Basic Research in Computer Science

On the Density of Normal Bases in Finite Fields

Gudmund Skovbjerg Frandsen

BRICS Report Series **RS-97-44**

ISSN 0909-0878 **December 1997**

See back inner page for a list of recent BRICS Report Series publications. Copies may be obtained by contacting:

BRICS
Department of Computer Science
University of Aarhus
Ny Munkegade, building 540
DK–8000 Aarhus C
Denmark
Telephone: +45 8942 3360
Telefax: +45 8942 3255
Internet: BRICS@brics.dk

BRICS publications are in general accessible through the World Wide Web and anonymous FTP through these URLs:

`http://www.brics.dk`
`ftp://ftp.brics.dk`
This document in subdirectory `RS/97/44/`

On the Density of Normal Bases in Finite Fields*

Gudmund Skovbjerg Frandsen

BRICS†
Department of Computer Science
University of Aarhus
Ny Munkegade
DK-8000 Aarhus C
DENMARK.
gudmund@brics.dk

Abstract

Let $\mathbb{F}_{q^n}$ denote the finite field with q^n elements, for q being a prime power. $\mathbb{F}_{q^n}$ may be regarded as an n-dimensional vector space over $\mathbb{F}_q$. $\alpha \in \mathbb{F}_{q^n}$ generates a *normal* basis for this vector space $(\mathbb{F}_{q^n} : \mathbb{F}_q)$, if $\{\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}\}$ are linearly independent over $\mathbb{F}_q$. Let $N(q,n)$ denote the number of elements in $\mathbb{F}_{q^n}$ that generate a normal basis for $\mathbb{F}_{q^n} : \mathbb{F}_q$, and let $\nu(q,n) = \frac{N(q,n)}{q^n}$ denote the frequency of such elements.

We show that there exists a constant $c > 0$ such that

$$\nu(q,n) \;\geq\; c\frac{1}{\sqrt{\lceil \log_q n \rceil}}, \qquad \text{for all } n, q \geq 2$$

and this is optimal up to a constant factor in that we show

$$0.28477 \;\leq\; \lim_{n\to\infty} \inf\; \nu(q,n)\sqrt{\log_q n} \;\leq\; 0.62521, \qquad \text{for all } q \geq 2$$

We also obtain an explicit lower bound:

$$\nu(q,n) \;\geq\; \frac{1}{e\lceil \log_q n \rceil}, \qquad \text{for all } n, q \geq 2$$

*Supported by the ESPRIT Long Term Research Programme of the EU, under project number 20244 (ALCOM-IT)

†Basic Research in Computer Science, Centre of the Danish National Research Foundation.

1 Introduction

When implementing arithmetic in a finite field $\mathbb{F}_{q^n}$, one may represent elements in $\mathbb{F}_{q^n}$ as n-vectors over $\mathbb{F}_q$. In this way addition becomes coefficient-wise addition on the n-vectors. Multiplication may be more or less difficult depending on the basis chosen. Any basis on the form $\{\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}\}$ where $\alpha \in \mathbb{F}_{q^n}$ is called a *normal* basis. When using a normal basis, raising to the q'th power is simply a cyclic shift of the coordinates in the vector representation. This has motivated an interest in normal bases.

According to the historical remarks in Bach and Shallit [1], Eisenstein [4] stated as early as 1850 that any finite field has a normal basis, and Hensel [7] published an explicit characterisation of the number of distinct normal bases in 1888. We describe the characterisation here, since our later analysis will build upon it. Our terminology is partly borrowed from Lidl and Niederreiter [9].

We need a function Φ_q that is an analogue of Euler's ϕ-function, but defined for polynomials over $\mathbb{F}_q$.

Definition 1 *For $f \in \mathbb{F}_q[x]$, define $\Phi_q(f)$ to be the number of polynomials $g \in \mathbb{F}_q[x]$ such that (i) $\deg(g) < \deg(f)$ and (ii) $\gcd(f, g) = 1$.*

Let $N(q, n)$ denote the number of elements in $\mathbb{F}_{q^n}$ that generate a normal basis for $\mathbb{F}_{q^n} : \mathbb{F}_q$. The characterisation is $N(q, n) = \Phi_q(x^n - 1)$.

The bounds $c\frac{n}{\ln \ln n} \leq \phi(n) \leq n$ on Eulers ϕ-function are wellknown. There are similar bounds on $\Phi_q(f)$. The upper bound $\Phi_q(f) \leq q^n$ is trivial and in Section 2, we prove the lower bound:

Theorem 2 *For any finite field $\mathbb{F}_q$ and for any polynomial $f \in \mathbb{F}_q[x]$ of degree $n \geq 2$ and such that $f(0) \neq 0$, we have*

$$\Phi_q(f) \geq \frac{q^n}{e\lceil \log_q n \rceil}.$$

In particular, the theorem translates to a bound on the frequency $\nu(q, n)$ of normal basis elements for $\mathbb{F}_{q^n} : \mathbb{F}_q$, since $\nu(q, n) = \frac{N(q,n)}{q^n} = \Phi_q(x^n - 1) \cdot q^{-n} \geq \frac{1}{e\lceil \log_q n \rceil}$.

