MINIMUM COMPLEXITY AND LOW-WEIGHT NORMAL POLYNOMIALS OVER FINITE FIELDS

Mahmood Alizadeh

Farshin Hormozi-nejad

Department of Mathematics and Statistics
Islamic Azad University, Ahvaz Branch
Iran
e-mails: alizadeh@iauahvaz.ac.ir
hormozi-nejad@iauahvaz.ac.ir

Abstract. In this paper, by using some algorithms, the distribution of the complexity of normal polynomials over finite fields of characteristic three with degree extensions up to 16 is provided. Also, the current results on the smallest known complexity for the remaining degree extensions up to 300 by using a combination of theorems and known exact values are given. In what follows, by using some algorithms, a table of normal trinomials and pentanomials with minimum complexity among all normal trinomials and pentanomials, respectively over $\mathbb{F}_3$, with their complexities for each degree n with $3^n \leq 10^{50}$ is presented. Also, either normal trinomials or pentanomials with minimum weight over $\mathbb{F}_3$, for each n, $106 \leq n \leq 300$ are listed.

Keywords: Complexity, finite fields, normal polynomial, trinomial, pentanomial.

2000 Mathematics Subject Classification: 12Y05.

1. Introduction

For a prime power $q = p^s (s \in \mathbb{N})$ and a positive integer $n \geqslant 2$, let $\mathbb{F}_q$ be the finite fields with q elements and $\mathbb{F}_{q^n}$ be its extension of degree n. A normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is a basis of the form $N = \{\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}\}$, where $\alpha \in \mathbb{F}_{q^n}$. In this case, α is called a normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, or that α generates the normal basis N. Let $\alpha_i = \alpha^{q^i}, 0 \leq i \leq n-1$, and $T = (t_{ij})$ be the $n \times n$ matrix given by

$$\alpha \cdot \alpha_i = \sum_{j=0}^{n-1} t_{ij}\alpha_j \quad 0 \leq i \leq n-1, \ t_{ij} \in \mathbb{F}_q. \tag{1}$$

The matrix T in (1) is called the *multiplication table* of the normal basis N. If α is a normal element, the multiplication table of the normal basis generated by α is also referred as the multiplication table of α. The number of non-zero entries in T is called the *complexity* of the normal basis N, denoted by c_N. The following theorem gives a lower bound for c_N.

Theorem 1.1 (Mullin et al. [18]) *For any normal basis N of F_{q^n} over F_q, $c_N \geq 2n-1$.*

A normal basis N is *called optimal normal basis* (ONB) if $c_N = 2n - 1$. It is well known that, when using normal bases, the speed of multiplications over $\mathbb{F}_q$ depends directly on c_N (see [6], Section 11.2.2), and it is important to use a normal basis in $\mathbb{F}_q$, with the lowest possible complexity. When no optimal normal basis exists, the problem of classifying the low complexity normal bases stays open.

A monic irreducible polynomial $F(x) \in \mathbb{F}_q[x]$ is called *normal polynomial* or *N-polynomial* if its roots form a normal basis or, equivalently, if they are linearly independent over $\mathbb{F}_q$. The elements in a normal basis are exactly the roots of some N-polynomial. Hence an N-polynomial is just another way of describing a normal basis. On the other side, the polynomials of low weight (with minimum number of nonzero coefficients) can lead to more efficient implementation of the arithmetic of $\mathbb{F}_q$. In [23] Seroussi presents a table of either irreducible trinomials or pentanomials (polynomials with three or five number of nonzero coefficients) over the finite field $\mathbb{F}_2$, For each degree n in the range $2 \leq n \leq 10,000$. In general the problem of existence of normal trinomials or pentonomials of each fixed degree n stays open. Peterson and Weldon [20] list a set of normal polynomial of degree $n \leq 34$ over $\mathbb{F}_2$. For a better understanding of the behavior of the complexities of normal elements in $\mathbb{F}_q$, tables summarizing the complexity distribution are important tools. In ([12], Section 3.3), Jungnickel provides a table with minimum and maximum complexities of normal elements in $\mathbb{F}_{2^n}$, for each n smaller than or equal to 30. In ([12], Section 5.4), for $31 \leq n \leq 60$, he provides a table due to Geiselmann [8] with the lowest complexities found via free polynomials. Masuda, Moura, Panario and Thomson [15] provide the distribution of the complexity of normal elements for binary fields with degree extensions up to 39, using some algorithms that test field elements. They also provide the current results on the smallest known complexity for the remaining degree extensions up to 528, using a combination of constructive theorems and known exact values.

Morgan and Mullen [17] published tables of primitive normal polynomials with three, four or five number of nonzero coefficients of degree n over $\mathbb{F}_p$ for each $p^n \leq 10^{50}$ with $p \leq 97$.

The software and hardware implementation of arithmetic in the fields with characteristic three has been intensively studied in recent years. Some results in the hardware or software implementations in the finite fields with characteristic three can be found in [9], [10], [11], [13], [19]. The elements of the finite fields $\mathbb{F}_{3^s}$ can be represented using a normal basis.

In this paper, using some algorithms that efficiently test normality of polynomials and compute the complexities of them, we provide the distribution of the complexity of normal polynomials for finite fields of characteristic three with degree extensions up to 16. We also provide current results on the lowest known complexity for the remaining degree extensions up to 300 by using a combination of theorems and known exact values. In the continue, using some algorithms, a table of normal trinomials and pentanomials with minimum complexity among all normal trinomials and pentanomials, respectively over $\mathbb{F}_3$, with their complexities for each degree n with $3^n \leq 10^{50}$ is presented. Also, either normal trinomials or pentanomials with minimum weight over $\mathbb{F}_3$, for each n, $106 \leq n \leq 300$ are listed.

2. Preliminaries

We need the following results for next study. The following proposition determine that whether an irreducible polynomial is normal or not.

Proposition 2.1 (Gao, see [16], Theorem 4.6) *Let $f(x)$ be an irreducible polynomial of degree n over $\mathbb{F}_q$. Let $\alpha_i = \alpha^{q^i}$, and $t_i = Tr_{q^n|q}(\alpha_0\alpha_i)$, $0 \leq i \leq n-1$, where $\alpha \in \mathbb{F}_{q^n}$ is a root of $f(x)$. Then $f(x)$ is a normal polynomial over $\mathbb{F}_q$ if and only if the polynomial $N(x) = \sum_{i=0}^{n-1} t_i x^i \in \mathbb{F}_q[x]$ is relatively prime to $x^n - 1$.*

Notation 2.2 *Let $f(x) = \sum_{i=0}^{n} c_i x^i$ be an N-polynomial over $\mathbb{F}_q$. Then $c_{n-1} \neq 0$.*

Proposition 2.3 ([16], Corollary 4.19) *Let $n{=}p^e$ for some e, and $f(x){=}\sum_{i=0}^{n} c_i x^i$ be an irreducible polynomial over $\mathbb{F}_q$. Then $f(x)$ is an N-polynomial if and only if $c_{n-1} \neq 0$.*

The number of normal polynomials of degree n over F_q will be compute by the following proposition.

Proposition 2.4 (Ore, [12], Theorem 3.1.5) *Let q be a power of the prime p, let n be a positive integer and write $n = p^a m$, where p does not divide m. Then the number of normal bases of F_{q^n} over F_q equals*

$$\frac{1}{n}\ \phi_q(x^n - 1) = (q^n/n) \prod_{d|m} (1 - q^{-o_d(q)})^{\phi(d)/o_d(q)},$$

where $\phi_q(f)$ is the number of polynomials of degree smaller than the degree of f which are relatively prime to f, $o_n(a)$ is the order of a modulo n, and $\phi(d)$ is the number of positive integers smaller than d that are relatively prime to d.

