/4}$.

Case 3: $q = p$

We want to construct an irreducible polynomial of degree p^e. In this case, we don't need any randomness at all. We make use of the following theorem from [Lang, p. 325, theorem 6.4].

Lemma 2.4. Let k be a field of characteristic p. Given $a \in k$, the polynomial $X^p - X - a$ either splits into linear factors in k or is irreducible over k.

Suppose, inductively, that we have an irreducible polynomial f of degree p^e. We show how to construct an irreducible polynomial of degree p^{e+1}. We can represent the field $K = \mathrm{GF}(p^{p^e})$ by $F(\alpha)$ where α is a root of f. Then $\{1, \alpha, \ldots, \alpha^{p^e-1}\}$ is a basis for K as a vector space over F. Our first task is to find an irreducible polynomial in $K[X]$ of degree p.

For any $a \in K$, lemma 2.4 implies that if $X^p - X - a$ does not have a root in K, it is irreducible. Suppose that $X^p - X - a$ has a root b in K. Let T be the trace from K to F. Then we have $T(a) = T(b^p - b) = 0$. But, since T is an F-linear map from K onto F, it must map one of the basis elements $1, \alpha, \ldots, \alpha^{p^e-1}$ to something other than zero. Thus, we can easily find an a such that $T(a) \neq 0$, and hence $X^p - X - a$ irreducible.

Suppose we have $X^p - X - a$ irreducible. Let β be a root and consider the extension $E = K(\beta)$. By lemma 2.3, $E = F(\beta)$. The minimum polynomial for β over F is of degree p^{e+1}, and can be computed by multiplying together conjugate factors

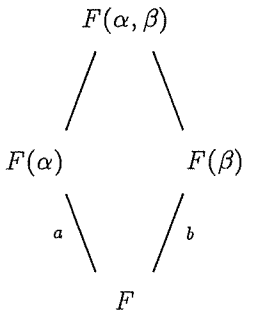
$$\prod_{i=0}^{p^e-1} (X^p - X - a^{p^i}).$$

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

Suppose we have constructed irreducible polynomials $f_1, \ldots, f_r \in F[X]$ of degrees $q_1^{e_1}, \ldots, q_r^{e_r}$. We show how to deterministically construct an irreducible polynomial in $F[X]$ of degree $n = q_1^{e_1} \cdots q_r^{e_r}$. 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.

Suppose f and g are given as described above. Let α and β be roots of f and g, respectively, in the algebraic closure $\bar{F}$ of F. Consider the fields $F(\alpha)$, $F(\beta)$, and the compositum $F(\alpha, \beta)$. We have the following

picture.

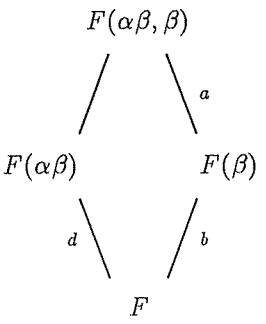


Let $d = [F(\alpha, \beta) : F]$. Since $a \mid d$, $b \mid d$, and $\gcd(a, b) = 1$, we must have $ab \mid d$. Therefore, $d = ab$. It follows that β has degree b over $F(\alpha)$ and α has degree a over $F(\beta)$. Therefore, f remains irreducible over $F(\beta)$ and g remains irreducible over $F(\alpha)$.

Now we move from the abstract to the concrete. Using f, we construct the field $F[X]/(f) = F(\alpha)$, where α be a root of f. Since g remains irreducible over $F(\alpha)$, we can construct the field $F(\alpha, \beta) = F(\alpha)[X]/(g)$, where β is a root of g. Thus, we no longer view α and β as elements of $\bar{F}$, but rather, they are elements of these concrete fields.

Lemma 2.5. $F(\alpha, \beta) = F(\alpha\beta)$.

Proof. First note that $\alpha\beta$ has degree a over $F(\beta)$. Indeed, if we have an equation $0 = (\alpha\beta)^t + c_{t-1}(\beta)(\alpha\beta)^{t-1} + \cdots + c_0(\beta)$, then since α has degree a over $F(\beta)$, we must have $t \geq a$. Similarly, $\alpha\beta$ has degree b over $F(\alpha)$. Let $d = [F(\alpha\beta) : F]$. Consider the following diagram.



Now, by Galois theory (see [Lang, p. 305, corollary 1.13]), $a \mid d$. Exchanging the roles of a and b, we see that $b \mid d$. Therefore, $ab \mid d$. We conclude that $d = ab$, and $F(\alpha\beta) = F(\alpha, \beta)$. ■

Once again, we compute the minimal polynomial for $\alpha\beta$ over F. This has degree ab.

3. Reduction to Factoring

Again, let $F = \mathrm{GF}(p)$ where p is prime, and let n be a positive integer. This section is devoted to a proof of

Theorem 3.1. Given an oracle for factoring polynomials over F, we can construct an irreducible polynomial over F of degree n in time polynomial in n and $\log p$.

Using Berlekamp's deterministic factoring algorithm, we immediately obtain

Corollary 3.2. We can construct an irreducible polynomial over F of degree n deterministically in time polynomial in n and p.

