BULLETIN OF THE POLISH
ACADEMY OF SCIENCES
MATHEMATICS
Vol. 59, No. 3, 2011

On Fully Split Lacunary Polynomials in Finite Fields

by

Khodakhast BIBAK and Igor E. SHPARLINSKI

Presented by Andrzej SCHINZEL

Summary. We estimate the number of possible degree patterns of k-lacunary polynomials of degree $t < p$ which split completely modulo p. The result is based on a combination of a bound on the number of zeros of lacunary polynomials with some graph theory arguments.

1. Introduction. Zeros and factorisations of lacunary polynomials, that is, polynomials of high degree with relatively small number of non-zero coefficients, have always been a subject of active investigation: see [2, 4, 7, 8, 10] and references therein. We say that a polynomial f over a field $\mathbb{K}$ is *k-lacunary* if it has at most $k+1$ non-zero coefficients, including a non-zero constant term, that is, if $f(0) \neq 0$ and

$$f(X) = a_0 + a_1 X^{t_1} + \cdots + a_k X^{t_k} \in \mathbb{K}[X] \tag{1}$$

for some positive integers $t_1 < \cdots < t_k$.

For example, a classical result of Descartes asserts that a k-lacunary polynomial $f \in \mathbb{R}[X]$ may have at most $2k$ real roots. Furthermore, Lenstra [8] has shown that for an algebraic number field $\mathbb{K}$ of degree m over $\mathbb{Q}$ and a k-lacunary polynomial $f \in \mathbb{K}[X]$, the product g of all irreducible divisors $h \mid f$ of degree at most $\deg h \le d$ is of degree

$$\deg g = O(k^2 2^{md} md \log(2mdk)).$$

Schinzel [10] has obtained a series of statistical results about the number of k-lacunary irreducible polynomials with prescribed coefficients. In particular, by [10, Corollary 2], for any algebraic numbers $a_0, \ldots, a_k$ there are at

2010 *Mathematics Subject Classification*: Primary 11T06; Secondary 05C69.
Key words and phrases: roots of lacunary polynomials, finite fields, domination number.

DOI: 10.4064/ba59-3-1

most $O(T^{\lfloor (k+1)/2 \rfloor})$ k-tuples of integers

$$\mathbf{t} = (t_1, \dots, t_k), \quad 1 \le t_1 < \cdots < t_k, \tag{2}$$

with $t_k \le T$ and such that the largest non-cyclotomic factor (that is, a factor which does not have roots that are roots of unity) of the k-lacunary polynomial (1) is reducible over $\mathbb{K} = \mathbb{Q}(a_1/a_0, \dots, a_k/a_0)$.

Here we consider a related question about estimating the number $N_k(p,t)$ of k-tuples (2) such that there is a k-lacunary polynomial of the form (1) of degree $t_k = t$ over the finite field $\mathbb{K} = \mathbb{F}_p$ of p elements, where p is a prime, that fully splits over $\mathbb{F}_p$.

THEOREM 1. *If a positive integer k is fixed then for any prime p and positive integer $t < p$, we have*

$$N_k(p,t) \le t^{k-k\lceil (k-3)/2 \rceil - 1} p^{(k-1)\lceil (k-3)/2 \rceil + o(1)}$$

as $p \to \infty$.

Clearly, Theorem 1 is non-trivial only for $k > 3$ and for

$$t > p^{1-1/k+\varepsilon}, \tag{3}$$

with some fixed $\varepsilon > 0$. Furthermore, for $t \gg p$ we obtain the bound

$$N_k(p,t) \le t^{\lceil k/2 \rceil + 1 + o(1)}.$$

Our result is based on a rather unusual combination of two techniques: a bound on the number of zeros of lacunary polynomials (see Section 2) and a bound on the so-called domination number of a graph (see Section 3).

Throughout the paper, the implied constants in the symbols 'O', '$\ll$' and '$\gg$' may depend on k (we recall that the notations $U \ll V$ and $V \gg U$ are equivalent to $U = O(V)$).