This result improves the lower bound on $\nu(q, n)$ given by von zur Gathen and Giesbrecht [11] by a constant factor.

However, there is an asymptotically stronger bound for $\Phi_q(x^n - 1)$. In Section 3, we prove the following result:

Theorem 3 *There is a constant c_1 such that*

$$\nu(q,n) \geq .28477 \frac{1}{\sqrt{\log_q n}}, \quad \text{for all } q \geq 2 \text{ and } n \geq q^{c_1}.$$

Combining this asymptotic bound with the simple bound $\nu(q,n) \geq \frac{1}{e\lceil \log_q n \rceil}$ for all q, n leads to an absolute bound:

Corollary 4 *There is a constant c such that*

$$\nu(q,n) \geq c \frac{1}{\sqrt{\lceil \log_q n \rceil}}, \quad \text{for all } q, n \geq 2.$$

In Section 4, we show the preceding result to be optimal in that

Theorem 5 *For every primepower q,*

$$\nu(q,n) < .62521 \frac{1}{\sqrt{\log_q n}}, \quad \text{for infinitely many } n.$$

2 A general lower bound for $\Phi_q(f)$

We will use a multiplicative characterisation of $\Phi_q(f)$. Let $f \in \mathbb{F}_q[x]$ with $f(0) \neq 0$ have the complete factorisation $f = \prod_{i=1}^{t} f_i^{e_i}$ over $\mathbb{F}_q$ (i.e. the irreducible factors f_i, f_j are distinct, when $i \neq j$). Then

$$\Phi_q(f) \;=\; q^n \cdot \prod_{i=1}^{t} (1 - \frac{1}{q^{n_i}}), \tag{1}$$

where n_i is the degree of f_i, and $n \geq 1$ is the degree of f (see [9] for a proof).

From (1), we see that $\Phi_q(f)$ only depends on the number of distinct irreducible factors f has of each degree. We introduce some useful notation:

Definition 6 *Let* $\mathrm{Irr}(q,d)$ *denote the number of monic irreducible polynomials $g \in \mathbb{F}_q[x]$, such that (i) g has degree d and (ii) $g(0) \neq 0$.*

Let $\mathrm{Irr}(q,d;f)$ *denote the number of monic irreducible polynomials $g \in \mathbb{F}_q[x]$, such that (i) g has degree d, (ii) $g(0) \neq 0$ and (iii) g divides f.*

In this notation, (1) translates into

$$\Phi_q(f) \;=\; q^n \cdot \prod_{d=1}^{n} (1 - \frac{1}{q^d})^{\mathrm{Irr}(q,d;f)}. \tag{2}$$

Clearly,

$$\deg(f) \geq \sum_{d=1}^{n} d \cdot \mathrm{Irr}(q,d;f), \tag{3}$$

and equality holds precisely, when f is square free. At this point, we observe that for a fixed $n = \deg(f)$, the minimal value of $\Phi_q(f)$ occurs, when f has as many distinct small degree factors as allowed by (3); i.e. if k is any integer such that $\deg(f) \leq 1 + \sum_{d=1}^{k} d \cdot \mathrm{Irr}(q,d)$, then

$$\Phi_q(f) \;\geq\; q^n \cdot \prod_{d=1}^{k} (1 - \frac{1}{q^d})^{\mathrm{Irr}(q,d)}. \tag{4}$$

To bound the right hand side of (4), we need upper bounds on both $\mathrm{Irr}(q,d)$ and possible values for k. It is known (see Lidl and Niederreiter [9]) that

$$q^k - 1 = \sum_{d|k} d \cdot \mathrm{Irr}(q,d). \tag{5}$$

From (5), we see that $n \leq 1 + \sum_{d=1}^{k} d \cdot \mathrm{Irr}(q,d)$ for $k = \lceil \log_q n \rceil$. It is also implied that

$$\mathrm{Irr}(q,d) \leq \frac{q^d - 1}{d}. \tag{6}$$

Combining with (4), we find

$$\Phi_q(f) \;\geq\; q^n \cdot \prod_{d=1}^{\lceil \log_q n \rceil} (1 - \frac{1}{q^d})^{\frac{q^d-1}{d}}. \tag{7}$$