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] 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 proceed iteratively as follows. At the beginning of stage i, $i = 1, \ldots, k$, we have an extension $F(\xi^{(i)})$ over F of degree m where where $\xi^{(i)}$ is a primitive q^i-th root of unity, and $f^{(i)}$ is the minimal polynomial for $\xi^{(i)}$ over F. Initially, $f^{(1)}$ is an irreducible factor of Φ_q.

Stage i ($1 \leq i < k$):
$\xi^{(i)}$ is a q-th residue. Let σ be the Frobenius automorphism $x \mapsto x^p$ on $F(\xi^{(i)})$. This naturally extends to an automorphism on $F(\xi^{(i)})[X]$. Put $g = X^q - \xi^{(i)}$ and compute $h = gg^\sigma \cdots g^{\sigma^{m-1}}$. Now, $g = X^q - \xi^{(i)} = (X - \alpha_1) \cdots (X - \alpha_q)$ where the α_s's are primitive q^{i+1}-th roots of unity. So we have

$$h = gg^\sigma \cdots g^{\sigma^{m-1}} = \prod_{s=1}^{q} \prod_{t=0}^{m-1} (X - \alpha_s^{\sigma^t}) = \prod_{s=1}^{q} h_s,$$

where each h_s is the minimal polynomial for α_s over F, and has degree m. We see that h is a polynomial over F of degree qm. We then extract an irreducible factor h_s and put $f^{(i+1)} = h_s$ for the next stage.

Stage k:
$\xi^{(k)}$ is a q-th nonresidue.

4. A New Randomized Algorithm

Again, let $F = \mathrm{GF}(p)$ where p is prime, and let n be a positive integer. This section is devoted to a proof of

Theorem 4.1. For any constant $0 < \alpha < 1/4$, there exists a randomized algorithm (depending on α) with the following properties. It uses about $n \log p$ 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 $1/p^{\alpha n}$.

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.

We obtain an irreducible polynomial f of degree m by factoring Φ_q. Using about $n \log p$ random bits, we can construct a list ρ of n numbers between 0 and $p-1$ with an almost-uniform distribution (see [Bach/Shoup, section 4] for details). Let $0 < \epsilon < 1$ be a constant. Algorithms in [Bach/Shoup] will completely factor Φ_q with failure probability $\leq 1/p^{(1-\epsilon)\frac{1}{4}n}$ using n random field elements in time polynomial in n and $\log p$. 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. To do this, we make use of the following

Lemma 4.2. Let $K = \mathrm{GF}(s)$ and let $d \mid s-1$, $d \neq 1$. Let $k = \lceil \frac{1}{2} \log_d s \rceil$. 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

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

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

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

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, 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 $k = \lceil \frac{1}{2} \log_d s \rceil$, 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 $\leq ((\frac{1}{2}\log_q s + 2)^2/s)^{1/2}$. There is constant $C(\epsilon)$ such that for $s > C(\epsilon)$, we have $(\frac{1}{2}\log_q s + 2)^2 < s^\epsilon$. Therefore, if $s \leq C(\epsilon)$, we can find a q-th nonresidue brute force search; otherwise, we can find a q-th nonresidue with failure probability $\leq 1/p^{(1-\epsilon)\frac{1}{2}m}$.

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 $1/p^{(1-\epsilon)\frac{1}{2}mu} \leq 1/p^{(1-\epsilon)\frac{1}{4}n}$, this last inequality following from the fact that $mu > n/2$.

If we reuse ρ for each of the randomized steps, the failure probability for the entire algorithm will be no more than $1/p^{(1-\epsilon)\frac{1}{4}n}$ times the number of random steps. There are at most $2\log n$ random steps (2 for each q, of which there are no more than $\log n$). So the failure probability is no more than $2\log n/p^{(1-\epsilon)\frac{1}{4}n}$. For fixed δ and sufficiently large p^n, this is no more than $1/p^{(1-\delta)(1-\alpha)\frac{1}{4}n}$. For small p^n we can use brute force search. Now choose ϵ and δ so that $\frac{1}{4}(1-\epsilon)(1-\delta) \leq \alpha$. This proves theorem 4.1.

Acknowledgements

The author would like to thank Eric Bach for many encouraging and helpful discussions.

References

[Adleman/Lenstra] L. Adleman and H. Lenstra, "Finding irreducible polynomials over finite fields," *1986 STOC*, pp. 350-355.

[Bach] E. Bach, "Realistic analysis of some randomized algorithms," *1987 STOC*, pp. 453-461.

[Bach/Shoup] E. Bach and V. Shoup, "Factoring polynomials using fewer random bits," University of Wisconsin–Madison, Comp. Sci. TR #757 (March 1988).

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

[Huang] M. Huang, "Riemann Hypothesis and finding roots over finite fields," *1985 STOC*, pp. 121-130.

[Ireland/Rosen] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag (1982).

[Lang] S. Lang, *Algebra (2d ed.)*, Addison-Wesley (1984).

[Rabin] M. Rabin, "Probabilistic algorithms in finite fields," *SIAM Journal on Computing*, Vol. 9, No. 2 (May 1980), pp. 273-280.

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

[Shoup] V. Shoup, "Finding witnesses using fewer random bits," University of Wisconsin–Madison, Comp. Sci. TR #725 (Nov. 1987).

[von zur Gathen] J. von zur Gathen, "Irreducible polynomials over finite fields," University of Toronto, Comp. Sci. TR #188/86 (Feb. 1986).