2. Zeros of lacunary polynomials. We need the following estimate from [1] on the number of zeros of lacunary polynomials over $\mathbb{F}_p$.

LEMMA 2. *For $k + 1 \ge 2$ elements $a_0, a_1, \dots, a_k \in \mathbb{F}_p^*$ and integers $0 = t_0 < t_1 < \cdots < t_k < p$, the number of solutions Q to the equation*

$$\sum_{i=0}^{k} a_i x^{t_i} = 0, \quad x \in \mathbb{F}_p^*,$$

with $t_0 = 0$, satisfies

$$Q \le 2p^{1-1/k} D^{1/k} + O(p^{1-2/k} D^{2/k}),$$

where

$$D = \min_{0 \le i \le k} \max_{j \ne i} \gcd(t_j - t_i, p-1).$$

LEMMA 3. *For $k+1 \geq 2$ elements $a_0, a_1, \ldots, a_k \in \mathbb{F}_p^*$ and integers $0 = t_0 < t_1 < \cdots < t_k < p$, the multiplicity of any root ρ of the polynomial*

$$\sum_{i=0}^{k} a_i X^{t_i} \in \mathbb{F}_p[X]$$

is at most k.

Proof. Let

$$F(X) = \sum_{i=0}^{k} a_i X^{t_i}.$$

Then for the jth derivative $F^{(j)}(X)$ we have

$$F^{(j)}(X)X^j = \sum_{i=0}^{k} \prod_{h=0}^{j-1} (t_i - h) a_i X^{t_i}$$

(where as usual, we set $F^{(0)}(X) = F(X)$). Thus, if $r \neq 0$ is a root of multiplicity at least $k+1 \leq t_k < p$ in the algebraic closure of $\mathbb{F}_p$, then

$$F^{(j)}(r) = 0, \qquad j = 0, \ldots, k.$$

Therefore, the homogeneous system of equations

$$\sum_{i=0}^{k} \prod_{h=0}^{j-1} (t_i - h) x_i = 0, \qquad j = 0, \ldots, k,$$

has a non-zero solution $x_i = a_i r^{t_i}$, $i = 0, \ldots, k$. This implies

$$\det\Big[\Big(\prod_{h=0}^{j-1} (t_i - h)\Big)_{i,j=0,\ldots,k}\Big] = 0,$$

which is impossible for $0 = t_0 < t_1 < \cdots < t_k < p$ as an easy calculation shows that

$$\det\Big[\Big(\prod_{h=0}^{j-1} (t_i - h)\Big)_{i,j=0,\ldots,k}\Big] = \prod_{0 \leq i < j \leq k} (t_j - t_i) \neq 0.$$

The above contradiction implies the desired result. ∎

3. Domination number of a graph. Let $G = (V, E)$ be a simple undirected graph of order n. A *dominating set* S of G is a vertex subset such that any vertex of $V \setminus S$ has a neighbour in S. Intuitively, a dominating set of a graph is a vertex subset whose elements, along with their neighbours, make up the vertex set of the graph.

The minimum cardinality of a dominating set of G is called the *domination number* $\gamma(G)$ of G. In other words,

$$\gamma(G) = \min_{S \subseteq V(G)} \Big\{ |S| : V(G) \subseteq \bigcup_{v \in S} \hat{N}(v) \Big\},$$

where $\hat{N}(v)$ denotes the closed neighbourhood of a vertex v.

We denote by $\delta(G)$ the minimum degree of G.

