Serdica J. Computing **2** (2008), 239–248

Serdica
Journal of Computing

Bulgarian Academy of Sciences
Institute of Mathematics and Informatics

ON THE ASYMPTOTIC BEHAVIOR OF THE RATIO BETWEEN THE NUMBERS OF BINARY PRIMITIVE AND IRREDUCIBLE POLYNOMIALS[*]

Yuri Borissov, Moon Ho Lee, Svetla Nikova

Abstract. In this paper, we study the ratio $\theta(n) = \dfrac{\lambda_2(n)}{\psi_2(n)}$, where $\lambda_2(n)$ is the number of primitive polynomials and $\psi_2(n)$ is the number of irreducible polynomials in $GF(2)[x]$ of degree n. Let $n = \prod\limits_{i=1}^{\ell} p_i^{r_i}$ be the prime factorization of n. We show that, for fixed l and r_i, $\theta(n)$ is close to 1 and $\theta(2n)$ is not less than $2/3$ for sufficiently large primes p_i. We also describe an infinite series of values n_s such that $\theta(n_s)$ is strictly less than $\dfrac{1}{2}$.

1. Introduction. One of the most fascinating areas of research in the theory of finite fields is the problem of finding irreducible and primitive polynomials (or elements), and even the problem of the existence of such kind of polynomials with specified properties has attracted a great deal of attention. Many

ACM Computing Classification System (1998): F.2.1.

Key words: finite fields, primitive and irreducible polynomials.

[*] This work was presented in part at the 8th International Conference on Finite Fields and Applications $\mathbf{F_{q^8}}$, Melbourne, Australia, 9-13 July, 2007.

authors have published works on this subject (see [3–10, 12, 14–19, 22]) and the list might not be complete. It is a folklore fact that "the number of binary primitive polynomials of given degree is on the same order of magnitude as the number of irreducible polynomials" (see e.g. [11]). In this paper, we try to substantiate the above claim by proving a few facts about the ratio between aforementioned numbers. Our results can also be interpreted probabilistically: to estimate the probability for a randomly chosen irreducible polynomial in $GF(2)[\mathbf{x}]$ of given degree to be primitive.

The paper is organized as follows. In the first section we recall basic definitions, facts and useful properties. In the next two sections we present our main results. The paper ends with some conclusions.

2. Background.

In this paper, we consider polynomials of one variable $\mathbf{x}$ over a finite field. Here, for the sake of completeness, we briefly recall some basic definitions and facts about polynomials in $GF(q)[\mathbf{x}]$, where $GF(q)$ is the Galois field of q elements (see, e.g., [13, 21]).

Definition 1. *A polynomial $f(\mathbf{x})$ is irreducible in $GF(q)[\mathbf{x}]$ if $f(\mathbf{x})$ cannot be factored into a product of lower-degree polynomials in $GF(q)[\mathbf{x}]$.*

It can be shown that any irreducible nth-degree polynomial in $GF(q)[\mathbf{x}]$ divides $\mathbf{x}^{q^n-1} - 1$.

Definition 2. *An irreducible polynomial $f(\mathbf{x}) \in \mathbf{GF(q)}[\mathbf{x}]$ of degree n is said to be primitive if the smallest positive integer m for which $f(\mathbf{x})$ divides $\mathbf{x}^m - 1$ is $m = q^n - 1$.*

By definition a primitive polynomial $f(\mathbf{x}) \in GF(q)[\mathbf{x}]$ is always irreducible in $GF(q)[\mathbf{x}]$, but the opposite does not always hold, i.e., there exist irreducible polynomials which are not primitive. As a simple example, consider the polynomial $\mathbf{x}^4 + \mathbf{x}^3 + \mathbf{x}^2 + \mathbf{x} + 1$, which is irreducible in $GF(2)[\mathbf{x}]$, but as a factor of $\mathbf{x}^5 + 1$, it is not primitive.

Let us denote by $M_n = 2^n - 1$ the n-th Mersenne number. From now on, we will consider only the binary polynomials, i.e., over $GF(2)$.

