AAECC 4, 263–268 (1993)

AAECC
Applicable Algebra in Engineering, Communication and Computing

Finding Irreducible and Primitive Polynomials

Igor E. Shparlinski

School of MPCE, Macquarie University, NSW 2109, Australia
E-mail: igor@macadam. mpce. mq. edu. au

Received October 17, 1991; revised version June 23, 1992

Abstract. In the paper some new fast constructions of irreducible and primitive polynomials are presented. For instance, it is shown, that for any Q large enough one can design a finite field $\mathbb{F}_q$ with $q = Q + o(Q)$ elements in polynomial time $(\log Q)^{O(1)}$.

Keywords: Algorithms in finite fields, polynomials over finite fields

I. Introduction

A very important area in theory of finite fields is designing fast algorithms for finding irreducible and primitive polynomials over finite fields. These polynomials have many applications in coding theory, cryptography, complexity theory, computer science, computational mathematics (see the books [9], [10] and the recent survey papers [3], [5], [18]).

We use the following notation: $\mathbb{F}_q$ is a finite field of q elements; $M_n(q)$, $I_n(q)$, and $G_n(q)$ are the set of all monic polynomials of degree n over $\mathbb{F}_q$, the subset of all irreducible polynomials from $M_n(q)$, and the subset of all primitive polynomials from $M_n(q)$, respectively; ε denotes any fixed positive number (the implied constants in the symbol "O" may depend on ε).

There are several classes of "explicitly given" irreducible polynomials. Unfortunately, the essential deficiency of these constructions is a very sparse sequence of degrees of generating polynomials which strongly depends on the field's characteristic p and on its size q. The classical example is the Artin–Schreier polynomial $f(x) = x^p + x + a$, where $0 < a < p$, which is irreducible over $\mathbb{F}_p$. A detailed survey of results of this type can be found in [6] and in Chap. 3 of [9].

It is very easy to construct a probabilistic polynomial-time algorithm for finding irreducible polynomials (since their density $|I_n(q)|/|M_n(q)|$ is, roughly speaking, $1/n$).

In [1], [7], [8], [13]–[15] some deterministic algorithms for finding irreducible polynomials of a given degree n were presented.

The algorithms of [8] and [13] have computing time $(np)^{O(1)}$ (in [13] only the case of p fixed was considered but, apparently, this is not essential). The currently

best deterministic unconditional algorithm proposed in [14], [15] uses

$$T = O(n^{3+\varepsilon} p^{1/2+\varepsilon} + n^{4+\varepsilon} \log^2 p) \tag{1}$$

arithmetical operations in $\mathbb{F}_p$, i.e. it is exponential with respect to the size of the input that is $(n \log p)^{O(1)}$.

On the other hand, for a large number of applications it is sufficient to find irreducible and primitive polynomials for some dense sequence of degrees n (instead of all $n \in \mathbb{N}$) or for some sequence of fields. This approach was suggested in [1], [7] for irreducible polynomials. Here we continue to develop this approach and extend it on primitive polynomials as well.

2. Irreducible Polynomials

Here we show that very simple considerations enable us to obtain an algorithm with polynomial computing time $(p \log N)^{O(1)}$ which for any $N \in \mathbb{N}$ computes an irreducible polynomial of degree $n = N + o(N)$ over $\mathbb{F}_p$.

Theorem 1. *For any $N \in \mathbb{N}$ in time $(p \log N)^{O(1)}$ one can find an irreducible polynomial $f \in I_n(p)$ of degree*

$$n = N + O(N \exp[-(\log \log N)^{1/2-\varepsilon}]). \tag{2}$$

Proof. Let us define

$$(d, p_1, p_2) = \begin{cases} (4, 3, 5), & \text{if } p = 2; \\ (4, 2, 5), & \text{if } p = 3; \\ (2, 2, 3), & \text{if } p > 3. \end{cases}$$