Proposition 2.5 ([16], Theorem 5.2) *Let $n+1$ is prime and q is primitive in Z_{n+1}. Then $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ has an optimal normal basis.*

Proposition 2.6 ([12], Theorem 3.3.13) *Let α and β generate normal bases A and B for $\mathbb{F}_{q^m}$ and $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, respectively. Assume that m and n are coprime and put $\gamma = \alpha \cdot \beta$. Then*

1. *γ generates a normal bases N for $\mathbb{F}_{q^{mn}}$ over $\mathbb{F}_q$.*
2. *$c_N = c_A \cdot c_B$.*

Let n, k be integers such that $r = nk+1$ is a prime, and let q be a prime power with $gcd(q, r) = 1$. Let β be a primitive rth root of unity in $\mathbb{F}_{q^{nk}}$. Furthermore, let G be the unique subgroup of order k in Z_r^*. The element $\alpha = \sum_{\gamma \in G} \beta^\gamma$ is called a Gauss period of type (n, k) over $\mathbb{F}_q$. In fact $\alpha \in \mathbb{F}_{q^n}$ and is a normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ if and only if $gcd(e, n) = 1$, where e is the index of q modulo r.

In this case, a normal basis generated by a normal Gauss periods is denoted by *GNB*. We will use of the normal Gauss periods over $\mathbb{F}_3$, listed in the Table 3 in [7], for construction of our tables.

Proposition 2.7 (see [1] and [5]) *Let α be a normal Gauss period of type (n,k) over $\mathbb{F}_3$ and N is the normal basis generated by α. Then*

1. $c_N \leq (k+1)n - k$.
2. *if* $k \equiv 0 \pmod 3$ *then* $c_N \leq nk - 1$.
3. *if* $k = 2$ *or 3 then* $c_N = 3n - 2$.
4. *if* $k = 4$ *then* $c_N \leq 5n - 7$.
5. *if* $k = 5$ *or 6 then* $c_N \leq 6n - 11$.

We give two classes of theorems which allows us to construct even more low complexity normal bases in subfields of finite fields containing optimal normal bases and normal basis generated by a Gauss period.

Proposition 2.8 ([5], Theorem 4.2) *Let α be a type $(n,3)$ Gauss period generating a normal basis N of $\mathbb{F}_{3^n}$ over $\mathbb{F}_3$. Further, suppose $n = ml$ be integers, $\beta = Tr_{3^n|3^m}(\alpha)$ and c_N is the complexity of the normal basis generated by β. Then*

1. *If m and l are odd, then $c_N \leq 3lm - 2$.*
2. *Otherwise, $c_N \leq 3lm - 1$.*

Proposition 2.9 [4] *Let $\alpha \in \mathbb{F}_{q^n}$ generate an optimal normal basis of Type I of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, $n > 2$, and $\beta = Tr_{q^n|q^m}(\alpha)$ with $m = \frac{n}{k}$ and $k \leq m$. Suppose c_N is the complexity of the normal basis generated by β. Then*

1. *If m is even and k is odd, then $c_N \leq (k+1)m - 3k + 2$.*
2. *Otherwise $c_N \leq (k+1)m - k$.*

The normal basis generated by Propositions 2.8 and 2.9 are denoted by *Trace GNB* and *Trace ONB*, respectively.

3. Algorithms

We assume that the arithmetic in $\mathbb{F}_q$ is given. The cost measure of an algorithm will be the number of operations in $\mathbb{F}_q$. The algorithms in this paper use basic polynomial operations like products, divisions, gcd's and to solve linear equation systems. We consider in this paper exclusively FFT (Fast Fourier Transform) based arithmetic, similar results hold for classical arithmetic. Let $M(n) = n\log(n)\log\log(n)$. The cost of multiplying and dividing two polynomials of degree at most n using fast arithmetic ([3], [21], [22]) can be taken as $O(M(n))$ and $O(\log(n)M(n))$, respectively, and the cost of gcd's between two polynomials of degree at most n can be taken as $O(\log(n)M(n))$ operations in $\mathbb{F}_q$.

The cost of computing $h^q \pmod f$ by using the classical *repeated squaring* method (see [14], pp. 441-442), where h is a polynomial over $\mathbb{F}_q$ of degree less than n, is $O(\log(q)M(n))$ in $\mathbb{F}_q$ using FFT based methods. The cost of solving a system of n linear equations with n variables is $O(n^2)$.

The following algorithm is a variant of Algorithm 2.1 in [2]. This algorithm efficiently tests normality of a given irreducible polynomial over $\mathbb{F}_q$.

Algorithm 3.1

Input: *An irreducible polynomial* $f(x) = \sum_{i=0}^{n} c_i x^i \in \mathbb{F}_q[x]$.

output: *Either 'f(x) is normal' or 'f(x) is not normal'.*

1) *if* $c_{n-1} \neq 0$
2) $n := deg(f(x))$;
3) *if* $n = p^e$, *for some* $e \in \mathbb{N}$, *then 'f(x) is a normal polynomial'*
4) *else*
5) *for* $j := 0$ *to* $n-1$
6) $t_j := \sum_{i=0}^{n-1} \left((x^{q^j+1} \pmod{f(x)})\right)^{q^i} \pmod{f(x)}$;
7) *end for*
8) $g := gcd\left(\sum_{j=0}^{n-1} t_j x^j, x^n - 1\right)$;
9) *if* $g = 1$, *then 'f(x) is a normal polynomial'*
10) *else 'f(x) is not a normal polynomial';*
11) *end if*
12) *end if*
13) *else 'f(x) is not a normal polynomial';*
14) *end if*

Obviously, by Notation 2.2, the irreducible polynomial $f(x) = \sum_{i=0}^{n} c_i x^i \in \mathbb{F}_q[x]$ is not an N-polynomial over F_q if $c_{n-1} = 0$. Also according to Proposition 2.3, if $n = p^e$, for some $e \in \mathbb{N}$, then $f(x) = \sum_{i=0}^{n} c_i x^i \in \mathbb{F}_q[x]$ is a normal polynomial over $\mathbb{F}_q$ if and only if $c_{n-1} \neq 0$. So the correctness of the above algorithm is based on Proposition 2.1.

Theorem 3.2 *The above algorithm correctly tests normality of irreducible polynomials, and uses* $O(nM(n)\ (n\log(q) + \log(n)))$ *operations in* $\mathbb{F}_q$.

Proof. The basic idea of this algorithm is to compute $x^{q^j+1} \pmod{f(x)}$ and $(x^{q^j+1})^{q^i} \pmod{f(x)}$ for each $0 \leq i, j \leq n-1$ by repeated squaring method, and then to take the correspondent *gcd*.

Obviously, line 6 of the algorithm computes $t_j = Tr_{q^n|q}(\alpha^{q^j+1})$, for each $0 \leq j \leq n-1$, where $\alpha \in \mathbb{F}_{q^n}$ is a root of $f(x)$. Hence, according to Proposition 2.1, the above algorithm correctly tests normality of irreducible polynomials. Our algorithm computes $x^{q^j} \pmod{f(x)}$, $x^{q^j} \cdot x \pmod{f(x)}$ and $(x^{q^j} \cdot x)^{q^i} \pmod{f(x)}$ for each $0 \leq i, j \leq n-1$. The number of polynomial multiplications in this algorithm, to compute all powers using repeated squaring is $(n-1)\log q + (n-1)^2 \log q$. So the cost of all exponentiations is $O(n^2 M(n)\log(q))$. The number of polynomial multiplications in this algorithm, to compute all $x^{q^j} \cdot x \pmod{f(x)}$, $0 \leq j \leq n-1$

is $n+n\log n$, and so the cost of compute them is $O(nM(n)\log(n))$. Therefore, in the worst case, the total cost of our algorithm, with consideration the cost of a gcd in the algorithm, is $O(nM(n)(n\log(q)+\log(n)))$ using FFT based multiplication algorithms. ∎

Since the elements in a normal basis are exactly the roots of some N-polynomials, there is a canonical one-to-one correspondence between N-polynomials and normal basis. So we may denote the complexity of the normal polynomial $f(x)$ by c_N, when the elements in the normal basis N are exactly the roots of $f(x)$. The following algorithm which is given in [2], computes the complexity of normal polynomials over $\mathbb{F}_q$.

