Tatra Mt. Math. Publ. **32** (2005), 129–142

TATRA MOUNTAINS
Mathematical Publications

SOME OBSERVATIONS CONCERNING IRREDUCIBLE TRINOMIALS AND PENTANOMIALS OVER $\mathbb{Z}_2$

Andrzej Paszkiewicz

ABSTRACT. In this paper we observe the number of irreducible trinomials and pentanomials over $\mathbb{Z}_2$.

1. Introduction

Primitive and irreducible polynomials with coefficients from finite fields play an important role in coding theory [1] and cryptography [2], [3]. Primitive polynomials of degree n over $\mathbb{Z}_p$ form a subset of irreducible polynomials of the same degree over $\mathbb{Z}_p$. For $p = 2$ and n such that $2^n - 1$ is a Mersenne prime both sets—primitive and irreducible polynomials of degree n—are the same. There can also be proved [4] the following

Theorem 1. *Let I_n and J_n be the number of irreducible and primitive polynomials of degree n, respectivelly, with coefficients from $\mathbb{Z}_2$ then for every $\varepsilon > 0$ there exist infinitely many natural numbers n with the property $J_n/I_n > 1 - \varepsilon$.*

P r o o f. The number of irreducible polynomials of degree n over $\mathbb{Z}_2$ can be expressed by the following formula $I_n = \frac{1}{n}\sum_{d|n}\mu(d)\cdot 2^{\frac{n}{d}}$, where μ denotes the Moebius function. The number of primitive polynomials of degree n over $\mathbb{Z}_2$ is expressed by the formula $J_n = \frac{2^n-1}{n}\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_k}\right)$, where $p_1, p_2, \ldots, p_k$ are all different prime factors of the number $2^n - 1$. Substituting in the last expression the factor $\frac{2^n-1}{n}$ by the smaller number I_n we obtain

$$\frac{J_n}{I_n} > \left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_k}\right). \tag{1}$$

2000 Mathematics Subject Classification: Primary 12E30; Secondary 12E05.
Keywords: irreducible polynomials, primitive polynomials.

It is a well known fact that each prime factor of the number 2^n-1, where n is prime has the form $k\cdot n+1$, where k is a positive integer. Let $p_1 < p_2 < \cdots < p_k$ be the different factors of the number 2^n-1. That means $2^n-1 \geqslant p_1\cdot p_2\cdots p_k \geqslant 2^k$, hence $n > k$ and $p_j \geqslant jn+1 > jn$ for $j = 1, 2, \ldots, k$. The last implies

$$\frac{1}{p_1}+\cdots+\frac{1}{p_k} < \sum_{j=1}^{k}\frac{1}{jn} = \frac{1}{n}\sum_{j=1}^{k}\frac{1}{j} < \frac{1+\ln k}{n} < \frac{1+\ln n}{n}\,.$$

From (1) it follows

$$\frac{J_n}{I_n} > \left(1-\frac{1}{p_1}\right)\ldots\left(1-\frac{1}{p_k}\right) > 1-\left(\frac{1}{p_1}+\cdots+\frac{1}{p_k}\right) > 1-\frac{1+\ln n}{n} \qquad (2)$$

and because the expression $(1+\ln n)/n$ tends to 0 as n tends to infinity we can make it smaller than arbitrary positive number ε, what finishes our proof. □

Otherwise it can also be proved [5] the following

Theorem 2. *For every natural number $n > 1$ and $\varepsilon > 0$ there exist infinitely many prime numbers $p > 2$ that $J_n/I_n < \varepsilon$, where I_n and J_n are the number of irreducible and primitive polynomials of degree n, respectivelly, with coefficients from $\mathbb{Z}_p$.*

P r o o f. As we know $I_n > \frac{1}{n}\left(p^n - n\cdot p^{\frac{n}{2}}\right)$ and $J_n = \dfrac{\varphi(p^n-1)}{n}$ where φ denotes the Euler's totient function, hence

$$\frac{J_n}{I_n} < \frac{\varphi(p^n-1)}{p^n-1}\cdot\frac{p^n-1}{p^n-n\cdot p^{n/2}}\,.$$

We obviously have

$$\lim_{n\to\infty}\frac{p^n-1}{p^n-n\cdot p^{n/2}} = 1\,.$$

Moreover from the formula

$$\frac{\varphi(n)}{n} = \prod_{p|n}\left(1-\frac{1}{p}\right)$$

it follows, that if $r|s$ then

$$\frac{\varphi(r)}{r} \geqslant \frac{\varphi(s)}{s}\,.$$

Hence

$$\frac{\varphi(p^n-1)}{p^n-1} \leqslant \frac{\varphi(p-1)}{p-1}\,.$$

If we will choose, prime numbers $q_1, \ldots, q_t$ such that

$$\prod_{j=1}^{t} \left(1 - \frac{1}{q_j}\right) < \frac{\varepsilon}{2}$$

and a prime number p such that $q_1, \ldots, q_t \,|\, p-1$ and

$$\frac{p^n - 1}{p^n - n \cdot p^{n/2}} < 2$$

we shall have

$$\frac{\varphi(p-1)}{p-1} \leqslant \prod_{j=1}^{t} \left(1 - \frac{1}{q_j}\right) < \frac{\varepsilon}{2}$$

and finally

$$\frac{J_n}{I_n} < \frac{\varepsilon}{2} \cdot 2 = \varepsilon \,.$$

Such a prime number p exists on the base of Dirichlet's theorem on prime numbers in arithmetic progressions, what ends the proof of our theorem. □