Definition 3. *The dual of an irreducible polynomial $f(\mathbf{x}) \in GF(2)[\mathbf{x}]$, denoted by $f^{\perp}(\mathbf{x})$, is the polynomial $f(\mathbf{x} + 1)$.*

It is easy to prove that $f(\mathbf{x})$ is a binary irreducible polynomial if and only if its dual $f^{\perp}(\mathbf{x})$ is irreducible. However, the duality operator does not necessarily preserve primitiveness. As a simple example, consider the primitive polynomial

$\mathbf{x}^4+\mathbf{x}^3+1$ whose dual polynomial is $\mathbf{x}^4+\mathbf{x}^3+\mathbf{x}^2+\mathbf{x}+1$, but the latter is not primitive as already mentioned.

The number of irreducible polynomials in $GF(2)[\mathbf{x}]$ of degree n is given by (see, e.g., [1, 11]):

$$\psi_2(n)=\frac{1}{n}\sum_{d|n}2^d\mu\left(\frac{n}{d}\right), \tag{1}$$

where μ is the well-known Möbius function (i.e., if N is a positive integer, the Möbius function $\mu(N)$ is 0 if p^2 divides N for some prime p; 1 if N is square free and contains an even number of prime factors; and -1 if N is square free and contains an odd number of prime factors; a literal interpretation gives $\mu(1)=1$).

While the number of binary primitive polynomials of degree n is given by:

$$\lambda_2(n)=\frac{\Phi(2^n-1)}{n}, \tag{2}$$

where Φ is the Euler function (i.e., $\Phi(N)$ is the number of positive integers smaller than N and coprime with N).

We shall also make use of the following lemma:

Lemma 1. *For any n the number of binary irreducible polynomials $\psi_2(n)$ does not exceed $(2^n-2)/n$, where the equality holds when n is a prime.*

Proof. The statement of Lemma 1 follows from the fact that the greatest two powers of 2 in formula (1) are obtained when we take as divisors n itself and its second largest divisor d in which case the quotient n/d is a prime number. □

Note that if $n=p^r$ (for p a prime number), we obtain $\psi_2(p^r)=2^{p^r}-2^{p^{r-1}}$.

In this paper, we study the ratios

$$\theta(n)=\frac{\lambda_2(n)}{\psi_2(n)} \quad \text{and} \quad \tau(n)=\frac{\Phi(2^n-1)}{M_n}. \tag{3}$$

Since $\psi_2(n)\le(2^n-2)/n<M_n/n$, we have $\theta(n)>\tau(n)$ for any $n>1$. On the other hand since every primitive polynomial is irreducible, clearly we have that $\lambda_2(n)\le\psi_2(n)$, i.e., $\theta(n)\le 1$. Hence the following relations hold:

$$1\ge\theta(n)>\tau(n)>0. \tag{4}$$

Let us also recall some facts from elementary Number Theory (see, e.g. [20]). Let $GCD(a,m)=1$, where as usual $GCD(\cdot,\cdot)$ is the greatest common divisor of its arguments. By the Euler-Fermat theorem we have $a^{\phi(m)} \equiv 1(\text{mod } m)$. Based on this define the index to which a belongs modulo m to be the smallest $\delta > 0$ such that $a^{\delta} \equiv 1(\text{mod } m)$. It is easy to prove that a belongs to δ modulo m if and only if δ divides any γ for which $a^{\gamma} \equiv 1(\text{mod } m)$. In particular the index δ divides $\phi(m)$.

3. Estimations on $\boldsymbol{\tau\left(\prod_{i=1}^{\ell} p_i^{r_i}\right)}$ and $\boldsymbol{\tau\left(2^{r_0}\prod_{i=1}^{\ell} p_i^{r_i}\right)}$. First we will prove the following theorem.

