Constructing finite field extensions with large order elements *

Qi Cheng†

Abstract

In this paper, we present an algorithm that given a fixed prime power q and a positive integer N, finds an integer $n \in [N, 2qN]$ and an element $\alpha \in \mathbf{F}_{q^n}$ of order greater than $5.8^{n/\log_q n}$, in time polynomial in N. We present another algorithm that find an integer $n \in [N, N + O(N^{0.77})]$ and an element $\alpha \in \mathbf{F}_{q^n}$ of order at least $5.8^{\sqrt{n}}$, in time polynomial in N. Our result is inspired by the recent AKS primality testing algorithm [1] and the subsequent improvements [4, 5, 3].

1 Introduction

It is well known that every finite field has multiplicative generators, which sometimes are called primitive elements. An important open problem in computational number theory is to construct a multiplicative generator for a given finite field. Although there are plenty of generators in a finite field [7, Chapter 1, Theorem 5.1], finding one is notoriously difficult, since we do not know how to test whether an element is a generator or not without factoring integers or finding discrete logarithms. Assuming GRH does not seem to help.

In practice, small characteristic fields are particularly useful. In this context, one can ask a relevant but less restrictive question: for a fixed prime power q, can we find an element in $\mathbf{F}_{q^n}$ with large order in time polynomial in n? Note in the question that we are not required to give the exact order of the element. Instead, we only need to give a proof that the element has high order. Besides the apparent connection to the generator problem, the problem is interesting in its own regard [12]. However, it does not seem easier than finding a primitive element if we require the order to be greater than q^{n^c} for a constant c. A weak solution was given in [6], which presented a polynomial time algorithm producing an element with order at least $n^{\log_q n}$. Another relevant question asks to find a number n greater than a given number N, and an element of order at least q^{n^c} in $\mathbf{F}_{q^n}$ for some constant c. The rationale of this question, which we call *the special finite field high order element problem*, is to deal with special finite fields first, and then try to increase the density of the sequence of n so that the high order element problem can be eventually solved. von zur Gathen and Igor Shparlinski [12, 11] have obtained the following results:

PROPOSITION 1.1. *Let q be a fixed prime power. For any positive integer N, an integer $n \geq N$ with $n = O(N \log N)$ and an element $\alpha \in \mathbf{F}_{q^n}$ of order at least $2^{(2n)^{1/2}-2}$ can be computed in time polynomial in N.*

PROPOSITION 1.2. *Let q be a fixed prime power. For any positive integer N, an integer $n \geq N$ with $n = N + O(N/\log^c N)$ and an element $\alpha \in \mathbf{F}_{q^n}$ of order at least $2^{10q^{-12}n^{1/2}-25}$ can be computed in time polynomial in N.*

*Part of the paper, in its preliminary form, appeared in the Proceedings of the ACM-SIAM Symposium on Discrete Algorithms (SODA) 2004.

†School of Computer Science, the University of Oklahoma, Norman, OK 73019, USA. Email: qcheng@cs.ou.edu. This research is partially supported by NSF Career Award CCR-0237845

All the above results are based on the properties of Gauss Periods. For a survey, see [12].

2 Our Results

A novel technique in the celebrated AKS primality testing algorithm and its subsequent improvements is to use polynomials of degree one to generate a large multiplicative subgroup modulo an integer and a polynomial. In this paper, we apply this idea to obtain a new solution to the special finite field high order element problem. Our result, which can be summarized in the following theorems, features a denser sequence of n and/or a much higher order.

THEOREM 2.1. *Let q be a fixed prime power. For a sufficiently large positive integer N we can compute in time polynomial in N an integer $n \in [N, 2qN]$ and an element $\alpha \in \mathbf{F}_{q^n}$ with order greater than $5.8^{n/\log_q n}$.*

THEOREM 2.2. *Let q be a fixed prime power. We can compute in time polynomial in N an integer $n \in [N, N + O(N^{0.77})]$ and an element $\alpha \in \mathbf{F}_{q^n}$ with order greater than $5.8^{\sqrt{n}}$.*

They are based on the following result.

