COMPUTATIONAL EXPERIENCES ON THE DISTANCES OF POLYNOMIALS TO IRREDUCIBLE POLYNOMIALS

A. Bérczes and L. Hajdu

Abstract. In this paper we deal with a problem of Turán concerning the 'distance' of polynomials to irreducible polynomials. Using computational methods we prove that for any monic polynomial $P \in \mathbb{Z}[x]$ of degree ≤ 22 there exists a monic polynomial $Q \in \mathbb{Z}[x]$ with $\deg(Q) = \deg(P)$ such that Q is irreducible over $\mathbb{Q}$ and the 'distance' of P and Q is ≤ 4.

1. Introduction

Let $|P|$ denote the length of a polynomial $P \in \mathbb{Z}[x]$, i.e. the sum of the absolute values of the coefficients of P. By the distance of $P, Q \in \mathbb{Z}[x]$ we mean $|P-Q|$. In 1962 P. Turán proposed the following problem (cf. [10]):

Does there exist an absolute constant C_1 such that for every $P(x) \in \mathbb{Z}[x]$ of degree m, there is a polynomial $Q(x) \in \mathbb{Z}[x]$ irreducible over $\mathbb{Q}$, satisfying $\deg(Q) \leq m$ and $|P-Q| \leq C_1$?

This is a very hard problem. It becomes easier if one removes the condition $\deg(Q) \leq m$. A. Schinzel [11] proved that for every $P \in \mathbb{Z}[x]$ of degree m there are infinitely many irreducible $Q \in \mathbb{Z}[x]$ such that

$$|P-Q| \leq \begin{cases} 2 & \text{if } P(0) \neq 0, \\ 3 & \text{otherwise.} \end{cases}$$

Further, one of these irreducible polynomials Q satisfies

$$\deg(Q) \leq e^{(5m+7)(|P|^2+3)}.$$

This deep theorem gives a partial answer to Turán's problem.

A similar problem was proposed in 1984 by M. Szegedy (cf. [4]):

Does there exist a constant C_2 depending only on m such that for any $P \in \mathbb{Z}[x]$ of degree m, $P(x) + b$ is irreducible over $\mathbb{Q}$ for some $b \in \mathbb{Z}$ with $|b| \leq C_2$?

This problem was partially solved by K. Győry [4]. He proved the following: Let $P \in \mathbb{Z}[x]$ be a polynomial of degree m with leading coefficient a_0. There exist an effectively computable constant C_3 depending only on m and $\omega(a_0)$, and $b \in \mathbb{Z}$ with $|b| \leq C_3$ for which $P(x) + b$ is irreducible over $\mathbb{Q}$. (Here $\omega(a_0)$ denotes the number of distinct prime divisors of a_0.)

[0] 1991 *Mathematics Subject Classification.* Primary 11C08, 11R09; Secondary 11T06, 11Y99.

Research of the second author was supported in part by Grants 014245 and T 016 975 from the Hungarian National Foundation for Scientific Research, by the Universitas Foundation of Kereskedelmi Bank RT and by Foundation for Hungarian Higher Education and Research.

Typeset by $\mathcal{AMS}$-TEX

If P is monic, then $\omega(a_0) = 0$. Hence for monic polynomials this theorem gives an affirmative answer to Szegedy's problem.

Results on the distribution of irreducible polynomials (mod p) (see e.g. [1], [2], [3], [5]) can make it easier to determine the Turán constant and Szegedy constant, at least for fixed degree. Using this approach, we give upper bounds for the Turán constant C_1 for monic polynomials P of degree not greater than 22. More precisely, we prove the following.

Theorem. *If $0 \leq n \leq 22$, then for every monic polynomial $P \in \mathbb{Z}[x]$ of degree n there exists an irreducible monic polynomial $Q \in \mathbb{Z}[x]$ of degree n such that*

$$|P - Q| \leq 4.$$

Our computations imply a slightly better result. The details can be found in the tables occurring in Section 3.