The situation described in the first theorem is more interesting from the practical point of view. The Theorem 1 gives for polynomials with coefficients from $\mathbb{Z}_2$ a starting point to the 2nd stage strategy of generating primitive polynomials. The first and easy stage is to generate an irreducible polynomial of a given degree and the second and more complicated stage is to verify whether it is also primitive. It is also easy to see that having one primitive polynomial of a given degree we can produce all other primitive polynomials of the same degree. It is interesting to generate irreducible polynomials with only few non-zero coefficients. These polynomials are very suitable to generate modular arithmetic of a finite field for coding theory as well as for cryptography. Short irreducible polynomials (polynomials with only few nonzero coefficients such as trinomials and pentanomials [3]) are well suitable for generating modular arithmetic by hardware. Moreover, having only one irreducible polynomial of the set of irreducible polynomials of a given degree, we can generate all other irreducible polynomials of that degree. This gives an easy way to replicate one irreducible polynomial over finite field.

2. Observations on irreducible trinomials and pentanomials over $\mathbb{Z}_2$

In the technical report [6] I have presented the largest table of primitive trinomials and pentanomials over $\mathbb{Z}_2$ up to degree of 640 without gaps. The

computation have been continued. All primitive trinomials and pentanomials (if a trinomial of a given degree does not exist) for degrees between 641 and 740 with two gaps for degrees 713 and 739. We do not include these results here because of existing large tables of primitive polynomials ([7]). It is worth mentioning that our software is at least twice as fast than the best presented in [7]. The method of obtaining primitive polynomials consists, as mentioned above, of 2 stages. In the first stage we generate an irreducible trinomial or if it does not exist a pentanomial. We did not find any case of positive integer n for which an irreducible pentanomial of degree n does not exist. In the second stage we investigate the order of the monomial X modulo polynomial $f(X)$ which is just tested for irreducibility. If the order is maximal and equal to $2^n - 1$, where $n = \deg\big(f(X)\big)$ then $f(X)$ is primitive. In the present paper we describe some observations concerning polynomials with three and five nonzero coefficients over $\mathbb{Z}_2$, called trinomials and pentanomials. This is result of a huge computational project for searching irreducible polynomials of high degree. In this project we have found for every number $n \leqslant 13122$ an irreducible trinomial (if it exists) and for each $n \leqslant 4000$ all irreducible trinomials of degree n. (Recently we have computationally advanced a project of finding all irreducible trinomials of degree n for each $n \leqslant 10000$.) For every $n \leqslant 10000$ we have found one irreducible pentanomial. Some interesting facts can be observed:

1. For about one half (exactly 5147) of all degrees $n \leqslant 10000$ there exists an irreducible trinomial over $\mathbb{Z}_2$ (see Fig. 1 below). In fact the rate of such $n \leqslant 10000$ for which an irreducible trinomial exists is a bit greater than 0.5.
2. The rate of trinomials of the degree of the form $8k + i$, $i = 0, 1, \ldots, 7$, seems to tend to some positive limits if $i \neq 3, 5$. The rate of irreducible trinomials of degree having the form $8k+3$ or $8k+5$ is extremely small. All trinomials of that form are collected in the Table 4.
3. For every $n \leqslant 10000$ there exists an irreducible pentanomial.
4. The maximum growth rate of the number of irreducible trinomials of a given degree n seems to be a logarithmic function of n (see Fig. 6 below).
5. The number $L_5(n)$ of pentanomials of degree n has a characteristic behavior. It is in some sense periodical with local minimal values for degrees being divisible by 8 (see Fig. 14 below).
6. The growth rate of the number of irreducible pentanomials of a given degree n seems to be a quadratic function of n (see Fig. 15–30).
7. The number $L_3(n)$ of irreducible trinomials of a given degree n over $\mathbb{Z}_2$ is in general an even number. There are only few numbers $n \leqslant 13122$ for which the number of irreducible trinomials of degree n is an odd

number. All these polynomials are of degree n of the form $n = 2 \cdot 3^k$. We listed all these polynomials in the Table 2.

8. $A_i(n)$—the number of degrees of the form $8k + i$, $i = 1, 2, \ldots, 7$, not exceeding n having irreducible trinomials seems to be proportional to n (Fig. 7–13).