Using that $(1 - \frac{1}{c})^{c-1} \geq \frac{1}{e}$, for $c > 1$, this can be rephrased to

$$\Phi_q(f) \;\geq\; q^n \cdot e^{-\sum_{d=1}^{\lceil \log_q n \rceil} \frac{1}{d}}, \tag{8}$$

and using that $\frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{k} \leq \ln k$, we finally get

$$\Phi_q(f) \;\geq\; q^n \cdot \frac{1}{e\lceil \log_q n \rceil}. \tag{9}$$

Remark. The above bound is only valid for polynomials f for which $f(0) \neq 0$. When changing the argument to general f, one needs to consider the irreducible polynomial x of degree 1, implying that the value of $\mathrm{Irr}(q,1)$ increases by 1. The above analysis can be adjusted to this case resulting in the slightly worse bound $\Phi_q(f) \geq q^n \cdot \frac{1}{4\lceil \log_q n \rceil}$.

3 A stronger lower bound for $\Phi_q(x^n - 1)$

In our proof of the lower bound for $\Phi_q(f)$, f being arbitrary, we considered a worst case, where all irreducible polynomials of small degree were factors of f. Intuitively, one might hope that $x^n - 1$ would never factorise in that way, i.e. for every n there would be a lot of small degree polynomials that did not divide

$x^n - 1$. This intuition turns out to be true, and when stated in a suitably formal manner it suffices to prove the stronger bound of Theorem 3.

From (6), we know that $\mathrm{Irr}(q, d; x^n - 1) \leq \frac{q^d-1}{d}$. We will divide the possible degrees d in two sets according to whether $\mathrm{Irr}(q, d; x^n - 1)$ has a value close to this upper bound or not.

Definition 7 *Let $A_{n,q}$ be the set of those degrees $d \in \{1, \ldots, n\}$ for which*

$$\mathrm{Irr}(q, d; x^n - 1) > \frac{q^d - 1}{d^3}.$$

Let $B_{n,q}$ be the set of those degree $d \in \{1, \ldots, n\}$ for which

$$\mathrm{Irr}(q, d; x^n - 1) \leq \frac{q^d - 1}{d^3}.$$

We can basically ignore the contribution from degrees in $B_{n,q}$:

Lemma 8

$$\nu(n, q) \geq \begin{cases} e^{-\zeta(3)} \approx .30058, & \text{for } A_{n,q} = \emptyset, \\ e^{-\gamma} \cdot e^{-\frac{1}{|A_{n,q}|}} \frac{1}{|A_{n,q}|}, & \text{for } A_{n,q} \neq \emptyset, \end{cases}$$

where γ denotes Euler's constant, and ζ is Riemann's function.

Proof. With arguments analogous to those used in section 2, we obtain a bound:

$$\begin{aligned} \nu(n, q) &= \Phi_q(x^n - 1) \cdot q^{-n} \\ &\geq \prod_{d \in A_{n,q}} (1 - \frac{1}{q^d})^{\frac{q^d-1}{d}} \cdot \prod_{d \in B_{n,q}} (1 - \frac{1}{q^d})^{\frac{q^d-1}{d^3}} \\ &\geq e^{-\sum_{d \in A_{n,q}} \frac{1}{d}} \cdot e^{-\sum_{d \in B_{n,q}} \frac{1}{d^3}} \\ &\geq e^{-\sum_{d=1}^{|A_{n,q}|} \frac{1}{d}} \cdot e^{-\sum_{d=|A_{n,q}|+1}^{n} \frac{1}{d^3}} \end{aligned}$$

In the case of $A_{n,q} = \emptyset$, we use the fact that $\sum_{d=1}^{\infty} \frac{1}{d^3} = \zeta(3)$, to get the bound

$$\nu(n, q) \geq e^{-\zeta(3)} \approx .30058$$

In the case of $A_{n,q} \neq \emptyset$, we use the two inequalities $\sum_{d=1}^{s} \frac{1}{d} \leq \ln s + \gamma + \frac{1}{2s}$ and $\sum_{d=s+1}^{\infty} \frac{1}{d^3} \leq \frac{1}{2s^2}$, to get the bound

$$\nu(n, q) \geq e^{-\gamma} \cdot e^{-\frac{1}{|A_{n,q}|}} \frac{1}{|A_{n,q}|}.$$

■

Our next task is to find an upper bound on $|A_{n,q}|$. We will do that implicitly by expressing a lower bound for n in terms of $|A_{n,q}|$. We start by improving the simple bound $\mathrm{Irr}(q, d; x^n - 1) \leq \frac{q^d-1}{d}$:

Lemma 9

$$\mathrm{Irr}(q, d; x^n - 1) \leq \frac{\gcd(q^d - 1, n)}{d}.$$

Proof. Let the monic irreducible polynomial $g \in \mathbb{F}_q[x]$ of degree d be a factor of $x^n - 1$, and let α be a root of g.