Then in time $(p \log n)^{O(1)}$ we choose $\psi \in G_d(p)$ and the nearest to N/d integer t of the form $t = p_1^k p_2^m$ where k and m are non-negative integers. It follows from [10], Theorem 3.35, that the polynomial $f(x) = \psi(x^t)$ of degree $n = dt$ is irreducible. The bound (2) follows from [2], Chap. 1, Sect. 2. In fact, the following statement was proved (with the help of the A.O. Gel'fond bound for linear forms in two logarithms). Let $1/2 < \vartheta < \omega < 1$ and primes p_1, p_2 be fixed, and let $M = p_1^{\alpha_1} p_2^{\alpha_2}$ where α_1, α_2 are natural numbers,

$$\alpha_1 < \frac{\vartheta \log M}{\log p_1}, \quad \alpha_2 < \frac{\vartheta \log M}{\log p_2}.$$

Define $\Delta = \exp[-(\log \log M)^{1/2-\varepsilon}]$. Then there is a divisor $t | M$ with $|\log t - \omega \log M| < \Delta$. (This is, in fact, a somewhere relaxed version of the corresponding theorem of [2]).

If we set

$$K = N/d, \quad \alpha_1 = \left[\frac{2 \log K}{3 \log p_1}\right], \quad \alpha_2 = \left[\frac{2 \log K}{3 \log p_2}\right], \quad M = p_1^{\alpha_1} p_2^{\alpha_2},$$

then $\log K = 0.75 \log M + O(1)$. Therefore, we can apply the previous statement

with $\vartheta = 2/3$, $\omega = \log K/\log M = 3/4 + o(1)$. Hence,

$$t = K\exp(\Delta) = K + O(K\Delta) = K + O(N\exp[-(\log\log N)^{1/2-\varepsilon}]),$$

and the proof is complete. ■

It seems that the bound (2) can be improved with the help of contemporary bounds for linear forms in logarithms. Probably, one can take $1-\varepsilon$ instead of $1/2-\varepsilon$ in the exponent in Theorem 1.

In a number of applications of finite fields, for example, when constructing some combinatorial designs, in coding theory, in cryptography, we must construct a finite field with the size which approximately equals a given $Q > 0$ large enough, however the field's characteristic and its degree may be arbitrary. Here we show that it can be done in polynomial time.

Theorem 2. *Let $A > 0$ be some constant. Then for any large enough Q one can construct the field $\mathbb{F}_q$ of $q = Q + O(Q\log^{-A} Q)$ elements in time $(\log Q)^{O(1)}$.*

Proof. For the construction we define

$$n = [\log Q/4A\log\log Q]$$

and let p be the nearest prime to $Q^{1/n} \sim \log^{4A} Q$. Then (see, for example, [11], Chap. 14) we have

$$p = Q^{1/n} + O(Q^{3/4n})$$

(contemporary results on the distribution of prime numbers imply a stronger bound, but it does not improve this theorem and Theorem 3 below, that uses the same considerations).

Putting $q = p^n$ we obtain

$$q = p^n = Q[1 + O(nQ^{-1/4n})] = Q + O(Q\log^{-A} Q).$$

Moreover, it follows from (1) that the field $\mathbb{F}_q$ can be constructed in time $(np)^{O(1)} = (\log Q)^{O(1)}$. ■

It is easy to show that instead of the very strong bound (1) the more simple Theorem 1 could be used (with some heavier machinery). Moreover, using this theorem we can obtain a smaller exponent of $\log Q$ in the bound of computing time.

3. Primitive Polynomials

Now we are going to consider primitive polynomials $f \in G_n(q)$, i.e. polynomials whose roots are primitive roots of $\mathbb{F}_{q^n}$ (the generators of the multiplicative group of this field).

It is essentially less known about constructing primitive polynomials in finite fields. Particularly, for testing the primitiveness of a given $f \in M_n(q)$, the factorization of $q^n - 1$ must be known. But all deterministic (and even probabilistic) integer factoring algorithms known nowadays are exponential ones (see [12]).

In the papers [16], [17] independently were presented two very similar constructions of small-sized sets $M \subseteq M_n(p)$, containing a primitive polynomial.

