ELEMENTS OF PROVABLE HIGH ORDERS IN FINITE FIELDS

SHUHONG GAO

ABSTRACT. A method is given for constructing elements in $\mathbb{F}_{q^n}$ whose orders are larger than any polynomial in n when n becomes large. As a by-product a theorem on multiplicative independence of compositions of polynomials is proved.

1. INTRODUCTION AND MAIN RESULTS

For a prime power q and a positive integer n, $\mathbb{F}_{q^n}$ denotes the finite field of q^n elements. It is a well-known open problem to give an efficient algorithm for constructing primitive elements in finite fields. There are algorithms in the literature that find a small set of elements with at least one element in the set being primitive [2, 12, 13, 14, 15]. However, the known methods for testing primitivity in $\mathbb{F}_{q^n}$ require factoring the integer $q^n - 1$ or computing discrete logarithms in $\mathbb{F}_{q^n}$. Both of the latter problems are notoriously difficult and are not known to be solvable in polynomial time. In practice, it is usually sufficient to have elements of high orders. But again, computing orders of elements in $\mathbb{F}_{q^n}$ requires factoring $q^n - 1$ or computing discrete logarithms in $\mathbb{F}_{q^n}$. The three related problems of finding primitive elements, recognizing primitive elements and computing orders of elements in finite fields are listed as open problems in [1] where more information on their statuses up to 1994 can be found.

Even though the problem of factoring integers remains hard (and so does computing discrete logarithms in finite fields), we can still ask if it is possible to find elements in $\mathbb{F}_{q^n}$ that can be proved being primitive or having high orders without the knowledge of how $q^n - 1$ factors. By "high orders" of elements in $\mathbb{F}_{q^n}$, we mean that the orders of elements must be larger than every polynomial in $n \log q$ when $q^n \to \infty$. There is some progress in this direction for $q = 2$. Recently, Gauss periods have been proven useful in efficient implementation of finite field arithmetic [6]. A special class of Gauss periods generate optimal normal bases [11, 10]. In [5], Gao and Vanstone find by computer experiments that type II optimal normal basis generators are often primitive and always have high orders. Later, von zur Gathen and Shparlinski [8] prove[1] that type II optimal normal basis generators indeed have orders at least $2^{\sqrt{2n}-2}$. This is the first result proving that certain elements in $\mathbb{F}_{2^n}$

Date: November 7, 1997.

1991 *Mathematics Subject Classification.* Primary 11T55; Secondary 11Y16, 68Q25, 11T06, 12Y05.

Key words and phrases. Finite fields, primitive elements, elements of provable high orders, compositions of polynomials.

To appear in *Proc. American Math. Soc.*

[1] Von zur Gathen & Shparlinski [8] prove only for a subclass of type II optimal normal basis generators, i.e., when 2 is primitive modulo $2n + 1$, but their argument can be easily modified to work for the general case.

have high orders without factoring $2^n - 1$ for infinitely many n. But this does not work for all n since, by Gao and Lenstra [4], most fields $\mathbb{F}_{2^n}$ do not have optimal normal bases. In general, $\mathbb{F}_{2^n}$ has a normal basis generated by Gauss periods if and only if $8 \nmid n$ [3]. Gao et al [7] show by computer experiments that Gauss periods always have high orders. It is still open to find a theoretical confirmation for this phenomenon of Gauss periods.

A new method is given below for constructing elements of provable high orders in $\mathbb{F}_{q^n}$ when q is fixed. Our lower bound for the orders of constructed elements is not as good as von zur Gathen and Shparlinski's for optimal normal basis generators, but our method works for all n and any fixed q. For an integer $n > 1$, define

$$\bar{n} = q^{\lceil \log_q n \rceil}.$$

So $\bar{n}$ is the smallest power of q bigger than or equal to n.