TABLE 1. $L_3(n,k) = \#\{$the number of irreducible trinomials of degree $\leqslant n : L_3(n) = k\}$ for $n = 400$.

k	$L_3(n,k)$	k	$L_3(n,k)$	k	$L_3(n,k)$	k	$L_3(n,k)$
1	2	1	0	21	0	31	0
2	589	12	88	22	7	32	3
3	4	13	0	23	0	33	0
4	490	14	37	24	8	34	1
5	5	15	0	25	0	35	0
6	353	16	23	26	3	36	0
7	0	17	0	27	0	37	0
8	253	18	14	28	4	38	1
9	0	19	0	29	0	39	0
10	160	20	13	30	2	40	1

TABLE 2. Complete list of degrees $1 < n \leqslant 13122$ and irreducible trinomials of degree n such that the number of irreducible trinomials of degree n is odd

6, 1, 0	162, 63, 0	4374, 729, 0
6, 3, 0	162, 81, 0	4374, 1701, 0
6, 5, 0	162, 99, 0	4374, 2187, 0
18, 1, 0	162, 135, 0	4374, 2673, 0
18, 7, 0	486, 81, 0	4374, 3645, 0
18, 9, 0	486, 189, 0	13122, 1547, 0
18, 11, 0	486, 243, 0	13122, 2187, 0
18, 15, 0	486, 297, 0	13122, 2923, 0
54, 9, 0	486, 405, 0	13122, 5103, 0
54, 21, 0	1458, 243, 0	13122, 6561, 0
54, 27, 0	1458, 567, 0	13122, 8019, 0
54, 33, 0	1458, 729, 0	13122, 10199,0
54, 15, 0	1458, 891, 0	13122, 10935, 0
162, 27, 0	1458, 1215, 0	13122, 11575, 0

The set $\{6, 18, 54, 162, 486, 1458, 4374, 13122\}$ is a complete list of all degrees n, $1 < n \leqslant 13122$, such that the number of irreducible polynomials of degree n is an odd number. It is easy to see that all these numbers are of the form $n = 2 \cdot 3^k$. We checked that for the next number $n = 39366$, which is of the form $2 \cdot 3^9$ all the irreducible polynomials of degree $n = 39366$ are as listed in the

Table 4 below. The triplets $(n, k, 0)$ in tables 2, 3, and 4 denote an irreducible trinomial of the form $X^n + X^k + 1$.

One can prove the following

THEOREM 3. *Every of the five trinomials below is irreducible over* $\mathbb{Z}_2$

1. $X^{2\cdot 3^k} + X^{3\cdot 3^{k-2}} + 1$;
2. $X^{2\cdot 3^k} + X^{7\cdot 3^{k-2}} + 1$;
3. $X^{2\cdot 3^k} + X^{9\cdot 3^{k-2}} + 1$;
4. $X^{2\cdot 3^k} + X^{11\cdot 3^{k-2}} + 1$;
5. $X^{2\cdot 3^k} + X^{15\cdot 3^{k-2}} + 1$.

We omit the proof of the theorem. As we can see from Tables 2 and 3, the list of 5 trinomials in Theorem 3 is not complete, because for degrees 13122 and 39366 we have exactly 9 irreducible trinomials.

TABLE 3. Complete list of irreducible trinomials of degree $n = 39366$

39366, 4641, 0	39366, 15309, 0	39366, 30597, 0
39366, 6561, 0	39366, 19683, 0	39366, 32805, 0
39366, 8769, 0	39366, 24057, 0	39366, 34725, 0

TABLE 4

Irreducible trinomials of degree $8k+3$	Irreducible trinomials of degree $8k+5$
below 10000	below 10000
3, 1, 0	5, 2, 0
11, 2, 0	21, 2, 0
35, 2, 0	29, 2, 0
123, 2, 0	93, 2, 0
147, 14, 0	253, 46, 0
155, 62, 0	333, 2, 0
651, 14, 0	845, 2, 0
979, 178, 0	861, 14, 0
2331, 178, 0	1029, 98, 0
2667, 254, 0	1085, 62, 0
5819, 1058, 0	2485, 142, 0
6027, 98, 0	4125, 2, 0
7203, 686, 0	4445, 254, 0
	4557, 98, 0
	4805, 1922, 0
	6757, 466, 0
	7077, 674, 0

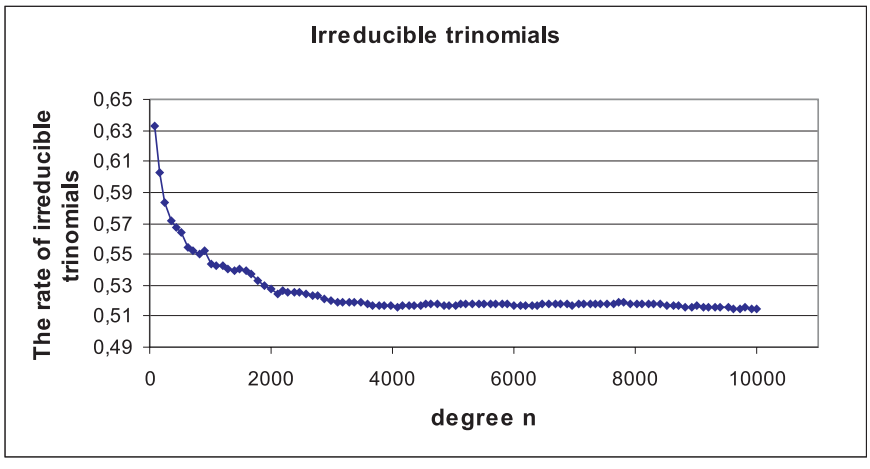

FIGURE 1. The rate of irreducible trinomials of degrees below 1000.