LEMMA 2.1. *Let r be a prime power. Let m be a positive divisor of $r-1$. Let $x^m - g$, $g \in \mathbf{F}_r$, be an irreducible polynomial over $\mathbf{F}_r$ and α be one of its roots in the extension field $\mathbf{F}_{r^m}$. Then for any $a \in \mathbf{F}_r^*$, $\alpha + a$ has order greater than*

$$\max_{0 \le d_- \le d \le m} \binom{m}{d_-} \binom{d-1}{d_- - 1} \binom{2m - d_- - d - 2}{m - d_- - 1}.$$

The finite field $\mathbf{F}_{r^m}$ is a Kummer extension of $\mathbf{F}_r$. By a numerical search [3], it can be shown that asymptotically, $\max_{0 \le d_- \le d \le m} \binom{m}{d_-} \binom{d-1}{d_- - 1} \binom{2m-d_- -d-2}{m-d_- -1}$ is $\Omega(5.8^m)$ when we take $d_- = 0.292m$ and $d = m/2$.

Proof. W.l.o.g., suppose that $\mathbf{F}_{r^m} = \mathbf{F}_r[x]/(x^m - g)$, and $\alpha = x \pmod{x^m - g}$. Denote the order of $\alpha + a$ by s. Then $\alpha + a$ is one of the roots of $X^s = 1$. We want to estimate the number of roots of $X^s = 1$. For any $c \in (\mathbf{F}_r^*)^{(r-1)/m}$, $c\alpha + a$ is one of the roots as well, since $c\alpha + a$ is a conjugate of $\alpha + a$ over $\mathbf{F}_r$. If A is a solution and B is a solution, then AB and A/B are solutions as well. We use this fact to find more solutions. Let $c_1, c_2, \cdots, c_m$ be a list of all the elements in $(\mathbf{F}_r^*)^{(r-1)/m}$. If $(e_1, e_2, \cdots, e_m)$ and $(e'_1, e'_2, \cdots, e'_m)$ are two different sequences of integers, suppose that $\sum_{1 \le i \le r-1} |e_i| = m - 1$, $\sum_{1 \le i \le r-1} |e'_i| = m - 1$, $|\{i : e_i < 0\}| = |\{i : e'_i < 0\}| = d_-$ and $\sum_{e_i < 0} |e_i| = \sum_{e'_i < 0} |e_i| = d$, we claim that $\prod_{1 \le i \le m} (c_i\alpha + a)^{e_i} \ne \prod_{1 \le i \le m} (c_i\alpha + a)^{e'_i}$. Assume that these two elements are equal, we have

$$\prod_{1 \le i \le m, e_i \ge 0} (c_i\alpha + a)^{e_i} \prod_{1 \le i \le m, e'_i < 0} (c_i\alpha + a)^{-e'_i} = \prod_{1 \le i \le m, e_i < 0} (c_i\alpha + a)^{-e_i} \prod_{1 \le i \le m, e'_i \ge 0} (c_i\alpha + a)^{e'_i}.$$

Since $\sum_{1 \le i \le m, e_i \ge 0} e_i + \sum_{1 \le i \le m, e'_i < 0} (-e'_i) = \sum_{1 \le i \le m, e_i < 0} (-e_i) + \sum_{1 \le i \le m, e'_i \ge 0} e'_i = m - 1$, we obtain that

$$\prod_{1 \le i \le m, e_i \ge 0} (c_i x + a)^{e_i} \prod_{1 \le i \le m, e'_i < 0} (c_i x + a)^{-e'_i} = \prod_{1 \le i \le m, e_i < 0} (c_i x + a)^{-e_i} \prod_{1 \le i \le m, e'_i \ge 0} (c_i x + a)^{e'_i}$$

in the ring $\mathbf{F}_r[x]$, contradicting the unique factorization of the ring.

Now consider the subset of $\mathbf{F}_{r^m}$:

$$S = \{ \prod_{1 \le i \le m} (c_i \alpha + a)^{e_i} | \sum_{1 \le i \le m} |e_i| = m-1, |\{i : e_i < 0\}| = d_-, \sum_{e_i < 0} |e_i| = d \}.$$

All of the elements in S are roots of $X^s = 1$. Thus $s \ge |S|$. The cardinality of S is $\binom{m}{d_-}\binom{d-1}{d_- -1}\binom{2m-d_- -d-2}{m-d_- -1}$. The exponential size of the group generated by linear factors in a polynomial ring was known before. Using negative exponents to obtain a better bound was suggested by Voloch [10] recently.