Algorithm 3.3
Input: *An N-polynomial $f(x)$ of degree n over $\mathbb{F}_q$.*
Out put: *The complexity c_N of normal polynomial $f(x)$.*

1) $c_N := 0$;
2) *for* $i := 1$ *to* n
3) *find solution* $T_i = (t_{i1}, t_{i2}, ..., t_{in})$ *of the following linear equation system:*

$$k_i(x) = \sum_{j=1}^{n} t_{ij} r_j(x), \tag{2}$$

where $r_j(x) = x^{q^{j-1}} \pmod{f(x)}$ *and* $k_i(x) = x^{q^{i-1}+1} \pmod{f(x)}$;
4) *for* $j := 1$ *to* n
5) *if* $t_{ij} \neq 0$ *then* $c_N = c_N + 1$;
6) *end for;*
7) *end for;*
8) *return* c_N.

Theorem 3.4 *The above algorithm computes the complexity of a normal polynomial, and uses $O(n(n^2 + M(n)\log(qn)))$ operations in $\mathbb{F}_q$.*

Proof. The basic idea of this algorithm is to compute $x^{q^{i-1}} \pmod{f(x)}$ for each $1 \leq i \leq n$ by repeated squaring, and then to solve the correspondent linear equation system. Clearly, line 3 of the algorithm solves the linear equation system

$$\alpha^{q^{i-1}+1} = \sum_{j=1}^{n} t_{ij} \alpha^{q^{j-1}} \quad 1 \leq i \leq n, \ t_{ij} \in \mathbb{F}_q,$$

where $\alpha \in \mathbb{F}_{q^n}$ is a root of $f(x)$. Hence, by (2), the above algorithm correctly computes the complexity of a normal polynomial.

This algorithm computes $x^{q^j} \pmod{f(x)}$ and $x^{q^j} \cdot x \pmod{f(x)}$ for each $0 \leq j \leq n-1$. The number of polynomial multiplications in this algorithm, to compute all powers using repeated squaring is $(n-1)\log q$. So the cost of all exponentiations is $O(nM(n)\log q)$. The number of polynomial multiplications in

this algorithm to compute all $x^{q^j} \cdot x \pmod{f(x)}$, $0 \leq j \leq n-1$ is $n + n \log n$, and so the cost of to compute them is $O(nM(n)\log(n))$. The cost of solving n times a system of n linear equations and n variables is $O(n^3)$. Therefore, the total cost of this algorithm is $O(n(n^2 + M(n)\log(qn)))$ using FFT based multiplication algorithms. ∎

4. Tables

By using the Algorithms 3.1 and 3.3, in Table 1, a statistical table consist the number of normal polynomials found ($No = \frac{1}{n}\phi_3(x^n - 1)$), minimum and maximum complexities (Min, Max), average, variance and standard deviation of their complexities ($Avg, Var, Std.\ Dev$) is given. Using Table 1 the distribution of the complexity of normal polynomials for finite fields of characteristic three with degree extensions up to 16 is provided. The Tables 3 and 4 give us the current results on the smallest known complexity for the degree extensions from 17 up to 300 by using a combination of theorems and known exact values. For convenience, in the Table 2, using the Proposition 2.5, we list all the values of $n \leq 10000$ for which there is an optimal normal polynomial of degree n over $\mathbb{F}_3$. We also provide a table, in the Table 5, of normal trinomials and pentanomials with minimum complexity among all normal trinomials and pentanomials, respectively over $\mathbb{F}_3$, with their complexities for each degree n with $3^n \leq 10^{50}$. In the continue, either normal trinomials or pentanomials with minimum weight over $\mathbb{F}_3$, for each n, $106 \leq n \leq 300$ are presented. For this, in our search procedure, for a given n, $106 \leq n \leq 300$, we first tried to locate a normal trinomial of degree n over $\mathbb{F}_3$. Failing this, a search was conducted among pentanomials. Among those polynomials, the polynomial $f(x)$ listed is such that the degree of $f(x) - x^n - a_{n-1}x^{n-1}$ for each $a_{n-1} \in \mathbb{F}_3^*$ is lowest. The results of this search procedure in a table in the Table 6 are listed.

The choice of n with $3^n \leq 10^{50}$, and $106 \leq n \leq 300$ as the stopping point for the Tables 5 and 6 respectively, are quite arbitrary, and it should not be particularly difficult to extend the tables to larger values of n. In the Tables 5 and 6 only the nonzero terms are represented. For example the polynomial $x^{35} + x^{34} + 2x^{23} + 2x^{10} + 1$ over $\mathbb{F}_3$ is represented as $35:1, 34:1, 23:2, 10:2, 0:1$. In the Table 5 the first column, headed by $f(x)$, contains the minimum complexity trinomials and pentanomials, the second column headed by c_N, contains the corresponding value of the complexity of $f(x)$, and the third column, headed by No, contains the number of all normal trinomials and pentanomials, which are founded by Algorithm 3.1.

n	No	Min	Max	Avg	Var	Std.Dev	Notes
2	2	4	4	4	0	0	
3	6	7	8	7.3333	0.2222	0.4714	
4	8	7	13	10.75	6.1875	2.4875	Optimal
5	32	13	20	17.0625	7.8086	2.7944	
6	54	11	32	24.3333	22.6667	4.761	Optimal
7	208	24	41	32.7596	15.6249	3.9528	
8	256	22	55	42.8203	29.7099	5.4507	
9	1458	25	69	53.7407	35.7723	5.981	
10	2560	28	85	66.6336	45.0837	6.7144	
11	10648	31	109	80.7938	51.2433	7.1584	
12	17496	49	127	96.071	62.7923	7.9242	
13	70304	58	145	112.6281	73.6445	8.5816	
14	151424	40	168	130.6227	85.6254	9.2534	
15	629856	43	199	150.0063	97.3465	9.8664	
16	819200	31	220	170.6615	110.8023	10.5263	Optimal

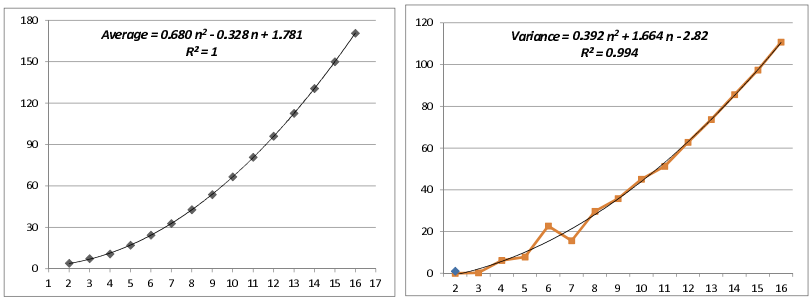

Table 1: The statistics on the complexity of normal polynomials of degree $n \leq 16$ over F_3

In the Table 6, the columns, headed by $f(x)$, contains either normal trinomials or pentanomials with minimum weight. All results in the tables were generated with some matlab programs based on the algorithms, which were stated in the Section . All tables and programs are available in electronic form from the authors.