The main idea of the proof is as follows. If $Q \in \mathbb{Z}[x]$ is a monic polynomial which is irreducible (mod p) for some prime p, then $Q(x)$ is also irreducible in $\mathbb{Z}[x]$. Hence, given a monic polynomial $P \in \mathbb{Z}[x]$ and a prime p, for every $Q \in \mathbb{Z}[x]$ which is (mod p) irreducible and monic and has the property $\deg(Q) = \deg(P)$, there exists an irreducible monic polynomial $R \in \mathbb{Z}[x]$ with $\deg(R) = \deg(P)$ such that the distance of R and P in $\mathbb{Z}[x]$ is not greater than the distance of Q and P in $\mathbb{Z}[x]$ (mod p). (The precise meaning of the distance of the elements of $\mathbb{Z}[x]$ (mod p) will be given later.) This means that in order to obtain bounds for Turán's constant concerning monic polynomials (of fixed degree) it is sufficent to investigate the elements of $\mathbb{Z}[x]$ (mod p), for some prime p.

The investigation of Szegedy's constants C_2 by computational methods seems to be more difficult.

2. Notation and algorithms

First we introduce our notation and some concepts that we need in the following. For every non–negative integer n let c_n^* (resp. c_n) be the smallest integer such that for every monic polynomial $P \in \mathbb{Z}[x]$ of degree n there exists an irreducible (resp. irreducible monic) polynomial $Q \in \mathbb{Z}[x]$ of degree not greater than n (resp. of degree n), such that $|P - Q| \leq c_n^*$ (resp. $\leq c_n$). For every $n \geq 0$, c_n^* and c_n obviously exist, and we have $c_n^* \leq c_n \leq n + 1$. (The second inequality follows from Eisenstein's theorem. Namely, if $P(x) = x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0$, $P \in \mathbb{Z}[x]$, then there exists a polynomial $Q(x) = x^n + b_{n-1}x^{n-1} + ... + b_1x + b_0$, $Q \in \mathbb{Z}[x]$ such that $\mid b_i - a_i \mid \leq 1$ if $1 \leq i \leq n-1$, $\mid b_0 - a_0 \mid \leq 2$ and b_i is even for $0 \leq i \leq n-1$, but b_0 is not divisible by 4. Then, by Eisenstein's theorem, Q is irreducible, and $|P - Q| \leq n + 1$ clearly holds.)

With this notation, our theorem asserts that

$$c_n \leq 4 \;\text{ if }\; 0 \leq n \leq 22.$$

As is shown e.g. by $P(x) = x^n$ if n is odd, and $P(x) = x^n - x^2 + x$ if n is even, we have $c_n \geq 2$ for $n \geq 3$.

For a prime number p, denote by $\mathbb{Z}_p[x]$ the residue class ring of $\mathbb{Z}[x]$ (mod p). If $T \in \mathbb{Z}[x]$ is a monic polynomial, denote by $T_p(x)$ the coresponding polynomial in

$\mathbb{Z}_p[x]$. Every $P \in \mathbb{Z}_p[x]$ of degree k has a unique representative of the form $\sum\limits_{i=0}^{k} b_i x^i$ with $b_i \in \mathbb{Z}$, $\frac{-p}{2} < b_i \leq \frac{p}{2}, i = 0, ..., k$. For $i = 0, ..., k$ set $c_i = b_i + p$, if $b_i < 0$ and $c_i = b_i$ otherwise. The p-length of $P \in \mathbb{Z}_p[x]$ is defined as $\sum\limits_{i=1}^{k} |b_i|$, and is denoted by $|P|_p$. By the distance of $P, Q \in \mathbb{Z}[x]$ (mod p) we mean $|(P-Q)_p|_p$. It is convenient to code the elements of $\mathbb{Z}_p[x]$. Using the above notation; let us define the function $f_p : \mathbb{Z}_p[x] \longrightarrow \mathbb{N}$ by

$$f_p(P) = \sum_{i=0}^{k} c_i p^i.$$

Obviously f_p is invertible; its inverse will be denoted by f_p^{-1}.