Theorem 1.1. *Let $g(x) \in \mathbb{F}_q[x]$ with $\deg g(x) \le 2\log_q n$ and $g(x) \ne ax^k$ or $ax^{p^\ell}+b$ for any $a, b \in \mathbb{F}_q$, $k, \ell \ge 0$, where p is the characteristic of $\mathbb{F}_q$. Suppose that $\alpha \in \mathbb{F}_{q^n}$ has degree n and is a root of $x^{\bar{n}} - g(x)$. Then α has order at least*

$$n^{\frac{\log_q n}{4\log_q(2\log_q n)} - \frac{1}{2}}.$$

This theorem suggests a straightforward method for finding elements of high orders in $\mathbb{F}_{q^n}$:

> *for each polynomial $g(x) \in \mathbb{F}_q[x]$ of degree at most $2\log_q n$, check if $x^{\bar{n}} - g(x)$ has an irreducible factor of degree n. If yes, then stop.*

By Theorem 1.1, any root of an irreducible factor of degree n of $x^{\bar{n}} - g(x)$ is an element in $\mathbb{F}_{q^n}$ of high order. Note that there are at most $q^{2\log_q n} = n^2$ choices for $g(x)$ and for each $g(x)$ it can be decided in time polynomial in n whether $x^{\bar{n}} - g(x)$ has an irreducible factor of degree n. The above algorithm runs in polynomial time when q is fixed.

In comparison, the approaches in [2, 12, 13, 14, 15] construct a small set with at least one primitive element but one can not tell which one is primitive by the current state of art. Our approach finds an element that satisfies some easily cheked conditions and is guaranteed to have high order, though not necessarily a primitive element.

One might ask whether there is always such a required polynomial $g(x) \in \mathbb{F}_q[x]$ of degree at most $2\log_q n$ for all n. In this respect, we prove the following result.

Theorem 1.2. *Let $P_q(m, n)$ be the probability of a random polynomial in $\mathbb{F}_q[x]$ of degree $m \ge n$ having at least one irreducible factor of degree n. Then*

$$P_q(m,n) \sim \frac{1}{n}, \quad \textit{as} \;\; n \longrightarrow \infty,$$

uniformly for q and $m \ge n$.

If we model a polynomial of the form $x^{\bar{n}} - g(x)$, $\deg g(x) \le 2\log_q n$ as a random polynomial of degree $\bar{n}$ in $\mathbb{F}_q[x]$, then Theorem 1.2 indicates that one should expect

$$q^{2\log_q n} \cdot \frac{1}{n} = n^2/n = n$$

polynomials $g(x) \in \mathbb{F}_q[x]$ of degree at most $2\log_q n$ such that $x^{\bar{n}} - g(x)$ has an irreducible factor of degree n. It is reasonable to expect at least one such $g(x)$ to exist. We did a computer experiment for polynomials over $\mathbb{F}_2$ for $n \le 300$. When

$q = 2$, our computer data show that such $g(x)$ do exist and even with a much smaller degree, i.e., $\le \lceil \log_2 n \rceil + 3$, for $n \le 300$. So the following conjecture seems plausible.

Conjecture 1.3. *For any integer $n > 1$, there is a polynomial $g(x) \in \mathbb{F}_q[x]$ of degree at most $2\log_q n$ such that $x^{\bar{n}} - g(x)$ has an irreducible factor of degree n.*

The proof of Theorem 1.1 needs some properties of composition of polynomials. Let $f(x) \in \mathbb{F}_q[x]$ and let $f^{(k)}(x)$ be the polynomial obtained by composing $f(x)$ with itself k times, i.e.,

$$f^{(1)}(x) = f(x), \quad f^{(k)}(x) = f(f^{(k-1)}(x)), \quad k \ge 2. \tag{1}$$

Then we prove that the polynomials $f^{(k)}(x)$, $k = 1, 2, \ldots$, are multiplicative independent except when $f(x)$ is a monomial or certain binomial. More precisely, we prove the following theorem which seems interesting by itself.

Theorem 1.4. *Suppose that $f(x) \in \mathbb{F}_q[x]$ is not a monomial nor a binomial of the form $ax^{p^\ell} + b$ where p is the characteristic of $\mathbb{F}_q$. Then the polynomials*

$$f(x), f^{(2)}(x), \ldots, f^{(n)}(x), \ldots \tag{2}$$

are multiplicatively independent in $\mathbb{F}_q[x]$, that is, if

$$\left(f(x)\right)^{k_1}\left(f^{(2)}(x)\right)^{k_2} \cdots \left(f^{(n)}(x)\right)^{k_n} = 1, \tag{3}$$

for any integers $n \ge 1, k_1, k_2, \ldots, k_n$, then $k_1 = k_2 = \ldots = k_n = 0$.