Since g divides $x^n - 1$ it follows that $\alpha^n = 1$. Since g is irreducible, of degree d, it follows that $\alpha \in \mathbb{F}_{q^d}$ and therefore $\alpha^{q^d - 1} = 1$. Combining, we get that $\alpha^{\gcd(q^d-1,n)} = 1$. Since there are at most k distinct k'th roots of unity in a field, we see that there are at most $\gcd(q^d - 1, n)$ distinct possible α's. Because g has precisely d distinct roots, and distinct g's have no common roots, there are at most $\gcd(q^d - 1, n)/d$ possible g's. ■

Combining this result with the lower bound $\mathrm{Irr}(q, d; x^n - 1) > \frac{q^d-1}{d^3}$ implied by $d \in A_{q,n}$, we can get our first lower bound on n.

Lemma 10

$$n \geq \frac{lcm_{d \in A_{q,n}}(q^d - 1)}{\prod_{d \in A_{q,n}}(d^2)}$$

Proof. Assume $d \in A_{q,n}$. Combining the definition of $A_{q,n}$ with Lemma 9, we see that $\frac{q^d-1}{d^3} \leq \frac{\gcd(q^d-1,n)}{d}$, or equivalently, $\gcd(q^d - 1, n) \geq \frac{q^d-1}{d^2}$. One may interpret this bound to say that n contains $q^d - 1$ as a factor except possibly for something very small (bounded by d^2). Since this is true for any $d \in A_{q,n}$, we see that n contains the least common multiple of the $(q^d - 1)$'s as a factor except possible for something small (bounded by the product of the d's squared). ■

The next step will be to phrase the preceding bound in terms of $|A_{q,n}|$.

Lemma 11 *Let A be a finite set of natural numbers, let $k = |A|$, and let q be a prime power, then*

$$\frac{lcm_{d \in A}(q^d - 1)}{\prod_{d \in A}(d^2)} \geq q^{ck^2 - o(k^2)}$$

where $c = \frac{\zeta(6)}{2\zeta(2)\zeta(3)} \approx .25726$.

Proof. The proof will consist in combining three lemmas that we state and prove separately in Section 5.

Let $C_n \in \mathbb{Q}[z]$ denote the nth cyclotomic polynomial. From Lemma 16 we have

$$\mathrm{lcm}_{d \in A}(q^d - 1) \;=\; \prod_{\{e \;|\exists d \in A \text{ such that } e \text{ divides } d\}} C_e(q) \;\geq\; \prod_{d \in A} C_d(q).$$

For ϕ denoting Euler's ϕ-function, we get in addition by Lemma 17

$$\mathrm{lcm}_{d\in A}(q^d-1) \;\geq\; \prod_{d\in A} q^{\phi(d)-2}.$$

Combining this calculation with Lemma 19, we find

$$\begin{aligned}\frac{\mathrm{lcm}_{d\in A}(q^d-1)}{\prod_{d\in A}(d^2)} &\geq q^{\sum_{d\in A}(\phi(d)-2\log_2 d-2)}\\ &\geq q^{ck^2-o(k^2)}.\end{aligned}$$

■

Proof of Theorem 3. In the case of $A_{q,n}=\emptyset$, it suffices by lemma 8 to note that $e^{-\zeta(3)}\approx .30058 > .28477$.

In the case of $A_{q,n}\neq\emptyset$, we combine Lemmas 10 and 11, and find

$$\log_q n \;\geq\; c|A_{q,n}|^2 - o(|A_{q,n}|^2) \tag{10}$$

for $c=\frac{\zeta(6)}{2\zeta(2)\zeta(3)}$. This may be reformulated as follows: For all $c'<c$ there exists $c''>0$, such that for all $n\geq q^{c''}$:

$$|A_{q,n}| \leq \frac{1}{\sqrt{c'}}\sqrt{\log_q n}$$

Combining this with Lemma 8 and the fact that $e^{-\frac{1}{x}}\to 1$ for $x\to\infty$, we see that for any $c'<c$ we can find c'', such that for all $n\geq q^{c''}$, we have

$$\nu(q,n) \;\geq\; e^{-\gamma}\sqrt{c'}\frac{1}{\sqrt{\log_q n}} \tag{11}$$

The statement of the theorem follows from noting that $e^{-\gamma}\sqrt{c} > .28477$. ■

4 Optimality of the lower bound on $\Phi_q(x^n-1)$

It will be argued that the lower bound of Theorem 3 is optimal up to a constant factor. The proof will consist in constructing an infinite sequence $\{n_k\}_{k=1}^{\infty}$ such that $\mathbb{F}_{q^n}:\mathbb{F}_q$ has exceptionally few normal bases for $n\in\{n_k\}$. The sequence $\{n_k\}$ will depend on q. Each number n_k will have the property that all irreducible polynomials of degrees at most k divides $x^{n_k}-1$ (except for the irreducible polynomial x that can never divide any polynomial of the form x^n-1).