When $\delta(G)$ is large enough, there are very good upper bounds for the domination number of the graph G in terms of $\delta(G)$ and n (see, for example, [3, 6]). However, for small values of $\delta(G)$ the classical result of Ore [9] is stronger and provides an upper bound for the domination number of a graph with no isolated vertices:

LEMMA 4. *If G is a graph of order n with $\delta(G) \geq 1$, then*

$$\gamma(G) \leq n/2.$$

4. Proof of Theorem 1. Since $p > t_k$, by Lemma 3 the multiplicity of each non-zero root of a polynomial of the form (1) does not exceed k. Hence, if a polynomial $F(X) \in \mathbb{F}_p[X]$ of the form (1) splits completely over $\mathbb{F}_p$ then the equation

$$a_0 + a_1 x^{t_1} + \cdots + a_n x^{t_k} = 0, \qquad x \in \mathbb{F}_p^*,$$

with $1 \leq t_1 < \cdots < t_k$ has at least t_k/k solutions. Then, from Lemma 2 we have

$$t_k/k = O(p^{1-1/k} D_{\mathbf{t}}^{1/k}),$$

where

$$D_{\mathbf{t}} = \min_{0 \leq i \leq n} \max_{j \neq i} \gcd(t_j - t_i, p-1).$$

Thus $D_{\mathbf{t}} t \mid p-1$ and, since k is fixed,

$$t \geq D_{\mathbf{t}} \gg t_k^k p^{-(k-1)} = t^k p^{-(k-1)}. \tag{4}$$

We now fix $D \mid p-1$, and for each $\mathbf{t} = (t_1, \ldots, t_k)$ construct a graph $G_{\mathbf{t}}(D)$ on $k+1$ vertices $0, \ldots, k$, connecting i and j if and only if $\gcd(t_i - t_j, p-1) \geq D$ (where, as before $t_0 = 0$).

Clearly, if $D_{\mathbf{t}} = D$ and $G_{\mathbf{t}}(D) = G$ then $\delta(G) \geq 1$.

Now, for a fixed positive integer $D \leq t < p$ and a graph G with $k+1$ vertices and $\delta(G) \geq 1$, we estimate the number $M_p(D, G, t)$ of vectors $\mathbf{t} = (t_1, \ldots, t_k) \in \mathbb{Z}^k$ with $1 \leq t_1 < \cdots < t_k$ and $t_k = t$ such that $G_{\mathbf{t}}(D) = G$. Summing over all graphs G (since k is fixed there are only finitely many graphs) and admissible values of D, that is, with $t \geq D \gg t^k p^{-(k-1)}$ (see (4)), leads to the desired estimate.

Given a graph G with $k+1$ vertices and $\delta(G) \geq 1$, we now fix a dominating set S in G of cardinality $\#S = \lfloor (k+1)/2 \rfloor$, which exists by Lemma 4

(obviously, we can always add more vertices to S if necessary to guarantee $\#S = \lfloor (k+1)/2 \rfloor$). So for each $j \notin S$ with $j \neq 0, k$, there is $i \in S$ such that $\gcd(t_i - t_j, q-1) \geq D$. So if t_i is fixed, then t_j can take at most

$$\sum_{\substack{d \mid p-1 \\ d \geq D}} \frac{t}{d} \ll \frac{t}{D} \sum_{d \mid p-1} 1 = \frac{t}{D} p^{o(1)} \tag{5}$$

values, where we have used the known bound on the divisor function, (see [5, Theorem 320]). Finally, when $t_k = t$ is fixed, each t_i, $i \in S$, can take at most t values.

Furthermore, if both $0, k \in S$ then there are only

$$\#S - 2 \leq \lfloor (k+1)/2 \rfloor - 2 = \lfloor (k-3)/2 \rfloor$$

elements t_i with $i \in S \setminus \{0, k\}$ to be chosen. After all values of t_i with $i \in S$ are fixed, we see from (5) that the remaining

$$k + 1 - \#S = \lceil (k+1)/2 \rceil$$

elements t_j, $j \notin S$, can be chosen in at most $(tp^{o(1)}/D)^{\lceil (k+1)/2 \rceil}$ ways. So in this case

$$M_p(D, G, t) \leq t^{\lfloor (k-3)/2 \rfloor} (t/D)^{\lceil (k+1)/2 \rceil} p^{o(1)} = t^{k-1} D^{-\lceil (k+1)/2 \rceil} p^{o(1)}. \tag{6}$$

