Density of Normal Elements

Shuhong Gao
Department of Mathematical Sciences
Clemson University
Clemson, South Carolina 29634-1907
USA
sgao@math.clemson.edu

Daniel Panario
Department of Computer Science
University of Toronto
Toronto, M5S 1A4
Canada
daniel@cs.toronto.edu

February 20, 1997

Running Head: Density of Normal Elements

Proofs should be sent to:

Shuhong Gao

Department of Mathematical Sciences

Clemson University

Clemson, South Carolina 29634-1907

USA

Phone Number: (864) 656 2729

Fax Number: (864) 656 5230

E-mai: sgao@math.clemson.edu

Abstract

Let $f \in \mathbb{F}_q[x]$ be a monic polynomial of degree n, and let $\Phi(f)$ denote the number of polynomials in $\mathbb{F}_q[x]$ of degree $< n$ that are relatively prime to f. Let $\kappa(f) = \Phi(f)/q^n$. We slightly improve the previous known lower bounds of $\kappa(f)$. The density of normal elements in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is $\kappa(x^n - 1) = \Phi(x^n - 1)/q^n$. We prove that $\kappa(x^n - 1) \geq C > 0$ for $n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$ where p_i are any fixed primes, e_i vary, and C is a constant independent of e_i's. Unfortunately, this is not true for general n. Indeed, we show an upper bound on $\kappa(x^n - 1)$ for infinitely many values of n that goes to 0 as n approaches infinity. This upper bound is almost tight with our lower bound for a general polynomial f.

1 Introduction

For a prime power q and an integer $n \geq 2$, let $\mathbb{F}_q$ and $\mathbb{F}_{q^n}$ be the finite fields with q and q^n elements, respectively. Let $f \in \mathbb{F}_q[x]$ be a monic polynomial of degree n, and let $\Phi(f)$ denote the number of polynomials in $\mathbb{F}_q[x]$ of degree $< n$ that are relatively prime to f. The function $\Phi(\cdot)$ is called the Euler totient function for polynomials over finite fields. Let $\kappa(f) = \Phi(f)/q^n$. In Section 2, we present a lower bound for $\kappa(f)$ that slightly improves the lower bounds in the liteature (Wiedemann 1986, von zur Gathen & Giesbrecht 1990, Frandsen 1991, and Giesbrecht 1993).

This kind of lower bound is useful for solving sparse linear equations (Wiedemann 1986), and for constructing normal elements over finite fields using randomized algorithms (von zur Gathen & Giesbrecht 1990 and Giesbrecht 1993). An element $\alpha \in \mathbb{F}_{q^n}$ is *normal* over $\mathbb{F}_q$ if and only if its conjugates $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$ are linearly independent over $\mathbb{F}_q$. When α is normal, the basis $(\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}})$ is called the *normal basis* generated by α. Ore (1934, Theorem 12) proves that the number of normal elements in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is $\Phi(x^n-1)$ (see also Lidl & Niederreiter 1983, p. 124, Theorem 3.73, and Menezes *et al.* 1993, Chap. 4). The density of normal elements in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is then $\kappa(x^n-1) = \Phi(x^n-1)/q^n$.

To construct a normal element in $\mathbb{F}_{q^n}$, one simple method is to draw an element uniform randomly from $\mathbb{F}_{q^n}$, test if it is normal, and repeat until a normal element is obtained. The density $\kappa(x^n-1)$ is the probability of a random element being normal. Thus one expects to draw $\lceil 1/\kappa(x^n-1)\rceil$ elements to get a normal one. A good lower bound for $\kappa(x^n-1)$ gives a good upper bound for the expected number of draws (or samplings). In Section 3, we prove that $\kappa(x^n-1) \geq C > 0$ for $n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$ where p_i are fixed primes, e_i vary, and C is a constant independent of e_i's (Theorem 3.3). Unfortunately, this is not true for general n. Indeed, we show an upper bound on $\kappa(x^n-1)$ for infinitely many values of n that goes to 0 as n approaches infinity (Theorem 3.4). This upper bound is almost tight with our lower bound of Section 2.