Theorem 1. *Let r_i, $i = 1, \ldots, \ell$ be some positive integers. Then for any odd primes p_i, $i = 1, \ldots, \ell$ we have:*

$$\tau\left(\prod_{i=1}^{\ell} p_i^{r_i}\right) > \exp\left(-\frac{1}{2}\sum_{(j_1,\ldots,j_\ell)\preceq(r_1,\ldots,r_\ell)} \frac{1}{\lg(2\prod\limits_{i=1}^{\ell} p_i^{j_i} + 1)}\right). \tag{5}$$

P r o o f. Let Q be the set of prime factors of $M_{\prod_{i=1}^{\ell} p_i^{r_i}}$. For an arbitrary $q \in Q$ (i.e., q a prime such that $2^{\prod_{i=1}^{\ell} p_i^{r_i}} \equiv 1(\text{mod } q)$), let δ be the index to which 2 belongs modulo q. By the general considerations preceding this section, it follows that δ is a divisor of both $\prod\limits_{i=1}^{\ell} p_i^{r_i}$ and $\phi(q) = q - 1$, i.e., there exists a tuple of integers $(j_1, \ldots, j_\ell) \preceq (r_1, \ldots, r_\ell)$, such that $\delta = \prod\limits_{i=1}^{\ell} p_i^{j_i}$ and $q = 2m\delta + 1$ for some positive m. Thus, q divides M_δ and $q \geq 2\delta + 1$.

Let $Q_{(j_1,\ldots,j_\ell)}$ be the subset of Q consisting of all primes which have an index δ exactly equal to $\prod\limits_{i=1}^{\ell} p_i^{j_i}$. Then clearly $Q = \bigcup\limits_{(j_1,\ldots,j_\ell)\preceq(r_1,\ldots,r_\ell)} Q_{(j_1,\ldots,j_\ell)}$.

First, let us give an upper bound on the cardinality $n_{(j_1,\ldots,j_\ell)}$ of $Q_{(j_1,\ldots,j_\ell)}$. Although more precise estimate of $n_{(j_1,\ldots,j_\ell)}$ might be possible, for our goals it is sufficient the following:

$$2^{\delta} > M_\delta > \prod_{q\in Q_{(j_1,\ldots,j_\ell)}} q \geq (2\delta + 1)^{n_{(j_1,\ldots,j_\ell)}}.$$

Taking the logarithm with base 2, we get: $\delta > n_{(j_1,\ldots,j_\ell)} \lg(2\delta + 1)$ or

$$n_{(j_1,\ldots,j_\ell)} < L\delta, \tag{6}$$

where for the sake of simplicity, we have put: $L = L(\delta) = \dfrac{1}{\lg(2\delta+1)}$.

Let $\pi_{(j_1,\ldots,j_\ell)} = \prod\limits_{q \in Q_{(j_1,\ldots,j_\ell)}} \left(1 - \dfrac{1}{q}\right)$. Replacing every q by the lower bound $2\delta + 1$ and taking into account (6), we get:

$$\begin{aligned}
\pi_{(j_1,\ldots,j_\ell)} &> (1 - \frac{1}{2\delta+1})^{L\delta} \\
&= (1 + \frac{1}{2\delta})^{-L\delta} \\
&= \left[(1 + \frac{1}{2\delta})^{2\delta}\right]^{-\frac{1}{2}L}
\end{aligned}$$

Since the inequality $\left(1 + \dfrac{1}{n}\right)^n < e$, where e is the base of natural logarithms, holds for every positive integer n, it follows that:

$$\pi_{(j_1,\ldots,j_\ell)} > e^{-\frac{1}{2}L} \tag{7}$$

The following is straightforward:

$$\begin{aligned}
\tau\left(\prod_{i=1}^{\ell} p_i^{r_i}\right) &= \frac{\Phi\left(M_{\prod_{i=1}^{\ell} p_i^{r_i}}\right)}{M_{\prod_{i=1}^{\ell} p_i^{r_i}}} = \prod_{q \in Q}\left(1 - \frac{1}{q}\right) \\
&= \prod_{(j_1,\ldots,j_\ell) \preceq (r_1,\ldots,r_\ell)} \; \prod_{q \in Q_{(j_1,\ldots,j_\ell)}} \left(1 - \frac{1}{q}\right) \\
&= \prod_{(j_1,\ldots,j_\ell) \preceq (r_1,\ldots,r_\ell)} \pi_{(j_1,\ldots,j_\ell)}.
\end{aligned}$$