4	6	16	18	28	30	42	52	78	88
100	112	126	136	138	148	162	172	196	198
210	222	232	256	268	280	282	292	316	330
352	378	388	400	448	460	462	486	508	520
556	568	570	592	606	616	630	640	652	676
690	700	738	750	772	796	808	810	820	822
856	858	880	906	928	940	952	976	1012	1038
1048	1060	1062	1086	1096	1108	1122	1192	1216	1228
1230	1276	1278	1290	1300	1326	1360	1372	1408	1422
1432	1446	1458	1480	1482	1492	1552	1566	1578	1600
1612	1626	1636	1662	1696	1698	1708	1720	1722	1732
1746	1830	1888	1900	1912	1948	1950	1972	1986	1996
1998	2010	2068	2080	2082	2128	2140	2142	2152	2212
2236	2238	2272	2308	2310	2332	2346	2356	2370	2380
2392	2416	2466	2476	2502	2538	2548	2608	2632	2646
2656	2658	2682	2692	2706	2718	2728	2730	2740	2752
2766	2776	2788	2800	2836	2860	2896	2908	2956	2968
3040	3088	3136	3162	3208	3256	3258	3270	3306	3328
3330	3388	3390	3412	3448	3460	3462	3532	3546	3556
3558	3570	3580	3582	3592	3616	3642	3676	3700	3726
3760	3796	3820	3822	3832	3916	3918	3928	3930	3942
3988	4000	4002	4012	4026	4048	4072	4132	4156	4158
4216	4218	4228	4230	4240	4242	4252	4288	4326	4336
4348	4362	4372	4396	4408	4420	4422	4446	4456	4480
4492	4506	4516	4518	4566	4602	4636	4638	4648	4650
4662	4672	4722	4758	4792	4816	4830	4876	4888	4902
4936	4972	4986	4998	5008	5020	5022	5080	5118	5188
5236	5260	5272	5296	5308	5332	5346	5380	5392	5406
5416	5418	5430	5440	5442	5476	5478	5502	5562	5572
5646	5656	5668	5682	5692	5716	5740	5778	5800	5812
5826	5848	5860	5896	5922	5980	6006	6028	6052	6088
6112	6150	6162	6172	6196	6198	6220	6256	6268	6316
6328	6342	6352	6366	6378	6388	6426	6448	6450	6472
6546	6568	6570	6606	6618	6652	6688	6690	6736	6760
6762	6822	6832	6856	6868	6870	6906	6916	6976	7000
7012	7038	7108	7120	7158	7192	7206	7228	7242	7252
7348	7410	7432	7456	7458	7516	7528	7540	7576	7602
7648	7672	7698	7722	7758	7792	7816	7828	7866	7876
7878	7900	7926	7936	7948	8008	8058	8068	8080	8092
8116	8166	8178	8236	8262	8272	8286	8296	8310	8368
8418	8428	8430	8442	8466	8536	8538	8562	8572	8596
8598	8608	8622	8646	8668	8692	8718	8730	8740	8752
8836	8838	8848	8860	8862	8886	8922	8968	8970	9006
9028	9040	9042	9066	9090	9126	9136	9150	9160	9172
9186	9198	9208	9256	9280	9282	9292	9318	9376	9390
9402	9412	9460	9462	9472	9496	9510	9520	9532	9546
9628	9630	9642	9676	9678	9688	9738	9748	9786	9810
9832	9870	9882	9906	9928	9966				

Table 2: All values of $n \leq 10000$ for which there is an optimal normal polynomial of degree n over $\mathbb{F}_3$

n	min	property	Method
17	91	Random	
18	35	Optimal	Pro 2.5
19	176	Random	
20	91	a.b(4,5)	pro 2.6
21	61	Trace ONB(k=2)	pro 2.9
22	64	GNB(k=3)	pro 2.7
23	137	Trace GNB (46, 3)	pro 2.8
24	154	a.b(3,8)	pro 2.6
25	121	Trace ONB(k=4)	pro 2.9
26	76	Trace ONB(k=2)	pro 2.9
27	183	Trace ONB(k=6)	pro 2.9
28	55	Optimal	pro 2.5
29	253	Trace ONB(k=8)	pro 2.9
30	59	Optimal	pro 2.5
31	537	Random	
32	280	GNB(k=8)	pro 2.7
33	187	GNB(k=6)	pro 2.7
34	166	Trace ONB(k=4)	pro 2.9
35	209	Trace GNB (70, 3)	pro 2.8
36	175	a.b(9,4)	pro 2.6
37	181	Trace ONB(k=4)	pro 2.9
38	569	GNB(k=15)	pro 2.7
39	115	Trace ONB(k=2)	pro 2.9
40	286	a.b(8,5)	pro 2.6
41	738	Trace GNB (246, 3)	pro 2.8
42	83	Optimal	pro 2.5
43	211	Trace ONB(k=4)	pro 2.9
44	130	Trace ONB(k=2)	pro 2.9
45	325	a.b(9,5)	pro 2.6
46	136	GNB(k=3)	pro 2.7
47	323	Trace ONB(k=6)	pro 2.9
48	217	a.b(3,16)	pro 2.6
49	241	Trace ONB(k=4)	pro 2.9
50	148	Trace ONB(k=2)	pro 2.9
51	637	a.b(3,17)	pro 2.6
52	103	Optimal	pro 2.5
53	1093	Trace ONB(k=20)	pro 2.9
54	209	Trace ONB(k=3)	pro 2.9
55	319	GNB(k=6)	pro 2.7
56	166	Trace ONB(k=2)	pro 2.9
57	617	Trace ONB(k=10)	pro 2.9
58	283	GNB(k=4)	pro 2.7
59	1103	Trace ONB(k=10)	pro 2.9
60	637	a.b(3,20)	pro 2.6
61	1021	Trace ONB(k=16)	pro 2.9
62	1301	GNB(k=21)	pro 2.7
63	187	Trace ONB(k=2)	pro 2.9
64	313	GNB(k=4)	pro 2.7
65	577	Trace ONB(k=8)	pro 2.9
66	196	GNB(k=3)	pro 2.7
67	331	Trace ONB(k=4)	pro 2.9
68	202	Trace ONB(k=2)	pro 2.9
69	205	Trace ONB(k=2)	pro 2.9
70	208	GNB(k=3)	pro 2.7
71	631	Trace ONB(k=8)	pro 2.9
72	550	a.b(9,8)	pro 2.6
73	361	Trace ONB(k=4)	pro 2.9
74	220	Trace ONB(k=2)	pro 2.9
75	847	a.b(3,25)	pro 2.6
76	1232	a.b(4,19)	pro 2.6
77	744	a.b(7,11)	pro 2.6
78	155	Optimal	pro 2.5
79	391	Trace ONB(k=4)	pro 2.9
80	467	Trace ONB(k=5)	pro 2.9
81	241	Trace ONB(k=2)	pro 2.9
82	737	GNB(k=9)	pro 2.7
83	497	Trace GNB (166, 3)	pro 2.8
84	385	a.b(3,28)	pro 2.6
85	1183	a.b(5,17)	pro 2.6
86	256	Trace ONB(k=2)	pro 2.9
87	1771	a.b(3,29)	pro 2.6

n	min	property	Method
88	175	Optimal	pro 2.5
89	3785	Trace ONB(k=42)	pro 2.9
90	713	GNB(k=7)	pro 2.7
91	1392	a.b(7,13)	pro 2.6
92	541	GNB(k=5)	pro 2.7
93	3759	a.b(3,31)	pro 2.6
94	369	Trace ONB(k=3)	pro 2.9
95	695	Trace ONB(k=6)	pro 2.9
96	1960	a.b(3,32)	pro 2.6
97	1633	Trace ONB(k=16)	pro 2.9
98	292	Trace ONB(k=2)	pro 2.9
99	295	Trace ONB(k=2)	pro 2.9
100	199	Optimal	Pro 2.5
101	701	Trace ONB(k=6)	pro 2.9
102	1213	GNB(k=11)	pro 2.7
103	4387	Trace ONB(k=42)	pro 2.9
104	611	Trace ONB(k=5)	pro 2.9
105	313	Trace ONB(k=2)	pro 2.9
106	1156	GNB(k=10)	pro 2.7
107	955	Trace ONB(k=8)	pro 2.9
108	1281	a.b(4,27)	pro 2.6
109	3349	Trace ONB(k=30)	pro 2.9
110	433	Trace ONB(k=3)	pro 2.9
111	1267	a.b(3,37)	pro 2.6
112	223	Optimal	Pro 2.5
113	3473	Trace ONB(k=30)	pro 2.9
114	673	GNB(k=5)	pro 2.7
115	571	Trace ONB(k=4)	pro 2.9
116	346	Trace ONB(k=2)	pro 2.9
117	5685	Trace ONB(k=48)	pro 2.9
118	1155	Trace ONB(k=9)	pro 2.9
119	1063	Trace ONB(k=8)	pro 2.9
120	2002	a.b(3,40)	pro 2.6
121	361	Trace ONB(k=2)	pro 2.9
122	1090	Trace ONB(k=8)	pro 2.9
123	727	GNB(k=6)	pro 2.7
124	1723	GNB(k=13)	pro 2.7
125	749	Trace GNB (250, 3)	pro 2.8
126	251	Optimal	Pro 2.5
127	631	Trace ONB(k=4)	pro 2.9
128	382	Trace ONB(k=2)	pro 2.9
129	1409	Trace ONB(k=10)	pro 2.9
130	641	GNB(k=4)	pro 2.7
131	785	Trace GNB (262, 3)	pro 2.8
132	910	a.b(3,44)	pro 2.6
133	4224	a.b(7,19)	pro 2.6
134	400	Trace ONB(k=2)	pro 2.9
135	939	Trace ONB(k=6)	pro 2.9
136	271	Optimal	Pro 2.5
137	953	Trace ONB(k=6)	pro 2.9
138	275	Optimal	Pro 2.5
139	691	Trace ONB(k=4)	pro 2.9
140	418	Trace ONB(k=2)	pro 2.9
141	2261	a.b(3,47)	pro 2.6
142	706	Trace ONB(k=4)	pro 2.9
143	1798	a.b(11,13)	pro 2.6
144	775	a.b(9,16)	pro 2.6
145	1585	GNB(k=10)	pro 2.7
146	436	Trace ONB(k=2)	pro 2.9
147	1607	GNB(k=10)	pro 2.7
148	295	Optimal	Pro 2.5
149	1333	Trace ONB(k=8)	pro 2.9
150	889	GNB(k=5)	pro 2.7
151	1051	Trace ONB(k=6)	pro 2.9
152	1360	Trace ONB(k=8)	pro 2.9
153	2275	a.b(9,17)	pro 2.6
154	609	Trace ONB(k=3)	pro 2.9
155	4775	Trace ONB(k=30)	pro 2.9
156	721	a.b(3, 52)	pro 2.6
157	4525	Trace ONB(k=28)	pro 2.9
158	472	Trace ONB(k=2)	pro 2.9