If $0 \in S$ but $k \notin S$, or $0 \notin S$ but $k \in S$, then the same argument implies

$$M_p(D, G, t) \leq t^{\lfloor (k-1)/2 \rfloor} (t/D)^{\lceil (k-1)/2 \rceil} p^{o(1)} = t^{k-1} D^{-\lceil (k-1)/2 \rceil} p^{o(1)}. \tag{7}$$

Finally, if both $0, k \notin S$ then we get

$$M_p(D, G, t) \leq t^{\lfloor (k+1)/2 \rfloor} (t/D)^{\lceil (k-3)/2 \rceil} p^{o(1)} = t^{k-1} D^{-\lceil (k-3)/2 \rceil} p^{o(1)}. \tag{8}$$

Clearly, the bound (8) dominates the bounds (6) and (7). In particular, for $t \geq D \gg t^k p^{-(k-1)}$ we obtain

$$M_p(D, G, t) \leq t^{k-1-k\lceil (k-3)/2 \rceil} p^{(k-1)\lceil (k-3)/2 \rceil + o(1)}.$$

Since, as we have mentioned, there are only finitely many possibilities for the graphs $G_{\mathbf{t}}(D)$, recalling (4) and the bound on the divisor function (see [5, Theorem 320]), we obtain the desired result.

5. Comments. A slight modification of our approach can easily produce a non-trivial bound for $1 \leq k \leq 3$ as well; however, we do not know how to relax the condition (3).

It is certainly an interesting question to show that almost all k-lacunary polynomials of a large degree are irreducible over $\mathbb{F}_p$. In fact, as a first step one can try to get a lower bound on the degree over $\mathbb{F}_p$ of the splitting field of a "random" k-lacunary polynomial.

Acknowledgements. The authors would like to thank the referee for the careful reading of the manuscript and helpful suggestions.

During the preparation of this work the second author was supported in part by the Australian Research Council Grant DP1092835.

References

[1] R. Canetti, J. B. Friedlander, S. V. Konyagin, M. Larsen, D. Lieman and I. E. Shparlinski, *On the statistical properties of Diffie–Hellman distributions*, Israel J. Math. 120 (2000), 23–46.

[2] Q. Cheng, S. Tarasov and M. Vyalyi, *Efficient algorithms for sparse cyclotomic integer zero testing*, Theory Comput. Syst. 46 (2010), 120–142.

[3] W. E. Clark, B. Shekhtman, S. Suen and D. C. Fisher, *Upper bounds for the domination number of a graph*, Congr. Numer. 132 (1998), 99–123.

[4] M. Filaseta, A. Granville and A. Schinzel, *Irreducibility and greatest common divisor algorithms for sparse polynomials*, in: Number Theory and Polynomials, London Math. Soc. Lecture Note Ser. 352, Cambridge Univ. Press, 2008, 155–176.

[5] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford Univ. Press, Oxford, 1979.

[6] T. W. Haynes, S. T. Hedetniemi and P. J. Slater, *Fundamentals of Domination in Graphs*, Dekker, 1998.

[7] H. W. Lenstra, *Finding small degree factors of lacunary polynomials*, in: Number Theory in Progress (Zakopane, 1997), Vol. 1, de Gruyter, Berlin, 1999, 267–276.

[8] —, *On the factorization of lacunary polynomials*, in: Number Theory in Progress (Zakopane, 1997), Vol. 1, de Gruyter, Berlin, 1999, 277–291.

[9] O. Ore, *Theory of Graphs*, Amer. Math. Soc. Colloq. Publ. 38, 1962.

[10] A. Schinzel, *Reducibility of lacunary polynomials, XII*, Acta Arith. 90 (1999), 273–289.

Khodakhast Bibak
Department of Combinatorics and Optimization
University of Waterloo
Waterloo, Ontario, Canada N2L 3G1
E-mail: kbibak@uwaterloo.ca

Igor E. Shparlinski
Department of Computing
Macquarie University
Sydney, NSW 2109, Australia
E-mail: igor@comp.mq.edu.au

Received April 29, 2011;
received in final form November 6, 2011 (7829)