2 Lower bounds on the Euler totient function for polynomials

For a monic $f \in \mathbb{F}_q[x]$, denote by

$$|f| = \#\Big(\mathbb{F}_q[x]/(f)\Big) = q^{\deg f}.$$

Then, similar to Euler function for integers, we have (see Lidl & Niederreiter 1983, p. 122, Lemma 3.69)

$$\Phi(f) = |f| \prod_{g|f,\, g \text{ irr.}} (1 - |g|^{-1}), \tag{1}$$

where the product ranges over all the irreducible monic factors g of f. Suppose that $f \in \mathbb{F}_q[x]$ has degree n and

$$f = f_1^{e_1} f_2^{e_2} \cdots f_r^{e_r}, \tag{2}$$

where $f_1, \ldots, f_r \in \mathbb{F}_q[x]$ are distinct irreducible factors of f. Let d_i denote the degree of f_i, $i = 1, \ldots, r$. Then (1) can be written as

$$\Phi(f) = q^n \prod_{i=1}^{r} \Big(1 - \frac{1}{q^{d_i}}\Big). \tag{3}$$

We focus on lower bounds for $\kappa(f) = \Phi(f)/|f|$, where $f \in \mathbb{F}_q[x]$ is monic of degree n. Several authors give lower bounds on $\kappa(f)$:

- Wiedemann (1986): $\kappa(f) \geq \frac{1}{6(1+\log_q n)}$.
- von zur Gathen & Giesbrecht (1990): $\kappa(f) > \frac{1}{16 \log_q n}$, and $\kappa(f) \geq \frac{1}{34}$ if $n \leq q^2$.
- Frandsen (1991): $\kappa(f) \geq (1 - \frac{1}{q})\frac{1}{e(1+\log_q n)}$, and $\kappa(f) \geq \frac{1}{2}$ if $q \geq 2n(n-1)$.
- Giesbrecht (1993): $\kappa(f) \geq \frac{1}{5 \log_q n}$ if $n > q$, and $\kappa(f) \geq \frac{1}{e}$ if $n \leq q$.

We prove a slightly improved lower bound on $\kappa(f)$ following the proof of Frandsen (1991).

Theorem 2.1 *For any $f \in \mathbb{F}_q[x]$ of degree n with $f(0) \neq 0$, if $n \geq q$ then*

$$\kappa(f) \geq \frac{1}{e^{\gamma + \frac{1}{2(1+\log_q n)}}(1+\log_q n)} > \frac{1}{e^{0.83}(1+\log_q n)},$$

where $\gamma = 0.577216\cdots$ is the Euler constant, and if $n < q$ then $\kappa(f) > 1/e$.

Proof. We use the notations in (2) and (3). For any positive integer m, $1-1/q^m \geq (1-1/q)^m$, when $q \geq 2$. We have

$$\kappa(f) = \prod_{i=1}^{r}\left(1 - \frac{1}{q^{d_i}}\right) \geq (1-1/q)^{\sum_{i=1}^{r} d_i} \geq (1-1/q)^n.$$

If $n < q$, then

$$(1-1/q)^n \geq (1-1/q)^{q-1} = ((1+1/(q-1))^{q-1})^{-1} \geq e^{-1}.$$

It remains to prove the case for $n \geq q$. For $1 \leq k \leq n$, let

$$\tau_k = \#\{i : d_i = k,\ 1 \leq i \leq r\}.$$

Then

$$\sum_{k=1}^{n} k\tau_k = n \quad \text{and} \quad \kappa(f) = \prod_{k=1}^{n}\left(1 - \frac{1}{q^k}\right)^{\tau_k}.$$

For $k \geq 1$, let I_k be the number of monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree k that are different from x. Then

$$\tau_k \leq I_k \leq \frac{q^k - 1}{k}, \quad k \geq 1. \tag{4}$$

The second inequality follows from the fact that each irreducible polynomial in $\mathbb{F}_q[x]$ of degree k divides $x^{q^k} - x$. Define $u = \lfloor \log_q n \rfloor$. Then

$$\sum_{k=1}^{u+1} kI_k \geq q^{u+1} - 1 \geq q^{\log_q n} = n = \sum_{k=1}^{n} k\tau_k. \tag{5}$$

The first inequality follows from the fact that the irreducible factors of $x^{q^{u+1}-1} - 1$ are distinct, not equal to x, and have degrees $\leq u+1$.