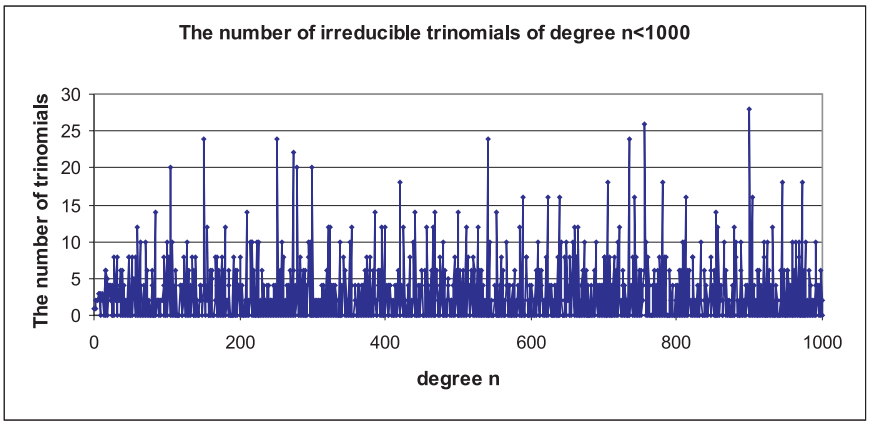

FIGURE 2

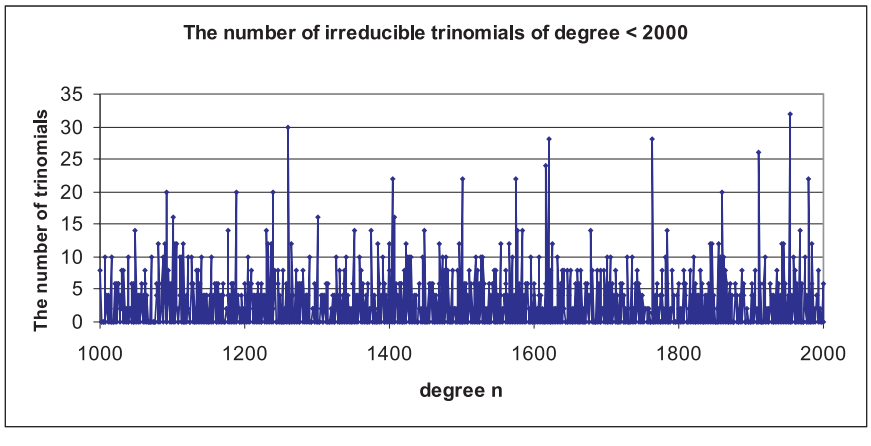

FIGURE 3

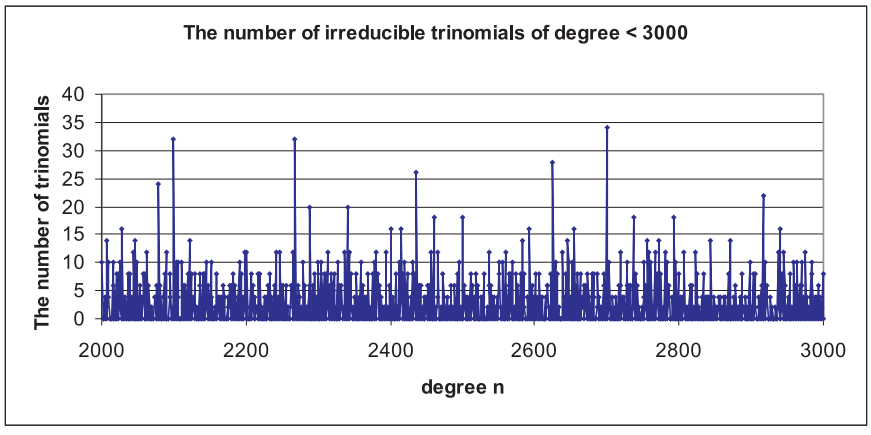

FIGURE 4

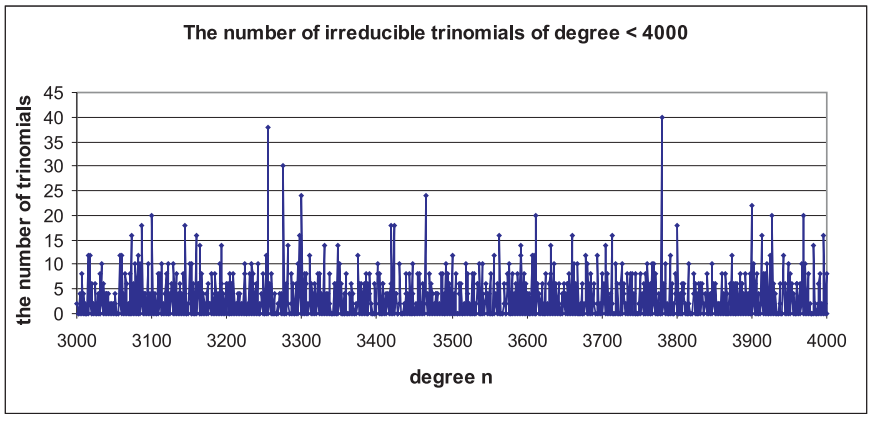

FIGURE 5

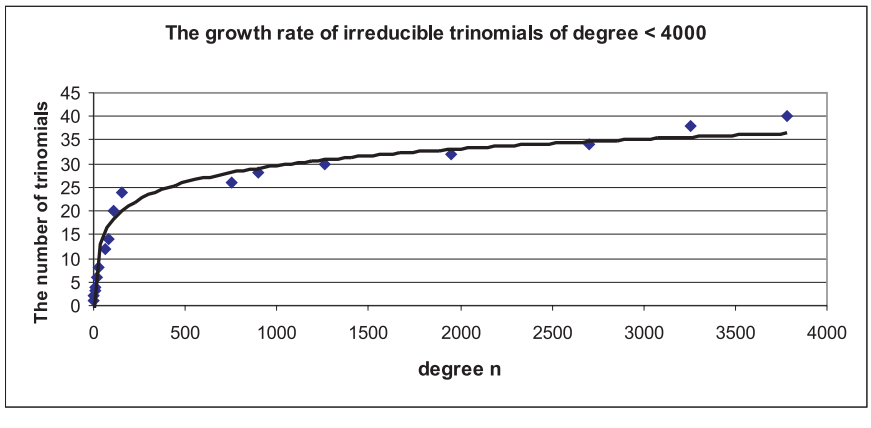

FIGURE 6

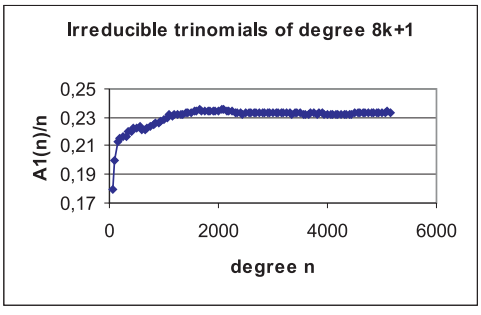

FIGURE 7

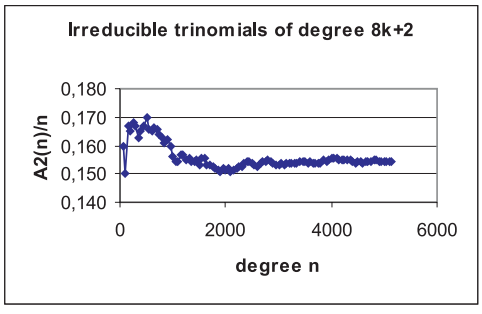

FIGURE 8

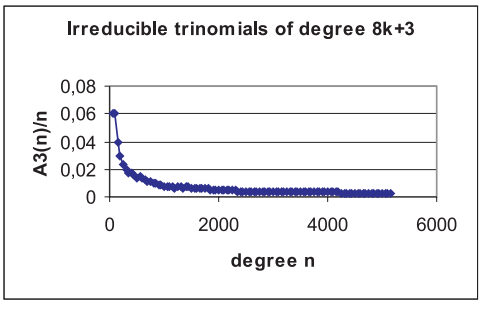

FIGURE 9

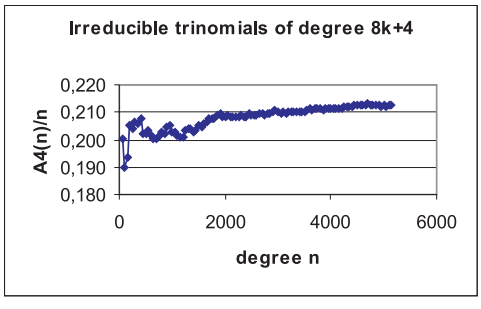

FIGURE 10

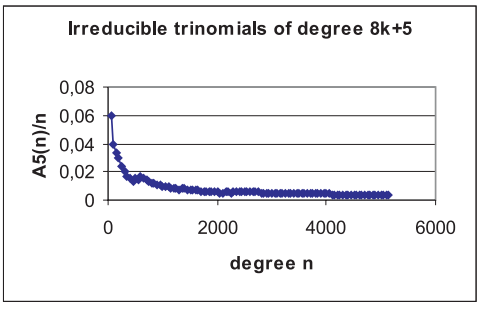

FIGURE 11

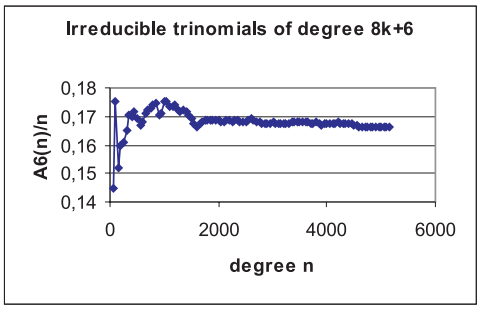

FIGURE 12

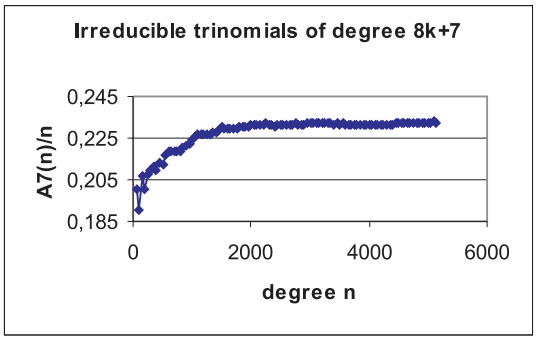

FIGURE 13

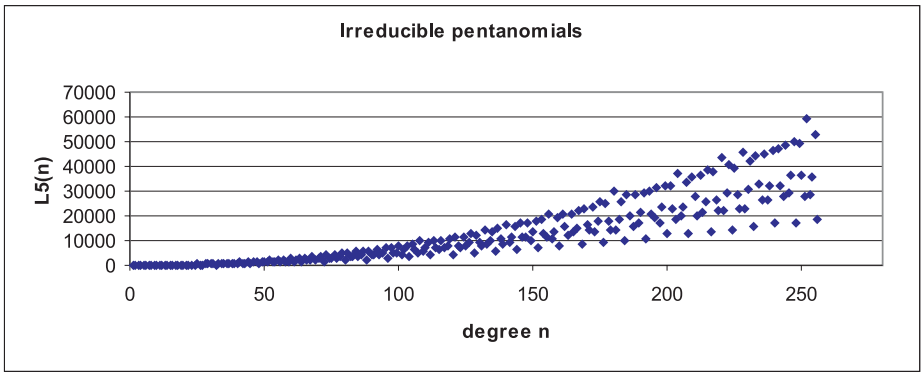

FIGURE 14

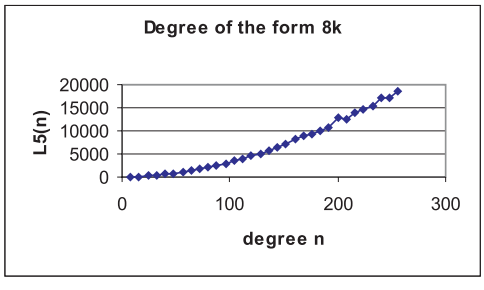

FIGURE 15

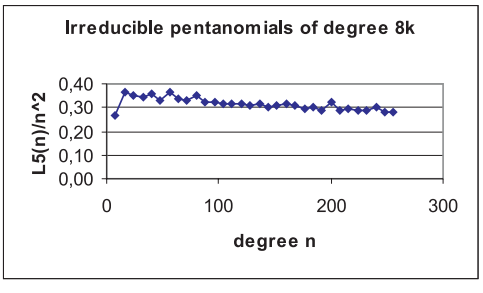

FIGURE 16

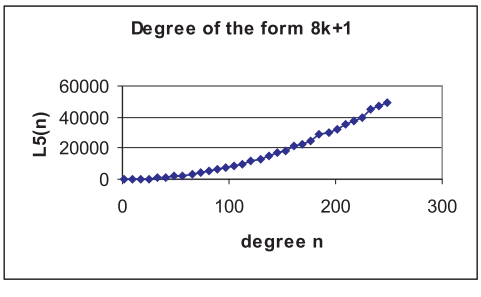

FIGURE 17

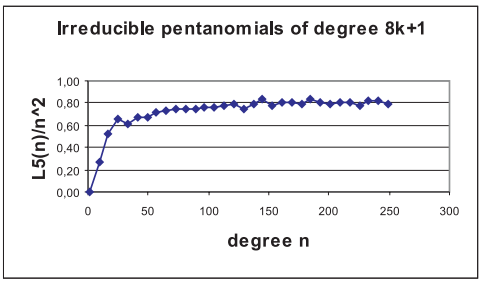