For every $n \geq 0$, denote by $c_n(p)$ (resp. $c_n^*(p)$) the smallest integer such that for each monic $P \in \mathbb{Z}_p[x]$ of degree n there exists an irreducible monic $Q \in \mathbb{Z}_p[x]$ of degree n (resp. of degree not greater than n) with $|P-Q|_p \leq c_n(p)$ (resp. $\leq c_n^*(p)$). It is clear that for every n and p we have $c_n^*(p) \leq c_n(p)$.

Description of the algorithm. To prove our theorem, it is sufficient to investigate the monic polynomials in $\mathbb{Z}[x]$ (mod p), where p is a prime. Let $P \in \mathbb{Z}[x]$ be a monic polynomial of degree n. Then there exists an irreducible monic $Q \in \mathbb{Z}_p[x]$ of degree n such that $|P_p - Q|_p \leq c_n(p)$. Clearly, if $R \in \mathbb{Z}[x]$ is monic, and $R_p(x) = Q(x)$, then R is irreducible. Hence we have $c_n(p) \geq c_n$ for all $n \geq 0$. If the relation $c_n^*(p) \geq c_n^*$ holds, it is not so easy to prove, because for every irreducible monic $Q \in \mathbb{Z}_p[x]$ of degree k ($k < n$) there exist a reducible polynomial $R \in \mathbb{Z}[x]$ of degree n with $R_p(x) = Q(x)$. (For example, if S is monic in $\mathbb{Z}[x]$ with $S_p(x) = Q(x)$, then one can choose $(px^{n-k} + 1)S(x)$ as $R(x)$.) So if we want to obtain a bound for c_n^*, then we must examine $c_n(p)$. In our algorithms we took the primes $p = 2$ and $p = 3$; in these cases (especially when $p = 2$) the computations are relatively simple, and with the help of certain filter conditions they can be made relatively fast.

Consider first the case $p = 2$. From now on by a polynomial we mean an element of $\mathbb{Z}_2[x]$.

It is sufficient to obtain the smallest number k_n, for which for every monic $P \in \mathbb{Z}_2[x]$ of degree n with the property $P(0) \neq 0$ there exist a monic irreducible $Q \in \mathbb{Z}_2[x]$ of degree n, such that $|P - Q|_2 \leq k_n$. Then $c_n(2) = k_n + 1$ holds, provided that $n \geq 2$. (The case $n < 2$ is trivial.)

For small degrees, say for $n \leq 13$, the values $c_n(2)$ can be computed easily, even the 'compare everything with everything else' method is fast enough. (At this stage one can make use of tables containing irreducible polynomials. Such tables can be found e.g. in [6], [7], [9]. The description of a computer program making certain tables of this kind can be found in [8] .)

Suppose now that $14 \leq n \leq 22$. Since in these cases the degree is relatively high, it is worthwile to use a further filter condition.

We shall use the fact that if a polynomial is irreducible then it has an odd number of nonzero coefficients. We shall need some lists in our algorithm. Let T_1 be a list of those 2048 polynomials which have nonzero constant terms and whose degrees are ≤ 11. Those polynomials, whose 2-length is even are (in some order) in the first 1024 place, and the others (in some order) are in the remaining places. Denote by T_2 a list of 2^{n-12} elements, consisting of zeros and ones. If

$k-1=\varepsilon_{n-13}2^{n-13}+...+\varepsilon_1 2+\varepsilon_0$, $\varepsilon_i\in\{0,1\}$, $i=0,...,n-13$ then the kth element of T_2 is 1 if the 2-length of the polynomial $P_k(x)=\varepsilon_{n-13}x^{n-13}+...+\varepsilon_1 x+\varepsilon_0$ is even, and 0 if it is odd. (By the help of the function f_2, these lists can be obtained by using a simple recursion.)