Then from (7) we get the desired lower bound on $\tau\left(\prod\limits_{i=1}^{\ell} p_i^{r_i}\right)$:

$$\tau\left(\prod_{i=1}^{\ell} p_i^{r_i}\right) > e^{-\frac{1}{2}\sum_{(j_1,\ldots,j_\ell) \preceq (r_1,\ldots,r_\ell)} \frac{1}{\lg\left(2\prod_{i=1}^{\ell} p_i^{j_i}+1\right)}} \qquad \square$$

Corollary 1. *For any fixed positive integers r_i and sufficiently large primes p_i, $i = 1, \ldots, \ell$ almost all irreducible polynomials of degree $\prod\limits_{i=1}^{\ell} p_i^{r_i}$ are primitive.*

Proof. Indeed, the ratio $\theta\left(\prod_{i=1}^{\ell} p_i^{r_i}\right)$ is greater than $\tau\left(\prod_{i=1}^{\ell} p_i^{r_i}\right)$, but the latter becomes greater than any constant $c < 1$ when p_i are chosen sufficiently large according to the lower bound proven in the previous theorem. □

Remark 1. Note that under the assumptions of Corollary 1 it follows by the same reasoning that almost all elements of the multiplicative group of the finite field $GF\left(2^{\prod_{i=1}^{\ell} p_i^{r_i}}\right)$ are primitive (i.e., of maximal possible order).

Now we will consider the case when the degree of the polynomial is $2^{r_0}n$, where n is an odd number with prime factorization $n = \prod_{i=1}^{\ell} p_i^{r_i}$ and $r_0 \geq 1$.

Theorem 2. *Let $r_0 \geq 0$ and r_i, $i = 1, \ldots, \ell$ be some positive integers. Then for any odd primes p_i, $i = 1, \ldots, \ell$ we have:*

$$(8)\quad \tau\left(2^{r_0}\prod_{i=1}^{\ell} p_i^{r_i}\right) > \tau(2^{r_0})\exp\left(-2^{r_0-1}\sum_{(j_1,\ldots,j_\ell)\preceq(r_1,\ldots,r_\ell)} \frac{1}{\lg\left(2\prod_{i=1}^{\ell} p_i^{j_i}+1\right)}\right).$$

Proof. The proof is by induction on r_0. The case $r_0 = 0$ is in fact the statement of Theorem 1 and gives the base of the induction. To prove the inductive step we use the following arguments. Since:

$$2^{2^{r+1}n} - 1 = (2^{2^r n} - 1)(2^{2^r n} + 1)$$

the prime factors of $2^{2^r n} + 1$ are prime factors of $2^{2^{r+1}n} - 1$. Thus, the index δ of 2 modulo such a prime factor is either equal to 2^{r+1} or of the form $2^{r+1}\prod_{i=1}^{\ell} p_i^{j_i}$ for some $(j_1, \ldots, j_\ell) \preceq (r_1, \ldots, r_\ell)$, where not all j_i are equal to 0. The prime factors of the first type contribute to $\tau(2^{r+1})$, while the contribution of those of the second type can be estimated in the same way as the corresponding prime factors of $2^{2^r n} - 1$, since they are of the form $m\delta + 1 = 2m\,2^r\prod_{i=1}^{\ell} p_i^{j_i} + 1$ for some positive m. □

To illustrate the consequences of Theorem 2 we formulate the following corollary, which is derived from the case $r_0 = 1$.