We claim that

$$\prod_{k=1}^{n}\left(1 - \frac{1}{q^k}\right)^{\tau_k} \geq \prod_{k=1}^{u+1}\left(1 - \frac{1}{q^k}\right)^{I_k}. \tag{6}$$

Indeed, it follows from (4) and (5) that

$$(u+1)\sum_{k=1}^{u+1}(I_k-\tau_k) \geq \sum_{k=1}^{u+1} k(I_k-\tau_k) \geq \sum_{k=u+2}^{n} k\tau_k \geq (u+1)\sum_{k=u+2}^{n}\tau_k,$$

and hence

$$\sum_{k=1}^{u+1}(I_k-\tau_k) \geq \sum_{k=u+2}^{n}\tau_k. \tag{7}$$

We have

$$\prod_{k=1}^{u+1}\left(1-\frac{1}{q^k}\right)^{I_k}\left(\prod_{k=1}^{u+1}\left(1-\frac{1}{q^k}\right)^{\tau_k}\right)^{-1} = \prod_{k=1}^{u+1}\left(1-\frac{1}{q^k}\right)^{I_k-\tau_k} \leq \prod_{k=1}^{u+1}\left(1-\frac{1}{q^{u+1}}\right)^{I_k-\tau_k}.$$

Using (7),

$$\prod_{k=1}^{u+1}\left(1-\frac{1}{q^{u+1}}\right)^{I_k-\tau_k} \leq \left(1-\frac{1}{q^{u+1}}\right)^{\sum_{k=1}^{u+1}(I_k-\tau_k)} \leq \left(1-\frac{1}{q^{u+1}}\right)^{\sum_{k=u+2}^{n}\tau_k}.$$

Finally,

$$\left(1-\frac{1}{q^{u+1}}\right)^{\sum_{k=u+2}^{n}\tau_k} \leq \prod_{k=u+2}^{n}\left(1-\frac{1}{q^{u+1}}\right)^{\tau_k} \leq \prod_{k=u+2}^{n}\left(1-\frac{1}{q^k}\right)^{\tau_k}.$$

This proves (6). Thus

$$\kappa(f) = \prod_{k=1}^{n}\left(1-\frac{1}{q^k}\right)^{\tau_k} \geq \prod_{k=1}^{u+1}\left(1-\frac{1}{q^k}\right)^{I_k} \geq \prod_{k=1}^{u+1}\left(1-\frac{1}{q^k}\right)^{\frac{q^k-1}{k}} \geq \prod_{k=1}^{u+1}\left(\frac{1}{e}\right)^{\frac{1}{k}} = \left(\frac{1}{e}\right)^{\sum_{k=1}^{u+1}\frac{1}{k}}.$$

For the approximation of $H_m = \sum_{k=1}^{m} 1/k$, we can use (see Graham *et al.* 1994, p. 452)

$$H_m = \ln m + \gamma + \frac{1}{2m} - \frac{1}{12m^2} + O(m^{-4}), \tag{8}$$

where $\gamma = 0.577216\cdots$ is the Euler constant. We finally obtain

$$\kappa(f) \geq \left(\frac{1}{e}\right)^{\ln(1+u)+\gamma+\frac{1}{2(1+u)}} \geq \frac{1}{e^{\gamma+\frac{1}{2(1+\log_q n)}}(1+\log_q n)} > \frac{1}{e^{0.83}(1+\log_q n)},$$

since when $n \geq q$, $\gamma + \frac{1}{2(1+\log_q n)} \leq \gamma + 1/4 < 0.83$. This completes the proof. $\square$

We should mention that the inequality (6) is used by Frandsen (1991). Our contribution is in its rigorous proof.

3 Density of normal elements

We stated in Section 1 that the density of normal elements in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is $\kappa(x^n-1) = \Phi(x^n-1)/q^n$. Theorem 2.1 give lower bounds on the density of normal elements. The question is: can we prove better lower bounds for the special polynomial $x^n - 1$? In this section, we give both positive and negative answers to this question. On the one hand, we show that, for infinitely many values of n, $\kappa(x^n-1) \geq C > 0$, for some constant C. On the other hand, for infinitely many n, we show an upper bound on $\kappa(x^n-1)$ that goes to 0 as n approaches infinity. This upper bound is almost tight with the lower bound in Theorem 2.1. First we state some useful lemmas.