FIGURE 18

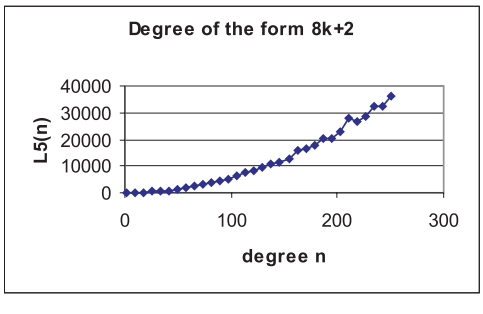

FIGURE 19

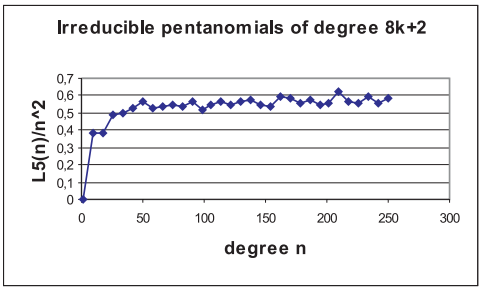

FIGURE 20

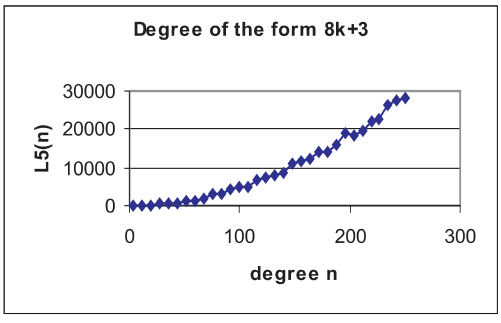

FIGURE 21

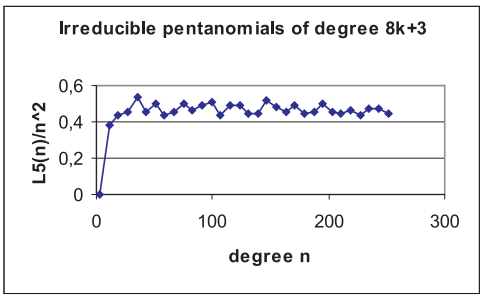

FIGURE 22

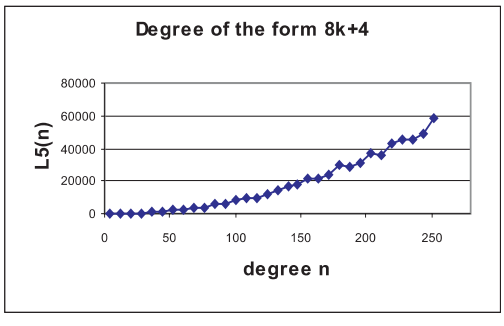

FIGURE 23

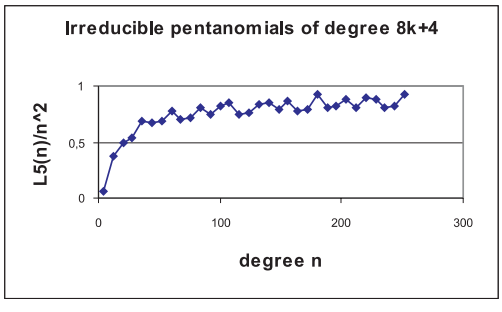

FIGURE 24

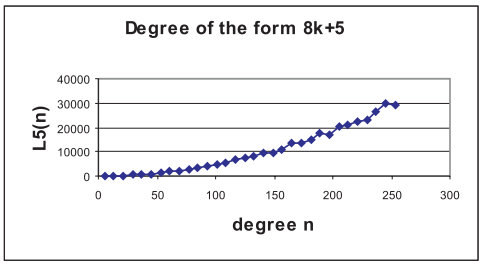

FIGURE 25

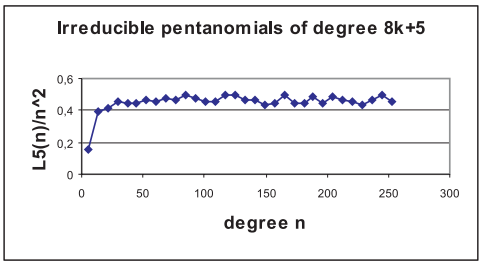

FIGURE 26

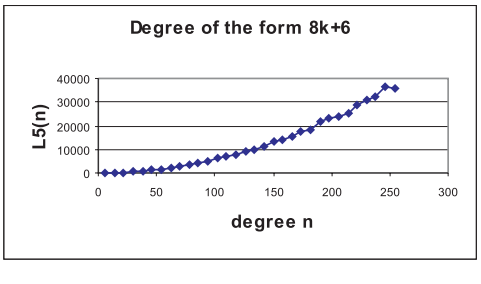

FIGURE 27

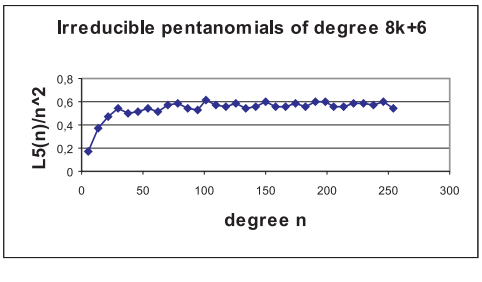

FIGURE 28

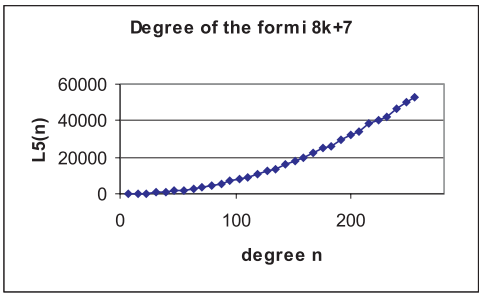

FIGURE 29

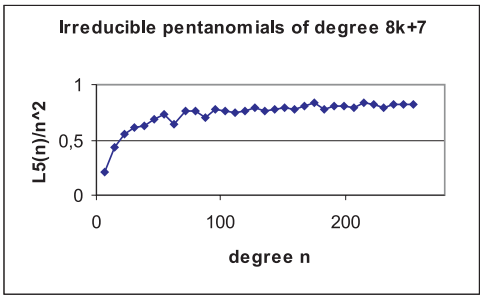

FIGURE 30

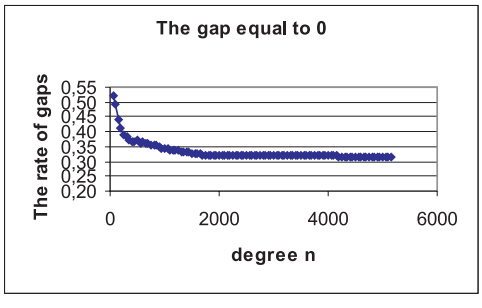

FIGURE 31

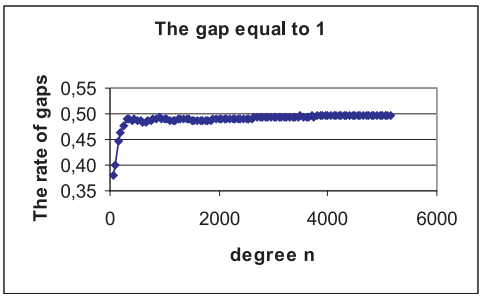

FIGURE 32

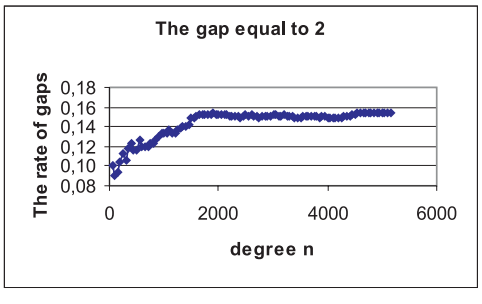

FIGURE 33

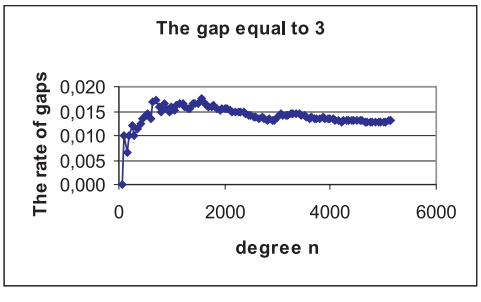

FIGURE 34