Our algorithm is the following. Consider the polynomials

$$x^n,\ x^n+x^{12},\ x^n+x^{13},\ x^n+x^{13}+x^{12},\ x^n+x^{14},\ \dots,\ x^n+x^{n-1}+\ \dots\ +x^{13}+x^{12}.$$

At the kth step we work with the polynomial $B_k(x)=x^n+x^{12}P_k(x), 1\le k\le 2^{n-12}$. Consider the polynomials $B_k(x)+C(x), C(x)\in T_1$. Using the lists T_1 and T_2 the parity of the 2-length of $B_k(x)+C(x)$ can be determined easily. Hence it is sufficient to change the coefficients of $B_k(x)+C(x)$ either at one or three, or at zero or two places, and determine the irreducibility of these transformed polynomials. (We have tested every occuring polynomial only once; we had a list in which we indicated whether a polynomial was tested yet, and if it was, then it is irreducible or not.) If every polynomial $B_k(x)+C(x)$ can be transformed into an irreducible polynomial, then we have $c_n(2)\le 4$. If for some polynomial $B_k(x)+C(x)$ all the polynomials obtained by a transformation are reducible, then we have $c_n(2)>4$. Our computations proved the first assertion, that is we have $c_n(2)\le 4$, if $14\le n\le 22$. If we change the coefficients of the polynomials at most two places, then we get $c_n(2)>3$, $14\le n\le 22$, and we obtain the extreme polynomials given in our tables. (If n and p are fixed, then by an extreme polynomial we mean a monic $P\in\mathbb{Z}_p[x]$ of degree n for which $|P-Q|_p=c_p(n)$ for some irreducible monic $Q\in\mathbb{Z}_p[x]$ of degree n, and $|P-Q'|_p\ge c_p(n)$ for every irreducible monic $Q'\in\mathbb{Z}_p[x]$ of degree n.)

Consider now the case $p=3$. From now on a polynomial means an element of $\mathbb{Z}_3[x]$.

In this case, if $n\ge 2$, it is sufficient to compute the smallest integer k_n, such that for every monic polynomial P of degree n with the property $P(0)=1$ there exist a monic irreducible polynomial Q for which $|(P-Q)_3|_3\le k_n$ or $|(P+1-Q)_3|_3\le k_n$ holds. Then we have $c_n(3)=k_n+1$, if $2\le n\le 12$. (The case $n<2$ is trivial.) In case $p=3$, the filter condition used in case $p=2$ could not be applied easily, hence our algorithm for $p=3$ was simpler (but less efficient) than for $p=2$. It worked in the same way as in the case of $p=2$ (using similar lists), but of course without the mentioned filter.

We would like to mention that in our programs we have dealt with the codes of the polynomials instead of the polynomials themselves. (The codes were given by the functions f_2 and f_3, respectively.)

The algorithms were written in MAPLE. The computation time for $p=2$ and $n=22$ was about 180 hours on a SUN Sparcstation 10.

We finish this section with a few remarks.

Remark 1. Our experiences suggest (which is not surprising) that the computation time (using these algorithms) is exponential in the degree. That is why we stopped at $n=22$. Using probabilistic algorithms one can hopefully get bounds for Turán's constant for higher degrees as well.

Remark 2. The use of primes greater than 3 would probably give better bounds, but, of course, it would increase the computation time. We have no experience in this direction.

Remark 3. From our computations a similar result follows for polynomials in $\mathbb{Z}[x]$ with leading coefficients divisible neither by 2, nor by 3. Using other primes, more general results could be obtained.

3. Tables

We created some tables by means of the above algorithms.

Description of the tables.