Does there exist an irreducible polynomial of form $x^m - g$ over $\mathbf{F}_r$? The following lemma answers the question.

LEMMA 2.2. *The polynomial $x^m - g$ is an irreducible polynomial over $\mathbf{F}_r$ if $m|r-1$ and g is not a l-th power in $\mathbf{F}_r$ for any $l|m$ $(l > 1)$, in particular, if g is a multiplicative generator of $\mathbf{F}_r$.*

Proof. Let α be a root of $x^m - g$ over some extension of $\mathbf{F}_r$. Denote $[\mathbf{F}_r(\alpha) : \mathbf{F}_r]$ by d. We have $[\mathbf{F}_r(a\alpha) : \mathbf{F}_r] = d$ for any $a \in (\mathbf{F}_r^*)^{(r-1)/m}$, and $a\alpha$ is also a root of $x^m - g$. This implies that $x^m - g$ can be factored into irreducible polynomials of degree d over $\mathbf{F}_q$, and $d|m$. Take the factor $f(x)$ satisfying $f(\alpha) = 0$. Assume $f(x)$ is monic, and the constant coefficient of $f(x)$ is f_0. The roots of $f(x)$ have form $\alpha, a_1\alpha, \cdots, a_{d-1}\alpha$. We have $f_0 = (\prod_{i=1}^{d-1} a_i)\alpha^d$. So $\alpha^d = \frac{m}{(\prod_{i=1}^{d-1} a_i)} \in \mathbf{F}_r^*$, and $(\alpha^d)^{m/d} = g$. This contradicts the condition in the lemma.

3 The Algorithms and The Proofs

Now we are ready to describe the algorithms. Let q be a fixed prime power. The input of the algorithm is a positive integer $N > 0$. The first algorithm is designed to prove the Theorem 2.1.

1. Find the smallest positive integer t such that $t(q^t - 1) \ge N$. Let $n = t(q^t - 1)$;
2. Find a generator in $\mathbf{F}_{q^t}$, denote it by g;
3. Solve the equation $x^{q^t - 1} - g = 0$ in $\mathbf{F}_{q^n}$, let α be one of the roots;
4. Output $\alpha + 1$ (or $\alpha + a$ for any $a \in \mathbf{F}_{q^t}^*$).

From Step 1, we see that $N \le n \le 2qN$. Step 2 and 3 altogether take time $(q^t)^{O(1)} = N^{O(1)}$. Hence the algorithm takes time $N^{O(1)}$. Applying Theorem 2.1 with $r = q^t \ge n/\log_q n$ and $m = r - 1$, we get that the order of the output element is greater than 5.8^{q^t} for a sufficiently large n, which is greater than $5.8^{n/\log_q n}$. This proves the Theorem 2.1.

The second algorithm is designed to prove Theorem 2.2

1. Find the smallest prime t greater than $\sqrt{N} + 1$.
2. Use the algorithm described in [9, Theorem 2.4] [8] to construct a small set $G \subseteq \mathbf{F}_{q^t}$ such that at least one of the elements in the subset is a primitive element.
3. For $g \in G$, testing the irreducibility of $x^t - g$. Stop if $x^t - g$ is irreducible over $\mathbf{F}_{q^{t-1}}$;
4. Solve the equation $x^t - g = 0$ in $\mathbf{F}_{q^{(t-1)t}}$, let α be one of the roots;
5. Output $\alpha + 1$ (or $\alpha + a$ for any $a \in \mathbf{F}_{q^t}^*$).

From Step 1, we see that $\sqrt{N}+1 \le t \le \sqrt{N}+O(\sqrt{N}^{0.525})$ [2]. Hence $N \le t(t-1) = N + O(N^{0.77})$. Testing irreducibility and factoring polynomials can be solved in polynomial time if the characteristic of the field is small. And there is at least one primitive element in G. (However, that $x^t - g$ is irreducible does not imply that g is a primitive element in $\mathbf{F}_{q^{t-1}}$.) Hence step 3 and 4 altogether take time $(t \log q)^{O(1)} = N^{O(1)}$. The whole algorithm takes time $N^{O(1)}$. Applying Theorem 2.1 with $r = q^{t-1}$ and $m = t$, the order of the output element is greater than 5.8^t for sufficiently large n, which is greater than $5.8^{\sqrt{n}}$.