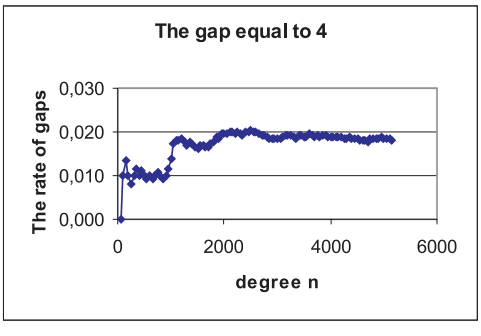

FIGURE 35

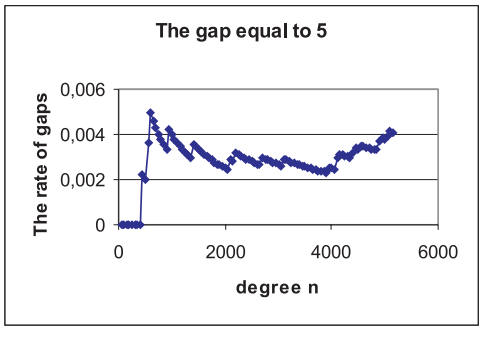

FIGURE 36

3. Observations on gaps between degrees for which irreducible trinomials over $\mathbb{Z}_2$ exist

Let $n < k$ be natural numbers such that for n and k there exists an irreducible trinomial of degree n and k. If degrees $n+1, \ldots, k-1$ are free of irreducible trinomials then the number $n-k-1$ will be called a gap. If for n and $n+1$ there exist irreducible trinomials then the gap between them is equal to 0. Some observation on gaps between degrees for which irreducible trinomials over $\mathbb{Z}_2$ exist can be observed:

1. The rate of gaps of a given length seems to tend fast to some limits;
2. The gaps (number of consecutive natural numbers for which an irreducible trinomial does not exist) does not seem to be large. The largest gap is equal to 7. We illustrate below the behavior of gaps.