The remainder of the paper is devoted to proving these results. Section 2 deals with properties of composition of polynomials and Theorem 1.4 is proved there. Theorem 1.1 is proved in Section 3, which can be read independently by assuming Theorem 1.4. Finally, Section 4 contains a proof of Theorem 1.2 and some computational data as well.

2. Composition of polynomials

Let $f(x) \in \mathbb{F}_q[x]$ with $\deg f = d \ge 1$. Use the notation in (1). Obviously, $f^{(k)}(x)$ has degree d^k.

Lemma 2.1. *There exists an integer k such that*

$$f^{(k)}(x) = cx^{d^k} \tag{4}$$

for some $c \in \mathbb{F}_q$ if and only if either

$$f(x) = ax^d \quad \text{for some } a \in \mathbb{F}_q \tag{5}$$

or

$$d = p^\ell \quad \text{and} \quad f(x) = ax^d + b \quad \text{for some } a, b \in \mathbb{F}_q \text{ with } a \ne 0, \tag{6}$$

where p is the characteristic of $\mathbb{F}_q$ and $\ell \ge 0$ is an integer.

Proof. If $f(x)$ is of the form (5), $f^{(k)}(x)$ is obviously of the form (4) for all k. We show that if $f(x)$ is of the form (6), then $f^{(k)}(x)$ is of the form (4) for some k. Suppose $q = p^m$. Since d is a power of p, $f^{(k)}(x)$ is a binomial for all k. In particular,

$$f^{(m)}(x) = ux^{d^m} + v$$

for some $u, v \in \mathbb{F}_q$ with $u \neq 0$. As $q | d^m$, we have $u^{d^m} = u$ and $v^{d^m} = v$. By composing $f^{(m)}(x)$ with itself n times, we have

$$f^{(nm)}(x) = c^n x^{d^{nm}} + (c^{n-1} + \cdots + c + 1)d.$$

If $c = 1$ then $f^{(pm)}(x) = x^{d^{pm}}$ is of the form (4). So assume $c \neq 1$. Then

$$f^{(nm)}(x) = c^n x^{d^{nm}} + \frac{c^n - 1}{c - 1} d$$

Take $n = q - 1$ then $c^n = 1$ and $f^{(nm)}(x) = x^{d^{nm}}$ is of the form (4).

Now assume that (4) holds for some $k \geq 2$. Write $f(x)$ as

$$f(x) = a_1 x^{d_1 p^\ell} + a_2 x^{d_2 p^\ell} + \cdots + a_t x^{d_t p^\ell} + b$$

where p is the characteristic of $\mathbb{F}_q$, $a_i \in \mathbb{F}_q \setminus \{0\}$, $b \in \mathbb{F}_q$, $t \geq 1$, $\ell \geq 0$, $d_1 > d_2 > \cdots > d_t \geq 1$, and $p \nmid \gcd(d_1, d_2, \ldots, d_t)$. Here $d = d_1 p^\ell$ is the degree of $f(x)$. For convenience, denote $r = p^\ell$. Let

$$\begin{aligned} h(x) &= a_1 x^{d_1} + a_2 x^{d_2} + \cdots + a_t x^{d_t} + b, \\ g_i(x) &= a_1^{r^{-i}} x^{d_1} + a_2^{r^{-i}} x^{d_2} + \cdots + a_t^{r^{-i}} x^{d_t} + b^{r^{-i}}, i \geq 1. \end{aligned}$$

Note that if $q = p^m$ then, for any $a \in \mathbb{F}_q$, $a^{r^{-i}} = a^{r^{i(m-1)}} \in \mathbb{F}_q$. Thus $g_i(x) \in \mathbb{F}_q[x]$ and

$$(g_i(x))^{r^i} = h(x^{r^i}), \quad \text{for all } i \geq 1.$$

Hence

$$\begin{aligned} f(x) &= h(x^r) \\ f^{(2)}(x) &= h\left((h(x^r)^r\right) = h\left((g_1(x))^{r^2}\right) = (g_2(g_1(x)))^{r^2} = (g_2 \circ g_1(x))^{r^2} \\ &\vdots \\ f^{(k)}(x) &= (g_k \circ g_{k-1} \circ \cdots \circ g_1(x))^{r^k}, k \geq 1. \end{aligned}$$

