ELSEVIER
Theoretical Computer Science 157 (1996) 273–275
Theoretical Computer Science

On finding primitive roots in finite fields

Igor Shparlinski

School of MPCE, Macquarie University, Sydney, NSW 2109, Australia

Abstract

We show that in any finite field $\mathbb{F}_q$ a primitive root can be found in time $O(q^{1/4+\varepsilon})$.

Let $\mathbb{F}_q$ denote a finite field of q elements. An element $\theta \in \mathbb{F}_q$ is called a primitive root if it generates the multiplicative group $\mathbb{F}_q^*$.

We show that a combination of known results on distribution primitive roots and the factorization algorithm of [6] leads to a deterministic algorithm to find a primitive root of $\mathbb{F}_q$ in time $O(q^{1/4+\varepsilon})$.

All implied constants in O-symbols depend on ε only that denotes and arbitrary positive number. Moreover, (and it is essential if we wish to get a real algorithm) all these constant can be evaluated effectively.

Lemma 1. *For the smallest primitive root θ_p modulo a prime p,*

$$\theta_p = O(p^{1/4+\varepsilon}).$$

Proof. See [1]. □

Lemma 2. *For any r there is a constant $p_0(r, \varepsilon)$ such that for $q = p^r$, where p is a prime number with $p \geqslant p_0(r, \varepsilon)$ and any root α of an irreducible polynomial of degree r over $\mathbb{F}_p$ there exists some integer t, $0 \leqslant t \leqslant p^{1/2+\varepsilon}$ such that $\alpha + t$ is a primitive root of $\mathbb{F}_q$.*

Proof. See [5] (or Theorem 3.5 of [10]). □

Lemma 3. *Let $q = p^r$, where p is a prime number then in time $p^{1+\varepsilon} r^{O(1)}$ one can construct a set $\mathfrak{M} \in \mathbb{F}_q$ of cardinality $|\mathfrak{M}| = pr^{O(1)}$ containing at least one primitive element.*

Proof. The result was proved in [8] and [9] independently (or [10, Theorem 2.4]). □

Lemma 4. *All prime divisors of integer m can be found in time $O(m^{1/4+\varepsilon})$.*

0304-3975/96/$15.00
SSDI 0304-3975(95)00164-6

Proof. See [6]. □

Theorem. *There is a deterministic algorithm to find a primitive root of* $\mathbb{F}_q$ *in time* $O(q^{1/4+\varepsilon})$.

Proof. First of all we note that in time $O(q^{1/4+\varepsilon})$ one can construct a set $\mathfrak{M} \in F_q$ with $|\mathfrak{M}| = O(q^{1/4})$ containing a primitive element of $\mathbb{F}_q$.

Indeed, let $q = p^r$, where p is a prime number.

For $r = 1$ and $r \geqslant 4$ our claim follows directly from Lemmas 1 and 3, respectively, (because $pr^{O(1)} \leqslant q^{1/4}(\log q)^{O(1)} = O(q^{1/4+\varepsilon})$ for $r \geqslant 4$).

For $2 \leqslant r \leqslant 3$, Lemma 2 and the $O(p^{1/2}r^{O(1)})$-algorithm of [7] to construct an irreducible polynomial $f(x) \in \mathbb{F}_p[x]$ of degree r give the desired set in the form

$$\mathfrak{M} = \{\alpha + t \mid 0 \leqslant t \leqslant rp^{1/2+\varepsilon}\},$$

where α is a root of $f(x)$ (i.e. we consider the following model of $\mathbb{F}_q$, $\mathbb{F}_q \simeq \mathbb{F}_p[x]/f(x)$, the isomorphism between different models can be found in polynomial time, see [3]). The cardinality of $\mathfrak{M}$ is $|\mathfrak{M}| = O(p^{1/2+\varepsilon}) = O(q^{1/4+\varepsilon})$ and it can be constructed in time $O(q^{1/4+\varepsilon})$.

Now let us find all prime divisors $l_1, \ldots, l_s$ of $q-1$, in time $O(q^{1/4+\varepsilon})$ using the algorithm of Lemma 4.

It is evident that $\mu \in \mathbb{F}_q$ is a primitive root if and only if $\mu^{(q-1)/l_i} \neq 1$ for every $i = 1, \ldots, s$. Testing all elements of $\mathfrak{M}$ and taking into account that $s = \omega(q-1) = O(\log q)$ we get the desired algorithm. □

We note that using a more complicated version of the Sieve method (from [2], say) one can get an algorithm with slightly better running time $q^{1/4}(\log q)^{O(1)}$.