Table 3: The smallest known complexities of normal polynomials of degree $17 \leq n \leq 300$ over $\mathbb{F}_3$

n	min	property	Method
159	5531	GNB(k=34)	pro 2.7
160	796	Trace ONB(k=4)	pro 2.9
161	4961	Trace ONB(k=30)	pro 2.9
162	323	Optimal	Pro 2.5
163	811	Trace ONB(k=4)	pro 2.9
164	973	GNB(k=5)	pro 2.7
165	493	Trace ONB(k=2)	pro 2.9
166	496	GNB(k=3)	pro 2.7
167	7471	Trace ONB(k=44)	pro 2.9
168	1162	a.b(3,56)	pro 2.6
169	841	Trace ONB(k=4)	pro 2.9
170	1523	GNB(k=8)	pro 2.7
171	2051	GNB(k=12)	pro 2.7
172	343	Optimal	pro 2.5
173	1037	Trace GNB (346, 3)	pro 2.8
174	1565	GNB(k=9)	pro 2.7
175	871	Trace ONB(k=4)	pro 2.9
176	526	Trace ONB(k=2)	pro 2.9
177	1234	Trace ONB(k=6)	pro 2.9
178	2669	GNB(k=15)	pro 2.7
179	1603	Trace ONB(k=8)	pro 2.9
180	2275	a.b(9, 20)	pro 2.6
181	1261	Trace ONB(k=6)	pro 2.9
182	2716	GNB(k=14)	pro 2.7
183	2003	Trace ONB(k=10)	pro 2.9
184	1465	GNB(k=7)	pro 2.7
185	1657	Trace ONB(k=8)	pro 2.9
186	2789	GNB(k=15)	pro 2.7
187	1303	Trace ONB(k=6)	pro 2.9
188	1115	Trace ONB(k=5)	pro 2.9
189	565	Trace ONB(k=2)	pro 2.9
190	563	GNB(k=3)	pro 2.7
191	3991	Trace ONB(k=20)	pro 2.9
192	2191	a.b(3,64)	pro 2.6
193	961	Trace ONB(k=4)	pro 2.9
194	580	Trace ONB(k=2)	pro 2.9
195	2135	GNB(k=10)	pro 2.7
196	391	Optimal	pro 2.5
197	3725	Trace ONB(k=18)	pro 2.9
198	395	Optimal	pro 2.5
199	991	Trace ONB(k=4)	pro 2.9
200	598	Trace ONB(k=2)	pro 2.9
201	2201	Trace ONB(k=10)	pro 2.9
202	801	Trace ONB(k=3)	pro 2.9
203	2435	GNB(k=12)	pro 2.7
204	1444	a.b(3,68)	pro 2.6
205	1021	Trace ONB(k=4)	pro 2.9
206	4471	Trace ONB(k=21)	pro 2.9
207	3425	a.b(9,23)	pro 2.6
208	2278	GNB(k=10)	pro 2.7
209	5456	a.b(11,19)	pro 2.6
210	419	Optimal	pro 2.5
211	9032	Trace ONB(k=42)	pro 2.9
212	1261	GNB(k=5)	pro 2.7
213	1485	Trace ONB(k=6)	pro 2.9
214	2344	Trace ONB(k=10)	pro 2.9
215	1499	Trace ONB(k=6)	pro 2.9
216	4026	a.b(8,27)	pro 2.6
217	12888	a.b(7,31)	pro 2.6
218	3224	GNB(k=15)	pro 2.7
219	2527	a.b(3,73)	pro 2.6
220	1093	GNB(k=4)	pro 2.7
221	1541	Trace ONB(k=6)	pro 2.9
222	443	Optimal	pro 2.5
223	6883	Trace ONB(k=30)	pro 2.9
224	670	Trace ONB(k=2)	pro 2.9
225	3025	a.b(9,25)	pro 2.6
226	3389	GNB(k=15)	pro 2.7
227	N/A		
228	4319	a.b(4,57)	pro 2.6
229	7069	Trace ONB(k=30)	pro 2.9

n	min	property	Method
230	688	Trace ONB(k=2)	pro 2.9
231	784	Trace ONB(k=2)	pro 2.9
232	463	Optimal	pro 2.5
233	7657	Trace ONB(k=32)	pro 2.9
234	1393	GNB(k=5)	pro 2.7
235	1171	Trace ONB(k=4)	pro 2.9
236	2116	Trace ONB(k=8)	pro 2.9
237	1653	Trace ONB(k=6)	pro 2.9
238	1183	GNB(k=4)	pro 2.7
239	2143	Trace ONB(k=8)	pro 2.9
240	1333	a.b(15,16)	pro 2.6
241	1681	Trace ONB(k=6)	pro 2.9
242	1444	a.b(2,121)	pro 2.6
243	727	Trace ONB(k=2)	pro 2.9
244	1216	Trace ONB(k=4)	pro 2.9
245	3133	a.b(5,49)	pro 2.6
246	736	GNB(k=3)	pro 2.7
247	1723	Trace ONB(k=6)	pro 2.9
248	2965	Trace ONB(k=11)	pro 2.9
249	2240	GNB(k=9)	pro 2.7
250	748	GNB(k=3)	pro 2.7
251	4751	Trace ONB(k=18)	pro 2.9
252	1309	a.b(4,63)	pro 2.6
253	1258	GNB(k=4)	pro 2.7
254	760	Trace ONB(k=2)	pro 2.9
255	3811	Optimal	pro 2.5
256	511	Optimal	pro 2.5
257	N/A		
258	1573	GNB(k=5)	pro 2.7
259	4344	a.b(7,37)	pro 2.6
260	778	Trace ONB(k=2)	pro 2.9
261	1551	GNB(k=6)	pro 2.7
262	785	GNB(k=3)	pro 2.7
263	1835	Trace ONB(k=6)	pro 2.9
264	1225	a.b(3,88)	pro 2.6
265	1321	Trace ONB(k=4)	pro 2.9
266	2386	Trace ONB(k=8)	pro 2.9
267	26495	a.b(3,89)	pro 2.6
268	535	Optimal	pro 2.5
269	2413	Trace ONB(k=8)	pro 2.9
270	1077	Trace ONB(k=3)	pro 2.9
271	1891	Trace ONB(k=6)	pro 2.9
272	1621	GNB(k=5)	pro 2.7
273	2760	a.b(7,39)	pro 2.6
274	1089	Trace ONB(k=3)	pro 2.9
275	3299	GNB(k=12)	pro 2.7
276	1435	a.b(4,69)	pro 2.6
277	1381	Trace ONB(k=4)	pro 2.9
278	832	Trace ONB(k=2)	pro 2.9
279	5285	Trace ONB(k=18)	pro 2.9
280	559	Optimal	pro 2.5
281	8681	Trace ONB(k=30)	pro 2.9
282	563	Optimal	pro 2.5
283	1975	Trace ONB(k=6)	pro 2.9
284	850	Trace ONB(k=2)	pro 2.9
285	853	Trace ONB(k=2)	pro 2.9
286	1137	Trace ONB(k=3)	pro 2.9
287	2003	Trace ONB(k=6)	pro 2.9
288	7000	a.b(9,32)	pro 2.6
289	8353	Trace ONB(k=28)	pro 2.9
290	3679	a.b(5,58)	pro 2.6
291	2031	Trace ONB(k=6)	pro 2.9
292	583	Optimal	pro 2.5
293	6133	Trace ONB(k=20)	pro 2.9
294	1753	GNB(k=5)	pro 2.7
295	14399	a.b(5,59)	pro 2.6
296	886	Trace ONB(k=2)	pro 2.9
297	4441	Trace ONB(k=14)	pro 2.9
298	1486	Trace ONB(k=4)	pro 2.9
299	2683	Trace ONB(k=8)	pro 2.9
300	1393	a.b(3,100)	pro 2.6