The equation (4) implies that

$$g_k \circ g_{k-1} \circ \cdots \circ g_1(x) = c^{r^{-k}} x^{d_1^k} = c_0 x^{d_1^k}, \tag{7}$$

where $c_0 = c^{r^{-k}} \in \mathbb{F}_q$, and $c_0 \neq 0$ as $c \neq 0$. Taking derivative on both sides of (7) yields

$$g_k'(g_{k-1} \circ \cdots \circ g_1(x)) \cdot g_{k-1}'(g_{k-2} \circ \cdots \circ g_1(x)) \cdots g_2'(g_1(x)) \cdot g_1'(x) = d_1^k c_0 x^{d_1^k - 1}. \tag{8}$$

Since $p \nmid \gcd(d_1, d_2, \ldots, d_t)$, $g_i'(x) \neq 0$ for all $i \geq 1$. So the polynomial on the left hand side of (8) is not zero. Therefore $p \nmid d_1$, otherwise the right hand side would be zero. As $d_1^k c_0 \neq 0$ in $\mathbb{F}_q$, the equation (8) implies that $g_1'(x)$ divides $x^{d_1^k - 1}$. Hence $g_1'(x)$ is a monomial. Since $p \nmid d_1$, we must have $p \mid d_i$ for $2 \leq i \leq t$. Hence

$$g_i'(x) = d_1 a_1^{-r^i} x^{d_1 - 1}, \quad i \geq 1.$$

By (8), $g_2'(g_1(x)) = d_1 a_1^{-r^2} (g_1(x))^{d_1 - 1}$ is also a factor of $x^{d_1^k - 1}$. If $d_1 > 1$ then $g_1(x)$ must be a monomial, hence $f(x)$ must be a monomial. If $d_1 = 1$, then $d_1 > d_2 > \cdots > d_t \geq 1$ implies that $t = 1$. Therefore $f(x)$ is a binomial of the form (6). □

Lemma 2.2. *Let e be the smallest positive integer k such that $x|f^{(k)}(x)$, and $e = \infty$ if $x \nmid f^{(k)}(x)$ for all $k \geq 1$. Then, for all $k, \ell \geq 1$,*

$$\gcd(f^{(k)}(x), f^{(\ell)}(x)) \neq 1 \quad \textit{iff} \quad k \equiv \ell \ (\text{mod} e).$$

(When $e = \infty$, $k \equiv \ell$ $(\text{mod} e)$ means that $k = \ell$.)

Proof. Suppose that $d(x) = \gcd(f^{(k)}(x), f^{(\ell)}(x))$ has degree ≥ 1 for some $k > \ell \geq 1$. Let β be a root of $d(x)$ in some extension field of $\mathbb{F}_q$. Then $f^{(k)}(\beta) = f^{(\ell)}(\beta) = 0$. Since $f^{(k)}(x) = f^{(k-\ell)}(f^{(\ell)}(x))$,

$$f^{(k-\ell)}(0) = f^{(k-\ell)}(f^{(\ell)}(\beta)) = f^{(k)}(\beta) = 0.$$

Thus $x|f^{(k-\ell)}(x)$ where $k - \ell \geq 1$. This proves the theorem when $e = \infty$.

Now assume that $e < \infty$. Let

$$f^{(e)}(x) = x^t g(x), \quad x \nmid g(x) \text{ and } t \geq 1.$$

Then, for every $i \geq 1$, $f^{(ie)}(x) = x^{t^i} h_i(x)$ for some $h(x) \in \mathbb{F}_q[x]$. If $k \equiv \ell$ $(\text{mod} e)$, say $k = \ell + ue$ where $u \geq 1$, then

$$f^{(k)}(x) = f^{(ue)}\left(f^{(\ell)}(x)\right) = \left(f^{(\ell)}(x)\right)^{t^u} h_u(x).$$

Hence $f^{(\ell)}(x)$ divides $f^{(k)}(x)$ and $\gcd(f^{(k)}(x), f^{(\ell)}(x)) \neq 1$. If $k \not\equiv \ell$ $(\text{mod} e)$, say $k = \ell + ue + r$ where $u \geq 0$ and $1 \leq r < e$. If $\gcd(f^{(k)}(x), f^{(\ell)}(x)) \neq 1$, then, by the above argument, $f^{(ue+r)}(0) = f^{(k-\ell)}(0) = 0$. Noting that

$$f^{(ue+r)}(x) = f^{(r)}\left(f^{(ue)}(x)\right) = f^{(r)}\left(x^{t^u} h_u(x)\right),$$

we have $f^{(r)}(0) = 0$, i.e., $x \mid f^{(r)}(x)$, contradicting the choice of e. Therefore $\gcd(f^{(k)}(x), f^{(\ell)}(x)) = 1$ when $k \not\equiv \ell$ $(\text{mod} e)$. □

We are now ready to prove Theorem 1.4. By Lemma 2.2, if $x \nmid f^{(n)}(x)$ for all $n \geq 1$, then the polynomials in (2) are pairwise relatively prime, and are thus multiplicatively independent as $\mathbb{F}_q[x]$ is a unique factorization domain.