Moreover these sets have the size

$$|M| = (pn)^{O(1)}$$

and can be constructed in time $(pn)^{O(1)}$. For instance, in finite fields of fixed characteristic the search of a primitive polynomial can be restricted by a polynomial-sized set of polynomials. It should be noted that for a fixed p the set constructed in [17] has the size $O(n^{10})$. In [16] a slightly different construction and Iwaniec's shifted sieve method produced the set of the size $O(n^{6+\varepsilon})$. In fact, this sieve method allows to obtain the same bound for the construction of [17] (with some different choice of parameters).

More exactly, let $m = [(6+\varepsilon)\log n/\log p] + 1$ and $\alpha \in \mathbb{F}_{p^{mn}}$ be a root of a polynomial $f \in I_{nm}(p)$, i.e.

$$\mathbb{F}_p(\alpha) = \mathbb{F}_{p^{mn}}$$

(it follows from (1) that we can find such polynomials in time $(pn)^{O(1)}$). Then the set

$$\mathfrak{M} = \{\mu = (\alpha + \lambda)^{(p^{mn}-1)/(p^n-1)} \mid \lambda \in \mathbb{F}_{p^m}\} \subseteq \mathbb{F}_{p^n}, \tag{3}$$

can be constructed in time $(np)^{O(1)}$, has the size $|\mathfrak{M}| \leqq pn^{6+\varepsilon}$ and for $n > n_0$, where n_0 is some constant depending only on ε, contains a primitive root of $\mathbb{F}_{p^n}$ (see [16], [17]).

Of course one can find a primitive polynomial among the minimal polynomials over $\mathbb{F}_p$ of elements of $\mathfrak{M}$.

From this result, an analogy of Theorem 2 for primitive roots can be proved, i.e. one can construct a field with the size approximately equal to a given Q and a primitive root of this field but in time $O(Q^{\varepsilon})$ only (instead of polynomial time in Theorem 2).

Theorem 3. *For sufficiently large Q one can construct the field $\mathbb{F}_q$ of $q = Q + O(Q\exp[-(\log Q)^{1-\varepsilon}])$ elements and its primitive roots $\vartheta \in \mathbb{F}_q$ in time* $\exp[O(\log Q/\log\log\log Q)]$.

Proof. Put

$$N = [\exp((\log\log Q)^{1/2})]$$

and $s = q_1 \cdots q_\omega$, where $q_1, \ldots, q_\omega$ are all primes not exceeding $0.4\log N$. Let $n = s[N/s]$ and p be the nearest to $Q^{1/n}$ prime number. Then (see [11], Chap. 14)

$$p = Q^{1/n} + O(Q^{3/4n})$$

(see the remark in the proof of Theorem 2). For large enough Q, the Prime Number Theorem yields $N^{1/3} \leqq s \leqq N^{1/2}$. Therefore $n = N + O(N^{1/2})$. Set $q = p^n$, then

$$q = Q[1 + O(nQ^{-1/4n})] = Q + O(Q\exp[-(\log Q)^{1-\varepsilon}]).$$

All prime divisors of $q - 1 = p^n - 1$ do not exceed $(p+1)^{\varphi(n)}$. From the definition of s we obtain

$$\varphi(n) \leqq \varphi(s)n/S = O(n/\log\log s) = O(n/\log\log n).$$

Hence, all prime divisors of $q-1$ can be found in time $\exp[O(\log Q/\log\log\log Q)]$. The field $\mathbb{F}_q$ and the set $\mathfrak{M} \subseteq \mathbb{F}_q$, defined in (3), can be constructed in time $(np)^{O(1)}$. The search of a primitive root among all elements of $\mathfrak{M}$ can be done in time $(np)^{O(1)}$

also (as soon the factorization of $q-1$ is known). Taking into account that

$$(np)^{O(1)} = \exp[O(\log Q/\log\log\log Q)],$$

we get the result. ■

If the field's characteristic is given then considerations, similar to those that were used in the proofs of Theorem 2 and Theorem 3, allow to find primitive roots in subexponential time for a sufficiently dense sequence of the degrees of extensions of the field $\mathbb{F}_p$.