Table 4: Continue of Table 3.

f(x)	C_N	No	f(x)	C_N	No
2:1,1:1,0:2	4	2	52:1,51:1,37:2,14:1,0:2	1685	300
3:1,2:1,0:2	7	2	53:1,52:1,34:2,19:2,0:2	1758	642
4:1,3:1,0:2	13	2	54:1,53:1,35:1,33:1,0:1	1857	458
4:1,3:1,2:1,1:1,0:1	7	4	55:1,54:1,49:2,15:2,0:2	1923	508
5:1,4:1,0:2	19	2	56:1,55:1,10:1,7:2,0:2	1951	276
5:1,4:1,2:1,1:2,0:2	13	14	57:1,56:1,26:2,4:2,0:1	2072	590
6:1,5:1,3:2,2:2,0:1	16	16	58:1,57:1,55:1,7:1,0:1	2152	420
7:1,6:1,3:2,2:2,0:2	24	38	59:1,58:1,42:2,33:2,0:2	2207	652
8:1,7:1,6:1,2:2,0:2	39	14	60:1,59:1,27:2,23:1,0:2	2310	318
9:1,8:1,3:2,1:2,0:2	43	62	61:1,60:1,52:2,37:2,0:2	2355	844
10:1,9:1,8:2,2:2,0:1	57	46	62:1,61:1,51:1,15:2,0:2	2448	502
11:1,10:1,7:1,3:2,0:2	66	86	63:1,62:1,45:2,27:1,0:2	2537	772
12:1,11:1,3:2,1:2,0:2	81	40	64:1,63:1,27:1,20:1,0:1	2607	368
13:1,12:1,0:2	121	2	65:1,64:1,20:2,7:2,0:1	2692	676
13:1,12:1,11:2,10:1,0:2	95	110	66:1,65:1,15:1,13:2,0:2	2785	604
14:1,13:1,8:1,3:1,0:1	112	78	67:1,66:1,60:2,10:2,0:1	2872	676
15:1,14:1,8:1,3:1,0:1	126	152	68:1,67:1,44:2,43:2,0:2	2962	398
16:1,15:1,11:1,2:1,0:1	149	80	69:1,68:1,64:1,36:2,0:2	3048	804
17:1,16:1,0:2	189	2	70:1,69:1,34:2,32:2,0:1	3118	584
17:1,16:1,7:2,2:2,0:2	160	150	71:1,70:1,61:2,50:1,0:2	3226	768
18:1,17:1,9:2,8:2,0:1	52	130	72:1,71:1,68:1,8:2,0:2	3348	296
19:1,18:1,8:2,3:2,0:1	218	176	73:1,72:1,0:2	3390	2
20:1,19:1,6:2,5:2,0:2	239	108	73:1,72:1,69:2,15:1,0:2	3410	980
21:1,20:1,15:2,4:2,0:1	258	206	74:1,73:1,66:2,35:2,0:1	3497	640
22:1,21:1,14:1,9:1,0:1	275	150	75:1,74:1,42:2,11:2,0:2	3600	950
23:1,22:1,19:2,14:2,0:1	317	226	76:1,75:1,23:1,11:2,0:2	3690	610
24:1,23:1,10:1,3:1,0:1	356	92	77:1,76:1,57:2,36:1,0:2	3800	990
25:1,24:1,8:2,3:2,0:1	377	282	78:1,77:1,66:2,38:1,0:2	3900	596
26:1,25:1,15:2,13:2,0:2	409	156	79:1,78:1,68:1,63:1,0:1	3998	750
27:1,26:1,15:1,3:2,0:2	435	274	80:1,79:1,35:1,4:1,0:1	4120	392
28:1,27:1,26:1,1:2,0:2	82	210	81:1,80:1,48:1,16:2,0:2	4192	1002
29:1,28:1,15:2,14:1,0:2	511	302	82:1,81:1,48:1,11:1,0:1	4293	672
30:1,29:1,5:1,3:1,0:1	551	258	83:1,82:1,67:1,1:1,0:1	4387	1124
31:1,30:1,21:2,11:2,0:2	588	260	84:1,83:1,53:2,10:2,0:1	4543	528
32:1,31:1,22:1,17:2,0:2	629	158	85:1,84:1,54:1,48:2,0:2	4619	1278
33:1,32:1,8:2,4:2,0:1	679	316	86:1,85:1,46:1,15:2,0:2	4771	708
34:1,33:1,24:2,20:1,0:2	707	230	87:1,86:1,83:2,55:1,0:2	4881	1144
35:1,34:1,23:2,10:2,0:1	754	402	88:1,87:1,66:1,35:1,0:1	5000	494
36:1,35:1,33:1,17:1,0:1	805	194	89:1,88:1,52:2,48:2,0:1	5111	1114
37:1,36:1,35:2,3:1,0:2	856	458	90:1,89:1,77:2,35:1,0:2	5201	888
38:1,37:1,15:1,13:1,0:1	891	272	91:1,90:1,71:2,6:2,0:1	5335	782
39:1,38:1,15:2,13:2,0:2	963	340	92:1,91:1,80:1,9:2,0:2	5475	668
40:1,39:1,28:2,23:2,0:2	1008	232	93:1,92:1,81:2,55:1,0:2	5577	1098
41:1,40:1,0:2	1116	2	94:1,93:1,53:2,8:1,0:2	5656	802
41:1,40:1,17:2,11:1,0:2	1038	520	95:1,94:1,9:2,3:2,0:2	5801	1168
42:1,41:1,26:1,14:2,0:2	1104	382	96:1,95:1,41:2,22:2,0:1	5958	452
43:1,42:1,26:1,25:1,0:1	1138	374	97:1,96:1,18:1,11:1,0:1	6089	1270
44:1,43:1,18:2,17:2,0:2	1226	270	98:1,97:1,43:2,33:1,0:2	6186	850
45:1,44:1,22:1,4:2,0:2	1275	486	99:1,98:1,57:2,18:2,0:2	6340	1270
46:1,45:1,19:2,15:1,0:2	1330	380	100:1,99:1,94:2,33:2,0:2	6449	748
47:1,46:1,44:1,39:2,0:2	1391	522	101:1,100:1,66:1,26:2,0:2	6581	1260
48:1,47:1,44:2,13:2,0:1	1475	198	102:1,101:1,54:2,52:2,0:1	6731	1018
49:1,48:1,26:2,14:1,0:2	1488	702	103:1,102:1,75:2,29:1,0:2	6864	1054
50:1,49:1,40:2,10:2,0:1	1549	366	104:1,103:1,27:1,18:1,0:1	6995	454
51:1,50:1,0:2	1705	2	105:1,104:1,33:2,28:2,0:2	7106	1146
51:1,50:1,42:2,33:2,0:2	1658	576			