4 Concluding Remarks

A few comments are in order

1. A similar idea can be applied to solve the problem of constructing extensions of $\mathbf{F}_{q^r}$ (q is a fixed prime power) with an element of provable high order.

2. Numerical evidences suggest that the order of g is often equal to the group order $q^n - 1$, and is close to the group order otherwise. However, it seems hard to prove it. In fact, this is one of the main obstacles in improving the space efficiency of AKS-style primality testing algorithm [1]. We make the following conjecture.

   CONJECTURE 1. *Let q be a prime power and n be a positive factor of $q-1$. Assume that $n \ge \log q$. Let $x^n - g$ ($g \in \mathbf{F}_q$) be an irreducible polynomial over $\mathbf{F}_q$ and let α be one of its roots. Then the order of $\alpha + 1$ is greater than $q^{n/c}$ for an absolute constant c.*

3. Let p be a prime. The Artin-Schreier extension of a finite field $\mathbf{F}_p$ is $\mathbf{F}_{p^p}$. It is easy to show that $x^p - x - a = 0$ is an irreducible polynomial in $\mathbf{F}_p$ for any $a \in \mathbf{F}_p^*$. So we may take $\mathbf{F}_{p^p} = \mathbf{F}_p[x]/(x^p - x - a)$. Let $\alpha = x \pmod{x^p - x - a}$. It can be shown similarly that the order of $\alpha + b$ for any $b \in \mathbf{F}_p$ is asymptotically greater than 5.8^p.

Acknowledgment: We thank Dr Igor Shparlinski for his suggestion to derandomize the second algorithm. We are grateful to Dr Pedro Berrizbeitia and Mr Yu-Hsin Li for helpful discussions.

References

[1] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. Primes is in P. *Annals of Mathematics*, 160(2):781–793, 2004.

[2] R. C. Baker, G. Harman, and J. Pintz. The difference between consecutive primes II. *Proc. London Math. Soc.*, 83(3):532–562, 2001.

[3] Daniel J Bernstein. Proving primality in essentially quartic random time. *Math. Comp.*, 76(257):389–403, 2007.

[4] Pedro Berrizbeitia. Sharpening "primes is in p" for a large family of numbers. *Math. Comp.*, 74(252):2043–2059, 2005.

[5] Qi Cheng. Primality proving via one round in ECPP and one iteration in AKS. In Dan Boneh, editor, *Proc. of the 23rd Annual International Cryptology Conference (CRYPTO)*, volume 2729 of *Lecture Notes in Computer Science*, pages 338–348, Santa Barbara, 2003. Springer-Verlag.

[6] Shuhong Gao. Elements of provable high orders in finite fields. *Proc. American Mathematical Society*, 127:1615–1623, 1999.

[7] Karl Prachar. *Primzahlverteilung*. Springer-Verlag, 1957.

[8] Victor Shoup. Searching for primitive roots in finite fields. *Math. Comp.*, 58:369–380, 1992.
[9] Igor E. Shparlinski. *Computational and Algorithmic Problems in Finite Fields*. Kluwer Academic, 1992.
[10] Jose F. Voloch. On some subgroups of the multiplicative group of finite rings. *Journal de Theorie des Nombres de Bordeaux*, 16:233–239, 2004.
[11] Joachim von zur Gathen and Igor Shparlinski. Orders of Gauss periods in finite fields. In *Proc. 6th Intern. Symp. on Algorithms and Computation*, volume 1004 of *Lecture Notes in Computer Science*. Springer-Verlag, 1995. Also appeared as Orders of Gauss periods in finite fields. Applicable Algebra in Engineering, Communication and Computing, **9** (1998), 15–24.
[12] Joachim von zur Gathen and Igor Shparlinski. Gauss periods in finite fields. In *Proc. 5th Conference of Finite Fields and their Applications*, pages 162–177. Springer-Verlag, 1999.