4. Problems for further investigations

Problem 1. *Do there exist limits* $\lim\limits_{n\to\infty} \frac{A_i(n)}{n}$, $i = 1, 2, \ldots, 7$, *where* $A_i(n)$ *is the number of degrees of the form* $8k+i$ *not exceeding* n *having irreducible trinomials over* $\mathbb{Z}_2$*?*

Problem 2. *Does there exist the limit* $\lim\limits_{n\to\infty} \frac{L_5(n)}{n^2}$, *where* $L_5(n)$ *is the number of irreducible pentanomials of degree* n*?*

Problem 3. *Are the gaps (number of consecutive natural numbers for which an irreducible trinomial does not exist) without irreducible trinomials over* $\mathbb{Z}_2$ *arbitrary large?*

REFERENCES

[1] BLAHUT, R. E.: *Theory and Practice of Error Control Codes*, Addison-Wesley, Reading Massachusetts, Menlo Park, 1984, (reprinted with correction).

[2] GOLOMB, S. W.: *Shift Register Sequences*, Holden-Day, San Francisco 1967, reprinted by Aegean Park Press, 1982.

[3] MENEZES, A. J. et al.: *Handbook of Applied Cryptography*, CRC Press, Boca Raton, New York, 1997.

[4] PASZKIEWICZ, A.: *On some quantitative relations between irreducible and primitive polynomials*, Biul. WAT **XXXVI** (1987), 29–35. (In Polish)

[5] PASZKIEWICZ, A.: *On relations between irreducible and primitive polynomials*, Biul. WAT **XLIII** (1994), 107–112. (In Polish)

[6] PASZKIEWICZ, A.: *Number theoretical generators of pseudorandom numbers. Methods of investigations, properties and applications*, Technical Report Nr. 503/G/1036/3290–2003.

[7] http://users2.ev1.net/~sduplichan/primitivepolynomials/primitivepolynomials.htm.

Received October 30, 2004

Warsaw University of Technology
Institute of Telecommunications
ul. Nowowiejska 15/19
PL–00-661 Warsaw
POLAND

E-mail: anpa@tele.pw.edu.pl