Table 5: Minimum complexity trinomials and pentanomials of degree $n \leq 105$ over F_3 with their complexities

106:1,105:1,10:2,1:2,0:2	156:1,155:1,27:2,1:1,0:2	206:1,205:1,25:1,1:2,0:2	256:1,255:1,15:2,1:1,0:2
107:1,106:1,14:2,1:2,0:1	157:1,156:1,6:1,1:1,0:1	207:1,206:1,8:1,1:2,0:2	257:1,256:1,9:1,1:2,0:2
108:1,107:1,16:2,1:2,0:2	158:1,157:1,28:1,1:1,0:1	208:1,207:1,26:1,1:2,0:2	258:1,257:1,12:1,1:1,0:1
109:1,108:1,17:2,1:2,0:2	159:1,158:1,24:2,1:2,0:1	209:1,208:1,12:1,1:2,0:2	259:1,258:1,28:1,1:2,0:2
110:1,109:1,49:2,1:1,0:2	160:1,159:1,2:2,1:2,0:1	210:1,209:1,43:1,1:1,0:1	260:1,259:1,10:2,1:2,0:2
111:1,110:1,16:1,1:1,0:1	161:1,160:1,17:2,1:2,0:2	211:1,210:1,9:1,1:2,0:2	261:1,260:1,19:2,1:2,0:2
112:1,111:1,14:1,1:1,0:1	162:1,161:1,15:2,1:2,0:2	212:1,211:1,28:2,1:2,0:1	262:1,261:1,6:1,1:1,0:1
113:1,112:1,10:2,1:2,0:2	163:1,162:1,11:1,1:2,0:2	213:1,212:1,8:1,1:1,0:1	263:1,262:1,12:1,1:2,0:2
114:1,113:1,28:1,1:2,0:2	164:1,163:1,17:2,1:1,0:2	214:1,213:1,24:1,1:1,0:1	264:1,263:1,83:2,1:1,0:2
115:1,114:1,2:2,1:2,0:2	165:1,164:1,4:1,1:2,0:2	215:1,214:1,13:1,1:2,0:2	265:1,264:1,12:1,1:1,0:1
116:1,115:1,17:1,1:2,0:2	166:1,165:1,6:1,1:1,0:1	216:1,215:1,18:1,1:2,0:2	266:1,265:1,11:1,1:2,0:2
117:1,116:1,12:1,1:2,0:2	167:1,166:1,18:1,1:1,0:1	217:1,216:1,30:2,1:2,0:2	267:1,266:1,2:2,1:2,0:2
118:1,117:1,22:2,1:2,0:1	168:1,167:1,6:2,1:2,0:1	218:1,217:1,8:1,1:2,0:2	268:1,267:1,110:1,1:1,0:1
119:1,118:1,8:2,1:2,0:2	169:1,168:1,6:1,1:2,0:2	219:1,218:1,2:2,1:2,0:2	269:1,268:1,5:2,1:1,0:2
120:1,119:1,14:2,1:2,0:1	170:1,169:1,3:2,1:1,0:2	220:1,219:1,3:2,1:1,0:2	270:1,269:1,16:1,1:1,0:1
121:1,120:1,0:2	171:1,170:1,23:2,1:1,0:2	221:1,220:1,4:2,1:2,0:1	271:1,270:1,3:2,1:2,0:2
122:1,121:1,11:2,1:2,0:2	172:1,171:1,7:1,1:1,0:1	222:1,221:1,16:2,1:2,0:1	272:1,271:1,94:1,1:2,0:2
123:1,122:1,4:1,1:2,0:2	173:1,172:1,20:1,1:1,0:1	223:1,222:1,15:2,1:1,0:2	273:1,272:1,29:2,1:2,0:2
124:1,123:1,38:1,1:1,0:1	174:1,173:1,46:2,1:2,0:1	224:1,223:1,28:2,1:2,0:1	274:1,273:1,53:2,1:1,0:2
125:1,124:1,11:1,1:1,0:1	175:1,174:1,28:2,1:2,0:1	225:1,224:1,11:1,1:2,0:2	275:1,274:1,10:2,1:2,0:2
126:1,125:1,6:2,1:2,0:2	176:1,175:1,163:1,1:1,0:1	226:1,225:1,22:2,1:2,0:2	276:1,275:1,15:1,1:1,0:1
127:1,126:1,3:1,1:2,0:2	177:1,176:1,16:1,1:1,0:1	227:1,226:1,13:1,1:2,0:2	277:1,276:1,8:1,1:2,0:2
128:1,127:1,10:1,1:1,0:1	178:1,177:1,22:2,1:2,0:2	228:1,227:1,16:2,1:2,0:2	278:1,277:1,9:1,1:2,0:2
129:1,128:1,2:2,1:2,0:2	179:1,178:1,9:1,1:2,0:2	229:1,228:1,3:1,1:1,0:1	279:1,278:1,15:1,1:2,0:2
130:1,129:1,51:1,1:2,0:2	180:1,179:1,115:2,1:1,0:2	230:1,229:1,22:2,1:2,0:1	280:1,279:1,14:1,1:2,0:2
131:1,130:1,4:2,1:2,0:1	181:1,180:1,7:1,1:1,0:1	231:1,230:1,42:2,1:2,0:1	281:1,280:1,3:1,1:2,0:2
132:1,131:1,18:1,1:1,0:1	182:1,181:1,13:1,1:2,0:2	232:1,231:1,90:2,1:2,0:2	282:1,281:1,15:2,1:1,0:2
133:1,132:1,11:2,1:2,0:2	183:1,182:1,42:2,1:2,0:2	233:1,232:1,29:2,1:2,0:2	283:1,282:1,3:1,1:2,0:2
134:1,133:1,10:1,1:1,0:1	184:1,183:1,13:2,1:1,0:2	234:1,233:1,11:2,1:2,0:2	284:1,283:1,19:2,1:1,0:2
135:1,134:1,16:1,1:2,0:2	185:1,184:1,6:1,1:1,0:1	235:1,234:1,2:2,1:2,0:1	285:1,284:1,18:1,1:1,0:1
136:1,135:1,20:2,1:2,0:1	186:1,185:1,8:1,1:2,0:2	236:1,235:1,4:2,1:2,0:1	286:1,285:1,33:1,1:2,0:2
137:1,136:1,0:2	187:1,186:1,15:2,1:1,0:2	237:1,236:1,14:1,1:1,0:1	287:1,286:1,2:2,1:2,0:1
138:1,137:1,46:2,1:2,0:1	188:1,187:1,3:1,1:1,0:1	238:1,237:1,3:1,1:2,0:2	288:1,287:1,34:2,1:2,0:1
139:1,138:1,2:2,1:2,0:1	189:1,188:1,9:1,1:2,0:2	239:1,238:1,12:2,1:2,0:1	289:1,288:1,8:1,1:1,0:1
140:1,139:1,23:1,1:1,0:1	190:1,189:1,40:1,1:1,0:1	240:1,239:1,17:1,1:2,0:2	290:1,289:1,8:2,1:2,0:1
141:1,140:1,5:1,1:1,0:1	191:1,190:1,13:2,1:1,0:2	241:1,240:1,2:1,1:2,0:2	291:1,290:1,25:2,1:2,0:2
142:1,141:1,4:1,1:1,0:1	192:1,191:1,14:2,1:2,0:1	242:1,241:1,91:1,1:2,0:2	292:1,291:1,3:2,1:1,0:2
143:1,142:1,5:1,1:2,0:2	193:1,192:1,5:1,1:1,0:1	243:1,242:1,45:1,1:2,0:2	293:1,292:1,10:1,1:1,0:1
144:1,143:1,18:2,1:2,0:1	194:1,193:1,40:2,1:2,0:1	244:1,243:1,31:1,1:1,0:1	294:1,293:1,40:2,1:2,0:1
145:1,144:1,2:1,1:2,0:2	195:1,194:1,11:1,1:1,0:1	245:1,244:1,24:2,1:2,0:1	295:1,294:1,56:2,1:2,0:2
146:1,145:1,28:2,1:2,0:1	196:1,195:1,3:2,1:1,0:2	246:1,245:1,88:1,1:1,0:1	296:1,295:1,102:1,1:2,0:2
147:1,146:1,3:1,1:2,0:2	197:1,196:1,45:1,1:2,0:2	247:1,246:1,21:1,1:2,0:2	297:1,296:1,78:1,1:1,0:1
148:1,147:1,26:1,1:2,0:2	198:1,197:1,22:1,1:1,0:1	248:1,247:1,20:2,1:2,0:1	298:1,297:1,34:2,1:2,0:2
149:1,148:1,10:1,1:2,0:2	199:1,198:1,15:1,1:2,0:2	249:1,248:1,11:2,1:2,0:2	299:1,298:1,10:1,1:1,0:1
150:1,149:1,21:1,1:2,0:2	200:1,199:1,19:2,1:2,0:2	250:1,249:1,107:2,1:1,0:2	300:1,299:1,3:2,1:1,0:2
151:1,150:1,39:2,1:1,0:2	201:1,200:1,20:1,1:2,0:2	251:1,250:1,53:1,1:2,0:2	
152:1,151:1,7:2,1:1,0:2	202:1,201:1,53:2,1:1,0:2	252:1,251:1,33:1,1:1,0:1	
153:1,152:1,7:1,1:2,0:2	203:1,202:1,10:2,1:2,0:1	253:1,252:1,40:1,1:1,0:1	
154:1,153:1,35:1,1:1,0:1	204:1,203:1,12:1,1:2,0:2	254:1,253:1,26:1,1:1,0:1	
155:1,154:1,2:1,1:2,0:2	205:1,204:1,18:1,1:1,0:1	255:1,254:1,4:2,1:2,0:2	