Lemma 3.1 *Let $\tau(d)$ denote the order of q modulo d and $\phi(d)$ be the Euler totient function for integers. Then,*

$$\kappa(x^n-1) = \prod_{d|n}\left(1 - q^{-\tau(d)}\right)^{\frac{\phi(d)}{\tau(d)}}. \tag{9}$$

Proof. See von zur Gathen & Giesbrecht (1990, p. 552). □

Lemma 3.2 *For any integer $m \geq 2$ and real number $0 < a \leq 1/2$,*

$$\prod_{k=1}^{\infty}(1 - a^{m^k}) \geq 1 - a^{m-1} \geq 1 - a. \tag{10}$$

Proof. $\prod_{k=1}^{\infty}(1-a^{m^k}) \geq 1 - \sum_{k=1}^{\infty} a^{m^k} \geq 1 - \sum_{k=0}^{\infty} a^{m+k} \geq 1 - \frac{a^m}{1-a} \geq 1 - a^{m-1}$. □

3.1 Fixed prime factors case

We show in this subsection that $\kappa(x^n-1)$ is bounded away from zero when n has fixed prime factors.

Theorem 3.3 *Let $n = p_1^{e_1}p_2^{e_2}\cdots p_t^{e_t}$, where p_i's are fixed distinct primes, and e_i's are arbitrary nonnegative integers. Then $\kappa(x^n-1) \geq C > 0$, where C is a constant independent of e_i's.*

Proof. Recall $\tau(p_i)$ is the order of q modulo p_i. Let $v_i \geq 1$ be given by $p_i^{v_i} \mid\mid \left(q^{\tau(p_i)}-1\right)$. Then

$$\tau(p_i^\ell) = \begin{cases} \tau(p_i) & \text{if } \ell \leq v_i, \\ p_i^{\ell - v_i}\tau(p_i) & \text{if } \ell > v_i. \end{cases}$$

This means that $\tau(p_i^\ell) = p_i^{\max\{\ell - v_i, 0\}}\tau(p_i)$.

An arbitrary divisor d of n is of the form $d = p_1^{d_1}p_2^{d_2}\cdots p_t^{d_t}$, with $0 \leq d_i \leq e_i$ for $1 \leq i \leq t$. Clearly, $\tau(d) = \mathrm{lcm}(\tau(p_1^{d_1}), \tau(p_2^{d_2}), \ldots, \tau(p_t^{d_t}))$, and is divisible by $\prod_{i=1}^t p_i^{\max\{d_i - v_i, 0\}}$. Thus

$$\tau(d) \geq \prod_{i=1}^t p_i^{\max\{d_i - v_i, 0\}}. \tag{11}$$

By (9), we have

$$\kappa(x^n - 1) = \prod_{\substack{d = p_1^{d_1}\cdots p_t^{d_t} \\ 0 \leq d_i \leq e_i,\ 1 \leq i \leq t}} \left(1 - q^{-\tau(d)}\right)^{\frac{\phi(d)}{\tau(d)}} \geq \prod_{\substack{d = p_1^{d_1}\cdots p_t^{d_t} \\ 0 \leq d_i \leq \infty,\ 1 \leq i \leq t}} \left(1 - q^{-\tau(d)}\right)^{\frac{\phi(d)}{\tau(d)}}.$$

Recalling that $\phi(d) = \prod_{i=1}^t p_i^{d_i - 1}(p_i - 1)$, and using (11), we obtain

$$\frac{\phi(d)}{\tau(d)} \leq \prod_{i=1}^t p_i^{v_i - 1}(p_i - 1) = C_1,$$

with C_1 a constant independent of e_i's. Then

$$\kappa(x^n - 1) \geq \left(\prod_{\substack{d = p_1^{d_1}\cdots p_t^{d_t} \\ 0 \leq d_i \leq \infty,\ 1 \leq i \leq t}} \left(1 - q^{-\tau(d)}\right)\right)^{C_1}.$$

By (11) and Lemma 3.2,

$$\prod_{\substack{d = p_1^{d_1}\cdots p_t^{d_t} \\ 0 \leq d_i \leq \infty,\ 1 \leq i \leq t}} \left(1 - q^{-\tau(d)}\right) \geq \prod_{0 \leq d_i \leq \infty,\ 1 \leq i \leq t} \left(1 - q^{-\prod_{i=1}^t p_i^{\max\{d_i - v_i, 0\}}}\right).$$