Definition 12 *For a given prime power q, define the infinite sequence $\{n_k\}_{k=1}^{\infty}$ by*

$$n_k = lcm_{d=1}^{k}(q^d-1)$$

This definition serves our purpose in that

Lemma 13 *For n_k as defined above,* $\mathrm{Irr}(q,d;x^{n_k}-1) = \mathrm{Irr}(q,d)$ *for all* $d \leq k$.

Proof. Every irreducible polynomial of degree d divides $x^{q^d-1}-1$ (as usual we make an exception for the irreducible polynomial x) (see Lidl and Niederreiter [9]), and since x^a-1 divides $x^{ab}-1$ for any positive integers a, b, we also have that $x^{q^d-1}-1$ divides $x^{n_k}-1$. ■

The size of n_k is also kept fairly small:

Lemma 14 *For all prime powers q, for all integers $k > 0$, and with n_k as defined above, it is the case that*

$$\log_q n_k = ck^2 + O(k \log k),$$

where $c = \frac{1}{2\zeta(2)} = \frac{3}{\pi^2} \approx .30396$

Proof. By lemma 16, we may express n_k in terms of cyclotomic polynomials

$$n_k \;=\; \prod_{d=1}^{k} C_d(q).$$

When using Lemma 17 to bound $C_d(q)$ in terms of Euler's ϕ-function and taking logarithms on both sides, we find

$$\log_q n_k \;=\; \sum_{d=1}^{k} \phi(d) + O(k).$$

The value of the accumulated sum of the ϕ-function is known (see Lemma 20), and we have

$$\log_q n_k \;=\; ck^2 + O(k \log k).$$

■

We will first find a bound on $\nu(n_k, q)$ in terms of k and then combine this with the previous bound on k in terms of n_k.

Lemma 15

$$\nu(n_k, q) \leq 1.1340 \cdot \frac{1}{k}.$$

Proof. Using the multiplicative characterisation of Φ from section 2, we find that

$$\nu(n_k, q) \;=\; \prod_{d=1}^{n_k} (1 - \frac{1}{q^d})^{\mathrm{Irr}(q,d,x^{n_k}-1)}.$$

By Lemma 13, the dependence of n_k can be restricted to the occurrence of k in the multiplication bound:

$$\nu(n_k, q) \;\leq\; \prod_{d=1}^{k} (1 - \frac{1}{q^d})^{\mathrm{Irr}(q,d)}.$$

To get the bound of the lemma, we show that

$$\prod_{d=1}^{l} (1 - \frac{1}{q^d})^{\mathrm{Irr}(q,d)} \;\leq\; 1.08\frac{1}{l} \qquad \text{for } l \leq 12 \tag{12}$$

and

$$\prod_{d=l+1}^{k} (1 - \frac{1}{q^d})^{\mathrm{Irr}(q,d)} \;\leq\; 1.05 \cdot \frac{l}{k} \qquad \text{for } l \geq 12. \tag{13}$$

Clearly, inequalities (12) and (13) combined imply the lemma. (12) may be verified by an explicit calculation using that $q \geq 2$, $\mathrm{Irr}(q,1) = q-1$, $\mathrm{Irr}(q,2) = (q^2-q)/2$, $\mathrm{Irr}(q,3) = (q^3-q)/3$, $\mathrm{Irr}(q,4) = (q^4-q^2)/4$ etc. (details are omitted for technical simplicity). To prove (13), we use that $(1-\frac{1}{c})^c \leq \frac{1}{e}$ for $c > 1$, and find that

$$\prod_{d=l+1}^{k} (1 - \frac{1}{q^d})^{\mathrm{Irr}(q,d)} \;\leq\; e^{-\sum_{d=l+1}^{k} \mathrm{Irr}(q,d)/q^d}.$$