Table 6: All normal trinomials or pentanomials with minimum weight of degree $106 \leq n \leq 300$ over F_3

5. Conjectures

By using the data in the Table 1, the statements of conjectures, which have been stated in [15] for finite fields with characteristic two, are studied for finite fields of characteristic three. the results of our studying procedure are described in the following conjectures.

Conjecture 5.1 *An upper bound for average of the complexities of normal polynomials of degree n over $\mathbb{F}_3$ is $\frac{n^2-n+2}{3}$.*

Conjecture 5.2 *An upper bound for variance of the complexities of normal polynomials of degree n over $\mathbb{F}_3$ is $\frac{n^2+3n-5}{2}$.*

Conjecture 5.3 *Since the probability of finding a normal polynomial of complexity $c_N \leq kn$ is similar to finding the density under the normalized curve as $P(c_N \leq kn) = P\left[Z \leq \frac{(kn-\mu)}{\sigma}\right]$, where μ and σ^2 denote the average and the variance of the complexities of normal polynomials of degree n over $\mathbb{F}_3$, respectively. So, according to the above conjectures, by giving $\mu = \frac{n^2-n+2}{3}$ and $\sigma^2 = \frac{n^2+3n-5}{2}$, computing the Z-score of kn gives $z_p = \frac{kn-\frac{n^2-n+2}{3}}{\sqrt{\frac{n^2+3n-5}{2}}}$. Hence, it is obvious that if k is a constant, then the Z-score becomes infinitely small. Relating this to the complexity distribution, this implies that the upper bound on the minimum complexity vanishes, which is a contradiction since the minimum possible complexity is $2n-1$. So there is no constant k such that the complexity c_N of $\mathbb{F}_{3^n}$ is bounded above by kn for all n.*

References

[1] Ahmadi, O., Hankerson, D., Menezes, A., *Software Implementation of Arithmetic in $\mathbb{F}_{3^m}$*, Lecture Notes in Computer Science, 2007, 85-102.

[2] Alizadeh, M., *Some algorithms for normality testing irreducible polynomials and computing complexity of the normal polynomials over finite fields*, Applied Mathematical Sciences, vol. 6, no. 40 (2012), 1997-2003.

[3] Cantor, D., Kaltofen, E., *On fast multiplication of polynomials over arbitrary algebras*, Acta. Inform., 28 (1991), 693-701.

[4] Christopoulou, M., Garefalakis, T., Panario, D., Thomson, D., *The trace of an optimal normal element and low complexity normal bases*, Des. Codes Cryptogr, 49 (2008), 199-215.

[5] Christopoulou, M., Garefalakis, T., Panario, D., Thomson, D., *Gauss periods as constructions of low complexity normal bases*, Des. Codes Cryptogr., vol. 62, issue 1 (2012), 43-62.

[6] COHEN, H., FREY, G., *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, Discrete Mathematics and its Applications Series, Chapman and Hall/CRC, 2006.

[7] FEISEL, S., GATHEN, J. VON ZUR, SHOKROLLAHI, M.A., *Normal Bases via General Gauss Periods*, Mathematics of Computation, vol. 68, no. 225 (1999), 271-290.

[8] GEISELMANN, W., *Algebraische Algorithmenentwicklung am Beispiel der Arithmetik in endlichen Körpern*, Dissertation, Universität Karlsruhe, 1992.

[9] GRABHER, P., PAGE, D., *Hardware acceleration of the Tate pairing in characteristic three*, Cryptographic Hardware and Embedded Systems-CHES 2005, LNCS 3659 (2005), 398-411.

[10] GRANGER, R., PAGE, D., STAM, M., *Hardware and software normal basis arithmetic for pairing based cryptography in characteristic three*, IEEE Transactions on Computers, 54 (2005), 852-860.

[11] HARRISON, K., PAGE, D., SMART, N., *Software implementation of finite fields of characteristic three, for use in pairing-based cryptosystems*, LMS Journal of Computation and Mathematics, 5 (2002), 181-193.

[12] JUNGNICKEL, D., *Finite Fields: Structure and Arithmetics*, B.I. Wissenschaftsverlag, Mannheim, Germany, 1993.

[13] KERINS, T., MARNANE, W., POPOVICI, E., BARRETO, P., *Efficient hardware for the Tate pairing calculation in characteristic three*, Cryptographic Hardware and Embedded Systems-CHES 2005, LNCS 3659 (2005), 412-426.

[14] KNUTH, D., *The art of computer programming*, Vol. 2: *Seminumerical algorithms*, 2nd ed. Addison-Wesley, Reading MA, 1981.

[15] MASUDA, A.M., MOURA, L., PANARIO, D., THOMSON, D., *Low Complexity Normal Elements over Finite Fields of Characteristic Two*, IEEE Trans. Comput., 57 (2008), 990-1001.

[16] MENEZES, A.J., BLAKE, I.F., GAO, X., MULLIN, R.C., VANSTONE, S.A., YAGHOOBIAN, T., *Applications of finite fields*, Kluwer Academic Publishers, Boston, Dordrecht, Lancaster, 1993.

[17] MORGAN, I.H., MULLEN, G.L., *Primitive normal polynomial over finite fields*, Math. Computation, 63 (1994), 759-765; Supplement: S19-S23.

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

[19] PAGE, D., SMART, N., *Hardware implementation of finite fields of characteristic three*, Cryptographic Hardware and Embedded Systems-CHES 2002, LNCS 2523 (2003), 529-539.

[20] Peterson, W.W., Weldon, E.J., Jr., *Error-correcting codes*, MIT Press, Cambridge, 1972.

[21] Schönhage, A., *Schnelle Multiplikation von Polynomenüber Körpern der Charakteristik 2*, Acta Inf., no. 7 (1977), 395-398.

[22] Schönhage, A., Strassen, V., *Schnelle Multiplikation großer Zahlen*, Computing, 7 (1971), 281-292.

[23] Seroussi, G., *Hewlett-Packard Laboratories, Table of Low-weight Binary Irreducible Polynomials,* Hewlett Packard Laboratories, (15 page), 1998.

Accepted: 07.02.2014