Theorem 4. *There is some absolute constant $C>0$ that for any $N\in\mathbb{N}$ an integer $n=N+O(N^{\varepsilon})$ and a primitive root $\vartheta\in\mathbb{F}_{p^n}$ can be found in time $\rho^{cN/\log\log N}$.*

Proof. For $N\in\mathbb{N}$ large enough we put $r=[10\log N/\log p]+1$, $s=q_1\cdots q_\omega$ where $q_1,\ldots,q_\omega$ are the prime numbers not exceeding $0.5\varepsilon\log N$, and $n=rs[N/rs]$. It is clear that $n=N+O(N^{\varepsilon})$. Let $\alpha\in\mathbb{F}_{p^n}$ be a root of a polynomial $f\in I_n(p)$. Define

$$\mathfrak{N}=\{\nu\,|\,\nu=(\alpha+\lambda);\ \lambda\in\mathbb{F}_{p^r}\}.$$

It is easy to see that $\mathfrak{N}$ contains less then pN^{10} elements and can be constructed in time $(pN)^{O(1)}$. Besides, it may be shown that $\mathfrak{N}$ contains a primitive root of $\mathbb{F}_{p^n}$ (completely analogously to the proof of corresponding results for $\mathfrak{M}$ from [16] or [17]).

It is clear that every prime divisor of p^n-1 does not exceed $(p+1)^{\varphi(n)}$. In the view of the choice of the parameters s and n we obtain $\varphi(n)\leqq\varphi(s)n/s=O(n/\log\log s)=O(N/\log\log N)$. Therefore, we have the desired result.

References

1. Adleman, L. M., Lenstra, H. W.: Finding irreducible polynomials over finite fields. Proc. 18 ACM Symp. Theory Comp. 350–355 (1986)
2. Babaev, G.: The distribution of integer points over algebraic surfaces. Dushanbe, 1966 (in Russian)
3. Bach, E.: Number-theoretic algorithms. Ann Rev Comp. Sci. **4**, 119–172 (1990)
4. Chistov, A. L.: The construction of a finite field in polynomial time. Proc. 7 All-Union Conf. on Math. Logic. Novosibirsk, 1984, p. 196 (in Russian)
5. Cohen, S. D.: Primitive elements and polynomials: existence results. Preprint 91/65, Glasgow University, pp. 1–12 (1991)
6. Cohen, S. D.: The explicit construction of irreducible polynomials over finite fields. Preprint 91/71, Glasgow University, pp. 1–7 (1991)
7. Von zur Gathen, J.: Irreducible polynomials over finite fields. Lecture Notes in Comp. Sci. vol. 241, pp. 252–262. Berlin, Heidelberg, New York: Springer 1986
8. Evdokimov, S. A.: Factoring a solvable polynomial over a finite field and the Generalized Riemann Hypothesis. Zapiski Nauchn. Semin. Leningr. Otdel. Matem. Inst. Acad. Sci. USSR, 1989, vol. 176, pp. 104–117 (in Russian)
9. Lidl, R., Niederreiter, H.: Finite fields. New York: Addison-Wesley 1983
10. MacWilliams F. J., Sloane, N. J. A.: The theory of error-correcting codes. Amsterdam: North-Holland 1977
11. Montgomery, H. L.: Topics in multiplicative number theory. Lecture Notes in Mathematics, vol. 227 Berlin, Heidelberg, New York: Springer 1971
12. Pomerance, C.: Factoring. Cryptology and Computational Number Theory. Proc. Symp. Appl. Math. **42**, 27–47 (1990)

13. Semaev, I. I.: Construction of irreducible polynomials over finite fields with linearly independent roots. Matem. Sbornik **135**(4), 520–532 (in Russian) (1988)
14. Shoup, V.: Removing randomness from computational number theory. Computer Science Technical Report no. 865 University Wisconsin Madison, 1989
15. Shoup, V.: New algorithms for finding irreducible polynomials over finite fields. Math. Comp. **54**(189), 435–447 (1990)
16. Shoup, V.: Searching for primitive roots in finite fields. Proc. 22 ACM Symp. on Theory of Comp. 546–554 (1990)
17. Shparlinski, I. E.: On primitive elements in finite fields and on elliptic curves. Matem. Sbornik **181**(9), 1196–1206 (in Russian) (1990)
18. Shparlinski, I. E.: On some problems of theory of finite fields. Uspechi Matem. Nauk **36**(1), 165–200 (in Russian) (1991)