Corollary 2. *For any fixed positive integers r_i and sufficiently large primes p_i, $i = 1, \ldots, \ell$ not less than $2/3$ of all irreducible polynomials of degree $2\prod_{i=1}^{\ell} p_i^{r_i}$ are primitive.*

Here we shall consider an application of Theorem 1. It is easily seen that from inequality $\theta(n) > \frac{1}{2}$ (see, e.g., [2]) there follows the existence of a primitive polynomial of degree n whose dual is primitive too. In order to have the inequality $\tau(p^r) > \frac{1}{2}$ for $1 \leq r \leq 4$ and an odd prime p, it is sufficient to choose $p \geq 3$. To add the case $r = 5$, we should choose $p \geq 5$ and the inequality $\tau(3^5) > \frac{1}{2}$ can be checked directly. In other words as a consequence of Theorem 1 we obtain that for any odd prime p and $1 \leq r \leq 5$ there exists a primitive polynomial of degree p^r such that its dual is also primitive. Note that the general fact of the existence of binary primitive polynomials of any degree > 1 with such a property was proven by S. D. Cohen in part 4 of [4] using deeper number-theoretic considerations.

4. An infinite series of integers n_s for which $\theta(n_s) < \frac{1}{2}$.

By using the well-known fact that $GCD(M_k, M_l) = M_{GCD(k,l)}$ (Knuth's GCD lemma, see e.g., [8]), and based on the inequality $\tau(12) = \frac{192}{455} < \frac{1}{2}$, one can easily obtain an infinite series of values n for which the ratio $\tau(n)$ does not reach the threshold value $\frac{1}{2}$. It would be much more interesting to prove the same for the ratio θ.

The following proposition holds.

Proposition 1. *There exists an infinite series of integers $n_s = 2^s, s \geq 7$ for which the number of primitive polynomials of degree n_s is strictly less than the half of the number of irreducible polynomials of that degree.*

Proof. The following computations are straightforward:

$$2^{2^s} - 1 = (2^{2^{s-1}})^2 - 1 = (2^{2^{s-1}} - 1)(2^{2^{s-1}} + 1)$$

and since $GCD(2^{2^{s-1}} - 1, 2^{2^{s-1}} + 1) = 1$ we have:

$$\tau(2^s) = \frac{\Phi(2^{2^s} - 1)}{2^{2^s} - 1} = \frac{\Phi(2^{2^{s-1}} - 1)}{2^{2^{s-1}} - 1} \cdot \frac{\Phi(2^{2^{s-1}} + 1)}{2^{2^{s-1}} + 1} < \frac{\Phi(2^{2^{s-1}} - 1)}{2^{2^{s-1}} - 1} = \tau(2^{s-1})$$

Direct calculations show that $\tau(64) < \frac{1}{2}$ and hence $\tau(2^s) < \frac{1}{2}$ when $s \geq 6$. So for $s > 6$, it follows that:

$$\Phi(2^{2^s} - 1) = \Phi(2^{2^{s-1}} - 1) \cdot \Phi(2^{2^{s-1}} + 1) < \frac{1}{2}(2^{2^{s-1}} - 1)2^{2^{s-1}}.$$

On the other hand we have that: $\psi_2(2^s) = \sum_{d|2^s} 2^d \mu\left(\frac{2^s}{d}\right) = (2^{2^{s-1}} - 1)2^{2^{s-1}}$ and from the above inequality if $s > 6$ we get:

$$\theta(2^s) = \frac{\Phi(2^{2^s} - 1)}{(2^{2^{s-1}} - 1)2^{2^{s-1}}} < \frac{1}{2}. \qquad \square$$

5. Conclusions. Based on number-theoretic considerations we present estimations on the ratio between the number of binary primitive and irreducible polynomials of degrees n and $2n$, for an arbitrary odd n. As a consequence we prove that when the powers (in the prime factorization of n) are fixed and the primes are sufficiently large, almost (not less than 2/3 of) all binary irreducible polynomials of these degrees are primitive, respectively.

Finally, we describe an infinite series of degrees (namely $n_s = 2^s, s \geq 7$) for which the number of primitive polynomials in $GF(2)[\mathbf{x}]$ is strictly less than $\frac{1}{2}$ of the number of corresponding irreducible polynomials.