It is well known (see Lidl and Niederreiter [9]) that (for $d \geq 2$ only, since we exclude the degree 1 polynomium x)

$$\mathrm{Irr}(q,d) = \frac{1}{d} \sum_{e|d} \mu(e) q^{d/e}.$$

This implies in particular that (for $d, q \geq 2$)

$$\mathrm{Irr}(q,d)/q^d \geq \frac{1}{d} - \frac{2}{d}(\sqrt{2})^{-d}.$$

Using the elementary inequalities $\sum_{d=l+1}^{k} \frac{1}{d} \geq \ln \frac{k}{l} - \frac{1}{2l}$ and $\sum_{d=l+1}^{k} \frac{2}{d}(\sqrt{2})^{-d} \leq \frac{2}{l+1}\frac{1}{\sqrt{2}-1}(\sqrt{2})^{-l}$ combined with the inequality

$$e^{\frac{1}{2l} + \frac{2}{l+1}\frac{1}{\sqrt{2}-1}(\sqrt{2})^{-l}} \leq 1.05 \quad \text{for } l \geq 12,$$

we obtain (13). ■

Proof of Theorem 5. From Lemma 14, we have that $c \cdot \frac{1}{\sqrt{\log_q n_k}} \geq \frac{1}{k}$ for infinitely many k for any $c > 1/\sqrt{2\zeta(2)} < .55133$. Combining with Lemma 15, we see that $\nu(q,n) \leq .55133 \cdot 1.1340 \cdot \frac{1}{\sqrt{\log_q n}}$ for infinitely many n. ■

5 Auxiliary results

Lemma 16 *Let A be a finite set of natural numbers, let q be a prime power, and let $C_n(z)$ denote the n^{th} cyclotomic polynomial. Then*

$$lcm_{d\in A}(q^d-1) = \prod_{\{e\ |\exists d\in A \text{ such that } e \text{ divides } d\ \}} C_e(q).$$

Proof. Let $C_n(z)$ denote the nth cyclotomic polynomial. It is known that $C_n(z)$ is irreducible over the field $\mathbb{Q}$ and that $z^d-1=\prod_{e|d} C_e(z)$ (see Hungerford [8, Prop. 8.2 and Prop 8.3]). In particular this implies

$$\gcd_{d\in A}(z^d-1) = \prod_{e|\gcd_{d\in A}(d)} C_e(z) = z^{\gcd_{d\in A}(d)}-1 \tag{14}$$

and

$$\operatorname{lcm}_{d\in A}(z^d-1) = \prod_{\{e\ |\exists d\in A \text{ such that } e \text{ divides } d\ \}} C_e(z). \tag{15}$$

It might be tempting to substitute q for z in (15) and call it a proof of the lemma. However, the validity of such substitution needs a careful argument. To see this, observe that it fails in a rather similar looking situation: Using that $C_2(z)=z+1$ and $C_6(z)=z^2-z+1$, we see that $\operatorname{lcm}(C_2(z),C_6(z))=C_2(z)\cdot C_6(z)$. However, $\operatorname{lcm}(C_2(2),C_6(2))=\operatorname{lcm}(3,3)=3\neq 9=C_2(2)\cdot C_6(2)$. The reason for this failure is of course that the "lcm" in (15) is taken in the polynomial ring $\mathbb{Q}[z]$, whereas the "lcm" of the lemma must be taken in the integer ring $\mathbb{Z}$. We therefore need a more elaborate argument.

For both $\mathbb{Q}[z]$ and $\mathbb{Z}$, the following generalisation of the classical formula $\operatorname{lcm}(x,y)=xy/\gcd(x,y)$ is valid (Marsh [10]). Let M be a finite subset of either $\mathbb{Q}[z]$ or $\mathbb{Z}$:

$$\operatorname{lcm}_{m\in M}(m) = \frac{\prod_{I\subseteq M,|I| \text{ odd}} \gcd_{m\in I}(m)}{\prod_{I\subseteq M,|I| \text{ even}} \gcd_{m\in I}(m)}. \tag{16}$$

This formula tells us that the least common multiple of a set of numbers M (or set of polynomials) is determined uniquely from the gcd's of all possible subsets of M. This means that if substitution of q for z is always valid in (14), then it is also always valid to substitute q for z in (15). Hence, we need only prove

$$\gcd_{d\in A}(q^d-1) = q^{\gcd_{d\in A}(d)}-1, \tag{17}$$

which follows from observing that a prime power p^k divides q^d-1 precisely when the order of q (modulo p^k) divides d. ∎

Lemma 17 *Let n be a natural number, let q be a prime power, and let $C_n(z)$ denote the n^{th} cyclotomic polynomial. Then*

$$\frac{1}{4}q^{\phi(n)} \;\leq\; C_n(q) \;\leq\; 4q^{\phi(n)}$$

where ϕ denotes Euler's ϕ-function.