So assume that $x \mid f^{(n)}(x)$ for some $n \geq 1$. Let e be the smallest such integer n, and

$$f^{(e)}(x) = x^t g(x), \quad t \geq 1, \ x \nmid g(x). \tag{9}$$

Lemma 2.1 implies that $\deg g(x) \geq 1$. By Lemma 2.2, $f^{(k)}(x)$ and $f^{(\ell)}(x)$ have a nontrivial common factor iff $k \equiv \ell$ $(\text{mod} e)$. We just need to show that, for each $n \geq 1$, $f^{(n)}(x)$ has a factor of degree ≥ 1 that is relatively prime to all $f^{(k)}(x)$ with $k < n$ and $k \equiv n$ $(\text{mod} e)$. Then the equation (3) implies that $k_n = 0$ and, recursively, $k_{n-1} = \ldots = k_1 = 0$.

Let $n = r + ue$ where $u \geq 1$ and $0 \leq r < e$. Then k is of the form $r + ie$, $0 \leq i \leq u - 1$. Denote $f_i(x) = f^{(r+ie)}(x)$ for $i \geq 0$. Then $f_u(x) = f^{(n)}(x)$ and $f_i(x) = f^{(k)}(x)$. By (9),

$$f_i(x) = f^{(e)}\big(f_{i-1}(x)\big) = \big(f_{i-1}(x)\big)^t g\big(f_{i-1}(x)\big), i \geq 1.$$

As $t \geq 1$, we see that $f_{i-1}(x) \mid f_i(x)$ for all $i \geq 1$. Consequently, $f_i(x)|f_{u-1}(x)$. Since $x \nmid g(x)$, $f_i(x)$ and $g\big(f_{u-1}(x)\big)$ are relatively prime for all $0 \leq i \leq u - 1$. This proves the theorem as $g\big(f_{u-1}(x)\big)$ is a factor of $f^{(n)}(x)$ of degree ≥ 1. □

3. Proof of Theorem 1.1

Denote $m = \bar{n}$. Since α is a root of $x^m - g(x)$, we have $\alpha^m = g(\alpha)$. The facts that m is a power of q and $g(x) \in \mathbb{F}_q[x]$ imply that,

$$\alpha^{m^2} = \big(g(\alpha)\big)^m = g(\alpha^m) = g(g(\alpha)) = g^{(2)}(\alpha).$$

Continuing raising to the mth power, we have

$$\alpha^{m^i} = g^{(i)}(\alpha), \text{ for } i \geq 0. \tag{10}$$

Let ϵ be the degree of $g(x)$. Then $2 \leq \epsilon \leq 2\log_q n$ and $g^{(k)}(x)$ has degree ϵ^k.

Set $S = \{\sum_{i=0}^{t-1} a_i m^i : 0 \leq a_i \leq \mu\}$ where t and μ are some positive integers. We show that if

$$\mu\,\epsilon^t \leq n, \tag{11}$$

then α^a are distinct elements in $\mathbb{F}_{q^n}$ for $a \in S$, thus α has order at least

$$\#S = (\mu+1)^t. \tag{12}$$

Suppose that there are integers $a \neq b$ in S such that $\alpha^a = \alpha^b$. Write $a = \sum_{i=0}^{t-1} a_i m^i$ and $b = \sum_{i=0}^{t-1} b_i m^i$ where $0 \leq a_i, b_i \leq \mu$ for $0 \leq i < t$. Then $\alpha^a = \alpha^b$ can be rewritten as

$$\prod_{i=0}^{t-1}\big(\alpha^{m^i}\big)^{a_i} = \prod_{i=0}^{t-1}\big(\alpha^{m^i}\big)^{b_i}.$$