Acknowledgements. This research was supported in part by the KRF 2007-521-D00330, R. of Korea.

Svetla Nikova was partially supported by the Concerted Research Action (GOA) Ambiorics 2005/11 of the Flemish Government, by the European Commission through the IST Programme under Contract IST-2002-507932 ECRYPT and the IAPP–Belgian State–Belgian Science Policy BCRYPT.

REFERENCES

[1] Berlekamp E. Algebraic Coding Theory. McGraw-Hill, New York, 1968.

[2] Borissov Y., S. Nikova, N. Manev. On primitive polynomials over GF(2) the duals of which are also primitive. In: Proc. of the Twenty-Seventh Symposium on Information Theory in the Benelux, 2006, 221–226.

[3] Brent R. Searching for primitive trinomials (mod 2). `http://wwwmaths.anu.edu.au/~brent/trinom.html`, 2008.

[4] Cohen S.D. Consecutive primitive roots in a finite field. *Proc. Amer. Math. Soc.*, **93** (1985), 189–197.

[5] Cohen S.D. Primitive polynomials with a prescribed coefficient. *Finite Fields Appl.* **12** (2006), 425–491.

[6] Cohen S.D., D. Mills. Primitive polynomials with first and second coefficients prescribed. *Finite Fields and Their Applications* **9**, No 3 (2003), 334–350.

[7] Dodunekov S. M. Essentially different irreducible polynomials over finite fields.*Ann. University of Sofia, Faculty of Mathematics and Mechanics* **66** 1971/72 (1974), 169–175 (in Russian).

[8] Eddington W. Will Eddington's Mersenne Page.
`http://www.garlic.com/~wedgingt/mersenne.html`, 2008.

[9] von zur Gathen J. Irreducible trinomials over finite fields. ISSAC, 2001, 332–336.

[10] von zur Gathen J., I. Shparlinski. Constructing elements of large order in finite fields. AAECC, 1999, 404–409.

[11] Golomb S. W. Shift register sequences. San Francisco, Holden-Day, 1967.

[12] Golomb S. W., Guang Gong. Actions of the Unitary Group on Irreducible/Primitive Polynomials and Their Applications to Randomness of Sequences. IEEE ITW 2007, Bergen, Norway, July 1–6, 2007.

[13] Lidl R., H. Niderreiter. Introduction to finite fields and their applications. Cambridge University Press, 1994.

[14] Lucas J., G. Mullen. Irreducible polynomials over GF(2) with prescribed coefficients. *Discrete Mathematics*, **274**, No 1–3 (2004), 265–279.

[15] Moreno O. On primitive elements of trace equal to 1 in $GF(2^m)^*$. *Discrete Mathematics*, **41**, No 1 (1982), 53–56.

[16] Rabin M. Probabilistic algorithms in finite fields. *SIAM J. Comput.*, **9** (1980), 273–280.

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

[18] Shparlinski I. On irreducible polynomials of small height over finite fields. *Appl. Algebra Eng. Commun. Comput.*, **7**, No 6 (1996), 427–431.

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

[20] Vinogradov I. M. Elements of number theory. Transl. from the 5th rev. ed. by S. Kravetz. New York, Dover Publ., 1954, VIII, 227 pp.

[21] Wicker S. Error control systems for digital communication and storage. Prentice Hall International, Inc., 1995.

[22] Zierler N., J. Brillhart. On primitive trinomials (mod 2). *Information and Control*, **13**, No 6 (1968), 541–554.

Yuri Borissov
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
Acad. G. Bonchev Str., Block 8
1113 Sofia, Bulgaria
e-mail: `youri@math.bas.bg`

Moon Ho Lee
Institute of Information and Communication
Chonbuk National University
R. Korea
e-mail: `moonho@chonbuk.ac.kr`

Svetla Nikova
ESAT/SCD/COSIC
Katholieke Universiteit Leuven
Belgium
e-mail: `svetla.nikova@esat.kuleuven.be`

Received July 16, 2008
Final Accepted October 24, 2008