The last expression can be rewritten as

$$\begin{aligned}
& \prod_{\substack{0 \leq d_t \leq v_t \\ 0 \leq d_i \leq \infty,\ 1 \leq i \leq t-1}} \left(1 - q^{-\prod_{i=1}^{t-1} p_i^{\max\{d_i - v_i, 0\}}}\right) \prod_{\substack{d_t > v_t \\ 0 \leq d_i \leq \infty,\ 1 \leq i \leq t-1}} \left(1 - q^{-\prod_{i=1}^{t-1} p_i^{\max\{d_i - v_i, 0\}} p_t^{d_t - v_t}}\right) \\
\geq & \prod_{0 \leq d_i \leq \infty,\ 1 \leq i \leq t-1} \left(1 - q^{-\prod_{i=1}^{t-1} p_i^{\max\{d_i - v_i, 0\}}}\right)^{v_t + 1} \prod_{0 \leq d_i \leq \infty,\ 1 \leq i \leq t-1} \left(1 - q^{-\prod_{i=1}^{t-1} p_i^{\max\{d_i - v_i, 0\}}}\right) \\
= & \prod_{0 \leq d_i \leq \infty,\ 1 \leq i \leq t-1} \left(1 - q^{-\prod_{i=1}^{t-1} p_i^{\max\{d_i - v_i, 0\}}}\right)^{v_t + 2}.
\end{aligned}$$

Repeating this process successively for $d_{t-1}, d_{t-2}, \ldots, d_1$, we obtain

$$\kappa(x^n - 1) \geq \left(1 - q^{-1}\right)^{C_1(v_1+2)\cdots(v_t+2)} = \left(1 - q^{-1}\right)^{\prod_{i=1}^{t} p_i^{v_i - 1}(p_i-1)(v_i+2)} = C > 0,$$

where C is a constant independent of e_i's. This completes the proof. □

The estimates in the above proof are very rough. One can use finer estimates to get a bigger constant C. But we do not intend to do so in this paper. In addition, we note that, by Theorem 3.3, there exists an infinite tower of finite fields whose densities of normal elements are all larger than a constant.

3.2 Upper bounds

The results in Theorem 3.3 may suggest that $\kappa(x^n - 1) \geq C > 0$ for all n for some constant C. In this section, we show that this is not true. Indeed, we show that the lower bound of normal elements given by Theorem 2.1 is almost tight for infinitely many n.

By the proof of Theorem 2.1, $\kappa(f)$ is small if f contains all the linear factors, quadratic factors, and so on, up to all the irreducible polynomials of degree m. For such f, Giesbrecht (1993, Theorem 3.13) actually proves that

$$\Phi(f)/|f| \leq \frac{1}{e^{H_m}} \left(1 + \frac{1}{\sqrt{q}}\right)^{q/(q-1)}. \tag{12}$$

Thus $\kappa(f)$ approaches 0 as m goes to infinity. In the following theorem, we prove that a result similar to (12) holds even when f is restricted to polynomials of the type $x^n - 1$. We state the upper bound explicitly in term of the degree n.

Theorem 3.4 *For any integer $m > 1$, let $n = (q-1)(q^2-1)\cdots(q^m-1)$. Let $c_q = \frac{q}{(q-1)(\sqrt{q}-1)}$. Then*

$$\frac{1}{e^{0.83}(1 + \log_q n)} \leq \kappa(x^n - 1) \leq \frac{1}{e^{\gamma - c_q}\sqrt{1 + \log_q n}}.$$

Proof. The lower bound is in Theorem 2.1.

Note that $e \le \left(1-n^{-1}\right)^{-n}$, $n \ge 2$. It follows from this that, for a divisor d of n,

$$e \le \left(1-q^{-\tau(d)}\right)^{-q^{\tau(d)}}.$$

From

$$\left(1-q^{-\tau(d)}\right)^{\frac{\phi(d)}{\tau(d)}} = \left(\left(\left(1-q^{-\tau(d)}\right)^{-q^{\tau(d)}}\right)^{\frac{\phi(d)}{q^{\tau(d)}\,\tau(d)}}\right)^{-1},$$

we derive

$$\left(1-q^{-\tau(d)}\right)^{\frac{\phi(d)}{\tau(d)}} \le \left(\frac{1}{e}\right)^{\frac{\phi(d)}{q^{\tau(d)}\,\tau(d)}}.$$

Therefore, considering (9), we obtain

$$\kappa(x^n-1) \le \left(\frac{1}{e}\right)^{\sum_{d|n}\frac{\phi(d)}{q^{\tau(d)}\,\tau(d)}}. \tag{13}$$

We develop a lower bound for the above exponent.

$$\sum_{d|n}\frac{\phi(d)}{q^{\tau(d)}\,\tau(d)} \ge \sum_{k=1}^{m}\sum_{\substack{d|q^k-1\\ \tau(d)=k}}\frac{\phi(d)}{k\,q^k} = \sum_{k=1}^{m}\frac{I_k}{q^k}.$$