By (10), we have

$$\prod_{i=0}^{t-1}\big(g^{(i)}(\alpha)\big)^{a_i} = \prod_{i=0}^{t-1}\big(g^{(i)}(\alpha)\big)^{b_i}.$$

Let

$$h_1(x) = \prod_{a_i > b_i}\big(g^{(i)}(x)\big)^{a_i - b_i} \quad \text{and} \quad h_2(x) = \prod_{a_i < b_i}\big(g^{(i)}(x)\big)^{b_i - a_i}.$$

Then $h_1(\alpha) = h_2(\alpha)$. Since α has degree n and $h_1(x)$ and $h_2(x)$ have degree at most

$$\sum_{i=0}^{t-1}\mu\epsilon^i = \mu\frac{\epsilon^t - 1}{\epsilon - 1} < \mu\epsilon^t \leq n,$$

$h_1(x)$ must equal to $h_2(x)$. Therefore $\prod_{i=0}^{t-1}\big(g^{(i)}(x)\big)^{a_i - b_i} = 1$. By Theorem 1.4, the polynomials

$$g(x), g^{(2)}(x), \ldots, g^{(n)}(x), \ldots$$

are multiplicatively independent in $\mathbb{F}_q[x]$. So $a_i - b_i = 0$ for $0 \leq i < t$, and thus $a = b$, contradicting $a \neq b$.

Finally, take

$$t = \left\lfloor \frac{\log_q n}{2\log_q \epsilon} \right\rfloor, \quad \mu = \lfloor\sqrt{n}\rfloor.$$

Then the equation (11) is satisfied, and

$$\#S = (\mu+1)^t \geq (\sqrt{n})^{\frac{\log_q n}{2\log_q \epsilon} - 1} = n^{\frac{\log_q n}{4\log_q \epsilon} - \frac{1}{2}} \geq n^{\frac{\log_q n}{4\log_q(2\log_q n)} - \frac{1}{2}}.$$

This finishes the proof. □

4. Polynomials with an irreducible factor of a given degree

The proof of Theorem 1.2 and some computational results are presented below.

To prove Theorm 1.2, let $N_q(m,n)$ be the number of polynomials in $\mathbb{F}_q[x]$ of degree m with at least one irreducible factor of degree n. By inclusion and exclusion principle, we have

$$N_q(m,n) = \sum_{i=1}^{\lfloor m/n \rfloor} (-1)^{i-1} \binom{I_n}{i} q^{m-ni}$$

where I_n is the number of irreducible polynomials of degree n in $\mathbb{F}_q[x]$. Then

$$P_q(m,n) = \frac{N_q(m,n)}{q^m} = \sum_{i=1}^{\lfloor m/n \rfloor} (-1)^{i-1} \binom{I_n}{i} q^{-ni}. \tag{13}$$

It is well-known (see [9], p142, Ex. 3.26 and 3.27) that

$$\frac{q^n}{n} - \frac{q(q^{n/2}-1)}{(q-1)n} \le I_n \le \frac{q^n - q}{n}.$$

So, uniformly for $q \ge 2$,

$$\frac{I_n}{q^n} \sim \frac{1}{n}, \text{ as } n \longrightarrow \infty. \tag{14}$$

Since $I_n/q^n \le 1$, we see that $\binom{I_n}{i} q^{-ni}$ decreases when i increases. Dropping all the terms on the right hand sight of (13) with $i \ge 1$ and those with $i \ge 2$, we have

$$\frac{I_n}{q^n} - \binom{I_n}{2} \frac{1}{q^{2n}} \le P_q(m,n) \le \frac{I_n}{q^n},$$

i.e.,

$$\frac{I_n}{q^n}\left(1 - \frac{I_n - 1}{2q^n}\right) \le P_q(m,n) \le \frac{I_n}{q^n}.$$

By (14), we see immediately that Theorem 1.2 holds. □

To verify Conjecture 1.3, we computed $g(x) \in \mathbb{F}_2[x]$ of smallest degree such that $x^{\bar{n}} + g(x)$ has an irreducible factor of degree n for $n \le 300$. When $q = 2$, the conjecture holds for all $n \le 300$. In Table 1 below, we list the $g(x)$ we found for degrees n around powers of 2. One can see that $\deg g(x) \le \lceil \log_2 n \rceil + 3 \le 2\lceil \log_2 n \rceil$ for all the degrees listed. It would be interesting to have a theoretical confirmation of the conjecture.