Proof. The nth cyclotomic polynomial $C_n(z)$ is monic of degree $\phi(n)$. One might therefore expect $C_n(q)$ to have a value not far from $q^{\phi(n)}$. To prove the bound of the lemma, we will use the multiplicative characterisation

$$C_n(z) = \prod_{d|n}(z^{n/d} - 1)^{\mu(d)}, \tag{18}$$

where μ denotes the Möbius function. We will also need a corresponding characterisation of ϕ (see Hardy and Wright [6]):

$$\phi(n) = \sum_{d|n}\mu(d)\frac{n}{d}. \tag{19}$$

Exponentiating with base q on both sides of (19) and combining with (18), where q is substituted for z, we find

$$C_n(q) = q^{\phi(n)}\prod_{d|n}(1 - \frac{1}{q^{n/d}})^{\mu(d)}. \tag{20}$$

To bound the size of the right factor in (20), we use that $\mu(d) \in \{-1, 0, 1\}$ and therefore

$$\prod_{d|n}(1 - \frac{1}{q^{n/d}})^{\mu(d)} \geq \prod_{d|n}(1 - \frac{1}{q^{n/d}}) \geq \prod_{i=1}^{\infty}(1 - \frac{1}{q^i}). \tag{21}$$

If we take the natural logarithm and use that $\ln(1-s) \geq s\ln\frac{1}{4}$ for $0 \leq s \leq \frac{1}{2}$, we find (for $q \geq 2$)

$$\ln\left(\prod_{i=1}^{\infty}(1 - \frac{1}{q^i})\right) \geq (\ln\frac{1}{4})\sum_{i=1}^{\infty}\frac{1}{q^i} \geq \ln\frac{1}{4},$$

from which it follows that $C_q(n) \geq \frac{1}{4}q^{\phi(n)}$. The upper bound on $C_q(n)$ is proved similarly. ■

Lemma 18 *Let A be a finite set of natural numbers, let $k = |A|$, and let ϕ denote Euler's ϕ-function, then*

$$\sum_{d\in A}\phi(d) \geq ck^2 - o(k^2)$$

where $c = \frac{\zeta(6)}{2\zeta(2)\zeta(3)} \approx .25726$.

Proof. The lower bound on $\sum_{d\in A}\phi(d)$ relies on using Dressler's result that only few integers are mapped to small values by ϕ. To state it formally, we define $M_n = \{x \in \mathbb{N} | \phi(x) \leq n\}$. Dressler [3] proved (see also Erdös [5] and Bateman [2]):

$$|M_n| = c'n + o(n) \quad \text{for } c' = \frac{\zeta(2)\zeta(3)}{\zeta(6)} \approx 1.9436. \tag{22}$$

It is clear that if A has the form M_n for some n, then $\sum_{d\in A}\phi(d)$ is minimised (with respect to a fixed $|A|$). Therefore choose l maximal such that $|M_l| \leq |A|$, and we have

$$\sum_{d\in A}\phi(d) \geq \sum_{d\in M_l}\phi(d) \tag{23}$$

In order to lower bound the latter sum, we observe that $\phi(d) = n$ for $d \in M_n - M_{n-1}$, implying that

$$\begin{aligned}\sum_{d\in M_n}\phi(d) &= \sum_{i=1}^{n} i(|M_i| - |M_{i-1}|) \\ &= n\cdot|M_n| - \sum_{i=1}^{n-1}|M_i|.\end{aligned}$$

Combining with (22), we get

$$\sum_{d\in M_n}\phi(d) = n\cdot c'n - \sum_{i=1}^{n-1} c'i + o(n^2) \tag{24}$$

$$= \frac{c'}{2}n^2 + o(n^2). \tag{25}$$

Finally, combining the definition of l with (22), we see that $l = \frac{1}{c'}|A| + o(|A|)$, which combined with (23) and (25) leads to

$$\sum_{d\in A}\phi(d) \geq \frac{1}{2c'}|A|^2 - o(|A|^2).$$

■

Lemma 19 *Let A be a finite set of natural numbers, let $k = |A|$, and let ϕ denote Euler's ϕ-function, then*

$$\sum_{d\in A}(\phi(d) - 2\log_2 d) \geq ck^2 - o(k^2)$$

where $c = \frac{\zeta(6)}{2\zeta(2)\zeta(3)} \approx .25726$.

Proof. This lemma is a technical variation of Lemma 18. The proof of the latter lemma also applies here, except that we need in addition to argue that $\sum_{d\in A} \log_2 d$ is bounded by $o(k^2)$. In the following, use the terminology from the proof of Lemma 18.