I. We computed the values of $c_n(2)$ for $0 \leq n \leq 22$. In the third column we include polynomials, which show that the corresponding values of $c_n(2)$ are sharp. Except for degrees $0, 1, 4, 6, 7$ and 9 we choose an extreme polynomial $P(x)$ of degree n, $n \leq 22$, for which $P(x) - x^n + 1$ is irreducible. (For the excluded degrees there are no such extreme polynomials.) We *conjecture* that for every $n \geq 10$ there exists an extreme polynomial having this property. For $n \leq 17$ we gave the number of the extreme polynomials as well. In the last column of the table there are polynomials which are irreducible, and whose distance to the extreme polynomial occurring in the preceding column is $c_n(2)$.

II. This table contains all the extreme polynomials of degree $2 \leq n \leq 6$ in case $p = 2$.

III. We computed the values of $c_n(3)$ for $0 \leq n \leq 12$. The extreme polynomials show that the corresponding values of $c_n(3)$ are sharp. The irreducible polynomials in the last column have the property that their distance to the corresponding extreme polynomial is $c_n(3)$.

IV. Using tables I and III we obtained bounds for c_n (and hence for c_n^*) for $0 \leq n \leq 22$.

Table I. $p = 2$

n	$c_n(2)$	*Extreme polynomials (and their number)*		*A nearest irreducible polynomial*
0	0	–	(0)	–
1	0	–	(0)	–
2	2	x^2	(1)	x^2+x+1
3	2	x^3	(1)	x^3+x+1
4	3	x^4+x^2	(1)	x^4+x+1
5	3	x^5+x	(2)	x^5+x^2+1
6	3	x^6+x^2	(7)	x^6+x+1
7	3	x^7+x^2	(17)	x^7+x+1
8	4	x^8	(1)	$x^8+x^4+x^3+x+1$
9	3	x^9+x^2	(72)	x^9+x+1
10	4	$x^{10}+x^8+x^7+x^6+$ $+x^4+x^3+x^2$	(1)	$x^{10}+x^8+x^7+x^6+1$
11	4	$x^{11}+x^9+x^8+x^7+x^5$	(2)	$x^{11}+x^9+x^8+x^7+$ $+x^3+x+1$
12	4	$x^{12}+x^9+x^7+x^2+x$	(4)	$x^{12}+x^7+x^5+x+1$
13	4	x^{13}	(16)	$x^{13}+x^6+x^4+x+1$
14	4	$x^{14}+x^9+x^7+x^6+x^5+x^4+x^2$	(48)	$x^{14}+x^7+x^5+x^4+$ $+x^3+x^2+1$
15	4	$x^{15}+x^7+x^5+x^3+x$	(83)	$x^{15}+x^7+x^4+x+1$
16	4	x^{16}	(168)	$x^{16}+x^6+x^2+x+1$
17	4	$x^{17}+x^8+x^7+x^4+$ $+x^3+x^2+x$	(334)	$x^{17}+x^8+x^3+x+1$
18	4	$x^{18}+x^{10}+x^8+x^3+x$		$x^{18}+x^{10}+x^9+x+1$
19	4	x^{19}		$x^{19}+x^6+x^2+x+1$
20	4	$x^{20}+x^{10}+x^7+x^3+x$		$x^{20}+x^{17}+x^{10}+x+1$
21	4	$x^{21}+x^9+x^8+x^5+x^4$		$x^{21}+x^{10}+x^9+x^4+1$
22	4	$x^{22}+x^{12}+x^9+x^7+x^6+x^3+x$		$x^{22}+x^{15}+x^7+x^6+$ $+x^3+x+1$

Table II. $p = 2$

Degree	*All extreme polynomials*
2	x^2
3	x^3
4	x^4
5	x^5+x x^5+x^4
6	x^6+x^2 $x^6+x^3+x^2+x$ x^6+x^4 $x^6+x^4+x^3+x^2$ $x^6+x^5+x^3+x$ $x^6+x^5+x^4+x^3$ $x^6+x^5+x^5+x^4+x^3+x^2+x$