We also computed the order of α which is a root of the irreducible factor of $x^{\bar{n}} + g(x)$ of degree n. In Table 1, "Ind" means the index of α which is by definition $(2^n - 1)/e$ where e is the order of α. Almost all the indices are smaller than n, i.e., the orders of α are at least $(2^n - 1)/n$, except for $n = 11, 30, 252$. For values of $n \le 300$ not listed in the table, the only exception is $n = 180$ with $g(x) = x^7 + x^5 + x^3 + x + 1$ and index 49775.

Acknowledgement. The author would like to thank Stephen D. Cohen for sharing his idea in the proof of Lemma 2.2, and Joel Brawley and Jenny Key for their useful comments and encouragement.

n	$\bar{n}$	$g(x)$	Ind	n	$\bar{n}$	$g(x)$	Ind
7	2^3	$x^2 + x + 1$	1	70	2^7	$x^8 + x^5 + x^4 + x^3 + 1$	3
8	2^3	$x^4 + x^3 + x + 1$	5	100	2^7	$x^6 + x^3 + x + 1$	11
9	2^4	$x^3 + x^2 + 1$	1	101	2^7	$x^8 + x^6 + x + 1$	1
10	2^4	$x^4 + x^3 + 1$	3	102	2^7	$x^7 + x^3 + x^2 + 1$	1
11	2^4	$x^5 + x^3 + x^2 + x + 1$	23	103	2^7	$x^7 + x^5 + 1$	1
12	2^4	$x^6 + x^4 + x^2 + x + 1$	1	104	2^7	$x^5 + x^3 + x + 1$	1
13	2^4	$x^3 + 1$	1	105	2^7	$x^8 + x^7 + x^5 + x^4 + x^3 + x^2 + 1$	1
14	2^4	$x^4 + x^2 + x + 1$	1	125	2^7	$x^3 + 1$	1
15	2^4	$x^2 + x + 1$	1	126	2^7	$x^9 + x^7 + x^4 + x^3 + x^2 + x + 1$	3
16	2^4	$x^5 + x^3 + x + 1$	3	127	2^7	$x^2 + x + 1$	1
17	2^5	$x^5 + x^3 + x + 1$	1	128	2^7	$x^7 + x^2 + x + 1$	1
18	2^5	$x^5 + x^2 + x + 1$	7	129	2^8	$x^8 + x^3 + x + 1$	1
19	2^5	$x^5 + x^3 + x^2 + x + 1$	1	130	2^8	$x^7 + x^6 + x^5 + x^3 + x^2 + x + 1$	1
20	2^5	$x^7 + x^4 + x^3 + x^2 + 1$	1	131	2^8	$x^8 + x^7 + x^3 + x + 1$	1
30	2^5	$x^3 + x + 1$	99	132	2^8	$x^8 + x^5 + x^4 + x^3 + 1$	117
31	2^5	$x^4 + x + 1$	1	133	2^8	$x^6 + x^4 + x^3 + x^2 + 1$	1
32	2^5	$x^7 + x^3 + x^2 + 1$	3	134	2^8	$x^8 + x^5 + 1$	3
33	2^6	$x^3 + x^2 + 1$	7	135	2^8	$x^{10} + x^7 + x^6 + x^5 + x^4 + x^3 + 1$	1
34	2^6	$x^6 + x^5 + x^4 + x^3 + x^2 + 1$	1	200	2^8	$x^9 + x^7 + x^6 + x^5 + x^4 + 1$	15
35	2^6	$x^7 + x^5 + x^4 + x^3 + x + 1$	1	201	2^8	$x^7 + 1$	1
36	2^6	$x^5 + x^4 + x^3 + x + 1$	1	202	2^8	$x^8 + x^5 + x^2 + x + 1$	3
37	2^6	$x^5 + 1$	1	203	2^8	$x^{11} + x^7 + x^2 + 1$	1
38	2^6	$x^6 + x^3 + 1$	3	204	2^8	$x^{10} + x^9 + x^5 + x^2 + 1$	1
39	2^6	$x^7 + x^5 + x^4 + x^2 + 1$	1	205	2^8	$x^9 + x^5 + x^4 + x^3 + 1$	1
40	2^6	$x^5 + x^3 + x^2 + 1$	11	250	2^8	$x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + 1$	1
60	2^6	$x^5 + x + 1$	15	251	2^8	$x^9 + x^8 + x^6 + x^5 + x^3 + x^2 + 1$	1
61	2^6	$x^6 + x^2 + x + 1$	1	252	2^8	$x^8 + x^7 + x^5 + x^4 + x^3 + x^2 + 1$	273
62	2^6	$x^4 + x^2 + x + 1$	3	253	2^8	$x^8 + x^7 + x^2 + x + 1$	1
63	2^6	$x^2 + x + 1$	7	254	2^8	$x^4 + x^2 + x + 1$	1
64	2^6	$x^4 + x^3 + x + 1$	1	255	2^8	$x^6 + x^3 + 1$	1
65	2^7	$x^3 + x^2 + 1$	1	256	2^8	$x^{10} + x^5 + x^2 + 1$	1
66	2^7	$x^7 + x^5 + x^4 + x^3 + 1$	1	257	2^9	$x^9 + x^8 + x^7 + x^5 + x^2 + x + 1$	1
67	2^7	$x^5 + x + 1$	1	258	2^9	$x^{10} + x^6 + x^4 + x^3 + x^2 + 1$	1
68	2^7	$x^7 + 1$	1	259	2^9	$x^{11} + x^9 + x^7 + x^4 + x^3 + 1$	1
69	2^7	$x^7 + x^6 + x^2 + x + 1$	1	260	2^9	$x^{10} + x^9 + x^8 + x + 1$	25