The inequality holds because the d in the second sum runs over only part of the divisors of n; the equality holds because, for fixed k, $\sum_{\substack{d|q^k-1\\ \tau(d)=k}}\phi(d)$ is the number of elements in $\mathbb{F}_{q^k}$ that have degree exactly k over $\mathbb{F}_q$, i.e., kI_k. By Lidl & Niederreiter (1983, Exercise 3.27),

$$I_k \ge \frac{q^k}{k} - \frac{q(q^{k/2}-1)}{k(q-1)}.$$

Thus

$$\begin{aligned}\sum_{d|n}\frac{\phi(d)}{q^{\tau(d)}\,\tau(d)} &\ge \sum_{k=1}^{m}\frac{I_k}{q^k} \ge \sum_{k=1}^{m}\frac{1}{k} - \frac{q}{q-1}\sum_{k=1}^{m}\frac{q^{k/2}-1}{kq^k} \ge H_m - \frac{q}{q-1}\sum_{k=1}^{m}\frac{1}{kq^{k/2}}\\ &\ge H_m - \frac{q}{q-1}\sum_{k=1}^{\infty}\left(\frac{1}{\sqrt{q}}\right)^k = H_m - \frac{q}{(q-1)(\sqrt{q}-1)} \ge \ln m + \gamma - c_q.\end{aligned}$$

Since $n=(q-1)(q^2-1)\cdots(q^m-1)$, we have

$$\log_q n = \sum_{i=1}^{m}\log_q(q^i-1) \le \sum_{i=1}^{m} i \le m^2-1,$$

i.e., $\ln m \geq \frac{1}{2}\ln(1+\log_q n)$. Therefore,

$$\sum_{d|n} \frac{\phi(d)}{q^{\tau(d)}\,\tau(d)} \geq \ln m + \gamma - c_q \geq \frac{1}{2}\ln(1+\log_q n) + \gamma - c_q.$$

Finally, using (13)

$$\kappa(x^n-1) \leq \left(\frac{1}{e}\right)^{\sum_{d|n}\frac{\phi(d)}{q^{\tau(d)}\,\tau(d)}} \leq \left(\frac{1}{e}\right)^{\frac{1}{2}\ln(1+\log_q n)+\gamma-c_q} = \frac{1}{e^{\gamma-c_q}\sqrt{1+\log_q n}}. \qquad \square$$

Conclusions. This paper provided lower bounds for $\kappa(\cdot)$ in general, and in the particular case of $\kappa(x^n-1)$. We slightly improved the previous known lower bounds for $\kappa(\cdot)$. Then, we focused on the particular case $\kappa(x^n-1)$ that gives the density of normal elements in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. It was shown that that $\kappa(x^n-1) \geq C > 0$ for $n = p_1^{e_1}p_2^{e_2}\cdots p_t^{e_t}$ where p_i's are fixed primes, e_i's vary, and C is a constant independent of e_i's. We also proved an upper bound on $\kappa(x^n-1)$ for infinitely many values of n that goes to 0 as n approaches infinity. This upper bound is almost tight with our lower bound for a general polynomial f.

References

[1] G.S. Frandsen, "Probabilistic construction of normal basis (note)", *DAIMI PB-361*, Computer Science Department, Aarhus University, Denmark, August 1991.

[2] J. von zur Gathen and M. Giesbrecht, "Constructing normal bases in finite fields", *J. Symbolic Computation*, **10** (1990), 547-570.

[3] M. Giesbrecht, *Nearly Optimal Algorithms for Canonical Matrix Forms*, Ph. D. Thesis, Technical Report 268/93, Department of Computer Science, University of Toronto, 1993.

[4] R. Graham, D.E. Knuth and O. Patashnik *Concrete Mathematics*, Addison-Wesley, Reading, MA, second edition 1994.

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

[6] A.J. Menezes, I.F. Blake, X. Gao, R.C. Mullin, S.A. Vanstone and T. Yaghoobian *Applications of Finite Fields*, Kluwer Academic Publishers, Boston/Dordrecht/Lancaster, 1993.

[7] O. Ore, "Contributions to the theory of finite fields", *Trans. Amer. Math. Soc.*, **36** (1934), 243-274".

[8] D. Wiedemann, "Solving sparse linear equations over finite fields", *IEEE Trans. Inform. Theory*, **32** (1986), 54–62.