Table III. $p = 3$

n	$c_n(3)$	*Extreme polynomials*	*A nearest irreducible polynomial*
0	0	–	–
1	0	–	–
2	1	x^2	$x^2 + 1$
3	2	x^3	$x^3 - x^2 + 1$
4	2	$x^4 - x^2 + x$	$x^4 - x^2 - 1$
5	2	x^5	$x^5 - x - 1$
6	2	$x^6 - x^2 + x$	$x^6 + x - 1$
7	3	$x^7 + x^4 + x$	$x^7 + x^5 + x + 1$
8	3	$x^8 - x^7 - x^6 + x^5 + x^3 - x$	$x^8 - x^7 - x^6 + x^5 +$ $+ x^3 - x^2 + x + 1$
9	3	$x^9 - x^5 + x^3 + x$	$x^9 - x^8 - x^7 - x^5 + x^3 + x + 1$
10	3	$x^{10} - x^7 - x^6 + x^5 + x^3 - x$	$x^{10} - x^9 - x^8 - x^7 - x^6 +$ $+ x^5 + x^3 - x + 1$
11	3	$x^{11} + x^5 - x^3 - x$	$x^{11} - x^{10} - x^8 + x^5 - x^3 - x + 1$
12	3	$x^{12} - x^{11} - x^{10} - x^9 - x^8 - x^7 -$ $- x^6 - x^5 - x^4 + x^3 + x^2 + x$	$x^{12} + x^{11} - x^{10} + x^9 - x^8 - x^7 -$ $- x^6 - x^5 - x^4 + x^3 + x^2 + x - 1$

Table IV.

Degree n	*Bound for* c_n
0	0
1	0
2	1
3	2
4	2
5	2
6	2
7	3
8	3
9	3
10	3
11	3
12	3
13	4
14	4
15	4
16	4
17	4
18	4
19	4
20	4
21	4
22	4

Acknowledgements

We would like to thank Professor K. Győry for his generous help, Professor I. Gaál for his valuable remarks and Professor A. Schinzel for encouragement. We are grateful to the referee as well for his useful suggestions.

References

1. S. D. Cohen, *The distribution of polynomials over finite fields*, Acta Arith. **17** (1970), 255–271.
2. S. D. Cohen, *The distribution of polynomials over finite fields, II*, Acta Arith. **20** (1972), 53–62.
3. S. D. Cohen, *Uniform distribution of polynomials over finite fields*, J. London Math. Soc. **6** (1972), 93–102.
4. K. Győry, *On the irreducibility of neighbouring polynomials*, Acta Arith. **67** (1994), 283–294.
5. D. R. Hayes, *The distribution of irreducibles in* GF[q,x], Trans. Amer. Math. Soc. **117** (1965), 101–127.
6. R. Lidl, H. Niederreiter, *Introduction to finite fields and their applications*, Cambridge Univ. Press, 1986.
7. I. H. Morgan, G. L. Mullen, *Primitive normal polynomials over finite fields*, Math. Comp. **63** (1994), 759–765.
8. S. Mossige, *Table of Irreducible Polynomials Over* GF[2] *of Degrees 10 Through 20*, Math. Comp. **26** (1972), 1007–1009.
9. W. W. Peterson, E. J. Weldon, Jr., *Error-Correcting Codes*, THE MIT PRESS, 1961.
10. A. Schinzel, *Reducibility of polynomials and covering systems of congruences*, Acta Arith. **13** (1967), 91–101.
11. A. Schinzel, *Reducibility of lacunary polynomials II*, Acta Arith. **16** (1970), 371–392.

Department of Mathematics and Informatics, Kossuth Lajos University, 4010 Debrecen, Pf. 12, Hungary

E-mail address: berczes@dragon.klte.hu, hajdul@math.klte.hu