TABLE 1. Smallest $g(x) \in \mathbb{F}_2[x]$ such that $x^{\bar{n}} + g(x)$ has an irreducilbe factor of degree n.

REFERENCES

[1] L.M. ADLEMAN AND K.S. MCCURLEY, "Open problems in number theorectic complexity, II," in *Proc. 1994 Algorithmic Number Theory Symposium*, LNCS 877, Springer-Verlag, 1994, 291–322.

[2] E. BACH, "Comments on search procedures for primitive roots," *Math. Comp.* **66** (1997), 1719-1727.

[3] S. GAO, "Gauss periods, groups, and normal bases," preprint, 1997.

[4] S. GAO AND H.W. LENSTRA, JR., "Optimal normal bases," *Designs, Codes and Cryptography* **2** (1992), 315-323.

[5] S. GAO AND S. VANSTONE, "On orders of optimal normal basis generators," *Math. Comp.* **64** (1995), 1227–1233.

[6] S. GAO, J. VON ZUR GATHEN AND D. PANARIO, "Gauss periods and fast exponentiation in finite fields," extended abstract in *Lecture Notes in Computer Science*, vol. 911, Springer-Verlag, 1995, 311–322.

[7] S. GAO, J. VON ZUR GATHEN AND D. PANARIO, "Gauss periods: orders and cryptographical applications," to appear in *Math. Comp.*, 1998.

[8] J. VON ZUR GATHEN AND I. SHPARLINSKI, "Orders of Gauss periods in finite fields," *Proc. 6th International Symposium on Algorithms and Computation, Cairns*, LNCS 1004, 1995, 208–215.

[9] R. LIDL AND H. NIEDERREITER, *Finite Fields*, Addison-Wesley, Reading, MA, 1983. (Now distributed by Cambridge University Press.)

[10] A.J. MENEZES (ED.), I.F. BLAKE, X. GAO, R.C. MULLIN, S.A. VANSTONE AND T. YAGHOOBIAN, *Applications of Finite Fields*, Kluwer, 1993.

[11] R.C. MULLIN, I.M. ONYSZCHUK, S.A. VANSTONE AND R.M. WILSON, "Optimal normal bases in $GF(p^n)$," *Discrete Applied Math.* **22** (1988/1989), 149-161.

[12] V. SHOUP, "Searching for primitive roots in finite fields," *Math. Comp.* **58** (1992), 369-380.

[13] I. Shparlinski "On primitive elements in finite fields and on elliptic curves," *Matem. Sbornik* **181** (1990), no. 9, 1196–1206. (in Russian)

[14] D. Wan "Generators and irreducible polynomials over finite fields," *Math. Comp.* **66** (1997), 1195–1212.

[15] Y. Wang, "On the least primitive root of a prime," *Scientia Sinica* **10** (1961), 1–14.

Department of Mathematical Sciences, Clemson University, Clemson, SC 29634 USA
E-mail address: sgao@math.clemson.edu