Let us also mention that the present construction has three quite different bottle-necks with the same complexity $O(q^{1/4+\varepsilon})$:

(1) factorization of $q-1$ using [6],

(2) finding a set containing a primitive root in case $q = p$ using [1],

(3) finding a set containing a primitive root in case $q = p^2$ using [5].

So it is very unlikely that it can be improved at the present time.

On the other hand, it should be mentioned that for many applications we do not actually need a primitive root. It is quite enough just to find a small set $\mathfrak{M}$ containing a primitive root and then use all its elements one by one (or even in parallel). In this case we get a better algorithm $O(q^{1/6+\varepsilon})$, at least under the Extended Riemann Hypothesis (as the cases $q = p$ and $q = p^2$ can be drastically improved, see [8]).

Open Question 1. *Find and algorithm to construct in polynomial time* $(\log q)^{O(1)}$ *a set* $\mathfrak{M}$ *of polynomial cardinality* $|\mathfrak{M}| = (\log q)^{O(1)}$ *containing a primitive root of* $\mathbb{F}_q$ *for any* q *(under the the Extended Riemann Hypothesis).*

Open Question 2. *Combining approaches of* [5] *and* [8, 9] *obtain an analog of Lemma 3 with* $p^{1/2+\varepsilon}$ *instead of* $p^{1+\varepsilon}$ *(or maybe even with* $p^{1/4+\varepsilon}$ *provided an appropriate generalization of* [1] *on non prime finite fields is found).*

Also, our algorithm gives the solution of the exact problem for $\mathbb{F}_q$, $q = p^r$, when p and r are given. On the other hand, for many applications it would be enough to solve an approximate problem when the characteristic p and some integer R are given and we have to find a primitive root in some field $\mathbb{F}_q$, $q = p^r$, with r approximately equal to R (in various senses, say with $r \sim R$, or $R \leqslant r = O(R)$, or even $R \leqslant r = R^{O(1)}$). Moreover for some combinatorial constructions it would be enough to find a primitive root in a field $\mathbb{F}_q$ with q approximately equal to some given integer Q (again in various senses, say with $q \sim Q$, or $Q \leqslant q = O(Q)$, or even $Q \leqslant q = Q^{O(1)}$). Some algorithms with running time $O(q^{\varepsilon})$ to solve some of these problems have been given in [11] (see also Section 2.2 of [10]).

More precisely, it was shown that for any p and R one can construct a field F_{p^r} with $r = R + O(R^{\varepsilon})$ and find its primitive root in time $p^{O(R/\log\log R)}$, and for any Q one can construct a field F_q with $q = Q + O\big(Q\exp[-(\log Q)^{1-\varepsilon}]\big)$ and find its primitive root in time $\exp[O(\log Q/\log\log Q)]$.

For a survey of many other results on distribution and finding primitive roots see [4, Ch. 3] and [10, Chs. 2 and 3].

References

[1] D.A. Burgess, On character sums and primitive roots, *Proc. Lond. Math. Soc.* **12** (1962) 179–192

[2] H. Iwaniec, On the problem of Jacobsthal, *Demonstratio Math.* **11** 1978 225–231

[3] H.W. Lenstra, Finding isomorphisms between finite fields, *Math. Comput.* **56** (1991) 329–347

[4] R. Lidl and H. Niederreiter, *Finite Fields* (Addison-Wesley, Reading, MA, 1983).

[5] G.I. Perelmuter and I.E. Shparlinski, On the distribution of primitive roots in finite fields, *Uspechi Matem. Nauk* **45** (1990) 185–186 (Russian).

[6] J.M. Pollard, Theorems on factorization and primality testing, *Math. Proc. Cambr. Philos. Soc.* **76** (1974) 521–528

[7] V. Shoup, New algorithms for finding irreducible polynomials over finite fields, *Math. Comput.* **54** (1990) 435–447

[8] V. Shoup, Searching for primitive roots in finite fields, *Math. Comput.* **58** (1992) 369–380

[9] I. Shparlinski, On primitive elements in finite fields and on elliptic curves, *Matem. Sbornik* **181** (1990) 1196–1206 (Russian).

[10] I. Shparlinski, *Computational and Algorithmic Problems in Finite Fields* (Kluwer, Dordrecht, 1992).

[11] I. Shparlinski, Finding irreducible and primitive polynomials, *Appl. Algebra in Eng. Commun. and Comput.* **4** (1993) 263–268.