It is known that $\phi(n) = \Omega(\frac{n}{\ln\ln n})$ (see Hardy and Wright [6]), which implies that $\log_2 d \leq 2\log_2 \phi(d)$ for d sufficiently large. We therefore get the following modified version of (23)

$$\sum_{d\in A}(\phi(d) - 2\log_2 d) \quad \geq \quad \sum_{d\in M_l} \phi(d) - 4\sum_{d\in M_l} \log_2 \phi(d) - O(1). \tag{26}$$

Using that $\phi(d) \leq d$, it follows from the definition of l that $\sum_{d\in M_l} \log \phi(d) = O(|A|\log|A|)$, which combined with (26) and the proof of Lemma 18 implies

$$\sum_{d\in A}(\phi(d) - 2\log_2 d) \quad \geq \quad \frac{1}{2c'}|A|^2 - o(|A|^2).$$

■

Lemma 20 *Let ϕ denote Euler's ϕ-function, then*

$$\sum_{d=1}^{k} \phi(d) = ck^2 + O(k\log k)$$

where $c = \frac{1}{2\zeta(2)} \approx .30396$.

Proof. This is well known, see Hardy and Wright [6].

References

[1] Erik Bach and Jeffrey Shallit. *Algorithmic Number Theory. Volume I: Efficient algorithms.* MIT Press, 1996.

[2] Paul T. Bateman. The distribution of values of the Euler function. *Acta Arith.* **21** (1972), 329–345.

[3] Robert E. Dressler. A density which counts multiplicity. *Pacific J. Math.* **34** (1970), 371–378.

[4] G. Eisenstein. Lehrsätze. *J. Reine Angew. Math.* **39** (1850), 180–182.

[5] Paul Erdös. Some remarks on Euler's ϕ-function and some related problems. *Bull. Amer. Math. Soc.* **51** (1945), 540–544.

[6] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers. (Third Edition).* Oxford University Press, 1954.

[7] K. Hensel. Ueber die Darstellung der Zahlen eines Gattungsbereiches für einen beliebigen Primdivisor. *J. Reine Angew. Math.* **103** (1888), 230–237.

[8] Thomas W. Hungerford. *Algebra.* Springer-Verlag, 1974.

[9] R. Lidl and H. Niederreiter. *Finite Fields*, Vol. 20 of *Encyclopedia of Mathematics and its Applications.* Addison Wesley, 1983.

[10] D. C. B. Marsh. Solution to problem E 2229. *Amer. Math. Monthly* **78** (1971), 299.

[11] Joachim von zur Gathen and Mark Giesbrecht. Constructing normal bases in finite fields. *J. Symbolic Computation* **10** (1990), 547–570.

Recent BRICS Report Series Publications

RS-97-44 **Gudmund Skovbjerg Frandsen.** ***On the Density of Normal Bases in Finite Fields*****. December 1997. 14 pp.**

RS-97-43 **Vincent Balat and Olivier Danvy.** ***Strong Normalization by Run-Time Code Generation*****. December 1997.**

RS-97-42 **Ulrich Kohlenbach.** ***On the No-Counterexample Interpretation*****. December 1997. 26 pp.**

RS-97-41 **Jon G. Riecke and Anders B. Sandholm.** ***A Relational Account of Call-by-Value Sequentiality*****. December 1997. 24 pp. Appears in** ***Twelfth Annual IEEE Symposium on Logic in Computer Science,*** **LICS '97 Proceedings, pages 258–267.**

RS-97-40 **Harry Buhrman, Richard Cleve, and Wim van Dam.** ***Quantum Entanglement and Communication Complexity*****. December 1997. 14 pp.**

RS-97-39 **Ian Stark.** ***Names, Equations, Relations: Practical Ways to Reason about 'new'*****. December 1997. ii+33 pp. This supersedes the earlier BRICS Report RS-96-31. It also expands on the paper presented in Groote and Hindley, editors,** ***Typed Lambda Calculi and Applications: 3rd International Conference,*** **TLCA '97 Proceedings, LNCS 1210, 1997, pages 336–353.**

RS-97-38 **Michał Hańćkowiak, Michał Karoński, and Alessandro Panconesi.** ***On the Distributed Complexity of Computing Maximal Matchings*****. December 1997. 16 pp. To appear in** ***The Ninth Annual ACM-SIAM Symposium on Discrete Algorithms,*** **SODA '98.**

RS-97-37 **David A. Grable and Alessandro Panconesi.** ***Fast Distributed Algorithms for Brooks-Vizing Colourings (Extended Abstract)*****. December 1997. 20 pp. To appear in** ***The Ninth Annual ACM-SIAM Symposium on Discrete Algorithms,*** **SODA '98.**

RS-97-36 **Thomas Troels Hildebrandt, Prakash Panangaden, and Glynn Winskel.** ***Relational Semantics of Non-Deterministic Dataflow*****. December 1997. 21 pp.**

RS-97-35 **Gian Luca Cattani, Marcelo P. Fiore, and Glynn Winskel.** ***A Theory of Recursive Domains with Applications to Concurrency*****. December 1997. ii+23 pp.**