ON INTEGER CHEBYSHEV POLYNOMIALS

LAURENT HABSIEGER AND BRUNO SALVY

ABSTRACT. We are concerned with the problem of minimizing the supremum norm on $[0, 1]$ of a nonzero polynomial of degree at most n with integer coefficients. We use the structure of such polynomials to derive an efficient algorithm for computing them. We give a table of these polynomials for degree up to 75 and use a value from this table to answer an open problem due to P. Borwein and T. Erdélyi and improve a lower bound due to Flammang et al.

1. INTRODUCTION

Let d_n denote the lowest common multiple of $1, 2, \dots, n$. The prime number theorem may be stated as

$$\lim_{n \to \infty} \frac{\log(d_n)}{n} = 1.$$

Let $\mathbb{Z}_n[X]$ be the set of polynomials of degree less than or equal to n with integral coefficients, and let I be the function that maps a polynomial $P(X)$ onto $\int_0^1 P(x)\,dx$. It is easy to see that

$$(1) \qquad I(\mathbb{Z}_{n-1}[X]) = \frac{\mathbb{Z}}{d_n}.$$

Nair [Nai82] used this property to show that $d_n \geq 2^n$ for $n \geq 9$, by considering the polynomial $X^n(1 - X)^n$. This method may be refined as follows. Assume that $P(X)$ is a polynomial of degree $k > 0$ with integral coefficients and such that

$$\|P\|_\infty := \max_{t \in [0,1]} |P(t)|$$

is small. Since P is non-zero, we have $I(P^{2n}) > 0$, for any nonnegative integer n. By (1), this implies the inequality $d_{2kn+1} \geq \|P\|_\infty^{-2n}$ from which we deduce

$$\liminf_{n \to \infty} \frac{\log(d_n)}{n} \geq -\frac{\log \|P\|_\infty}{k}.$$

This motivates the study of the polynomials $P_k \in \mathbb{Z}_k[X]$ and the quantities C_k such that

$$(2) \qquad \|P_k\|_\infty = \min_{P \in \mathbb{Z}_k[X] \setminus \{0\}} \|P\|_\infty, \qquad \text{and} \qquad C_k = -\frac{1}{k} \log \|P_k\|_\infty,$$

for positive integers k. According to [BE95], the polynomials P_k are called integer Chebyshev polynomials in the interval $[0, 1]$. In [Ber88] these polynomials are also called polynomials of minimal diophantic deviation from zero.

Much is known about these polynomials and their asymptotic structure. It was proved by Snirelman (see [Ber67]) that the sequence $(C_k)_{k \in \mathbb{N}^*}$ converges to a limit C; Borwein and Erdélyi [BE95] showed that $C \in (0.8586616, 0.8657719)$; and the lower bound was improved by Flammang to 0.8591282 [Fla95, FRS95]. Therefore one cannot prove the prime number theorem in this way. However the problem of finding the integer Chebyshev polynomials in the interval $[0, 1]$ is interesting in itself. (See [BE95, Mon94] and the references therein. In particular, Borwein and Erdélyi state in [BE95] that "Even computing low-degree examples is complicated.")

In this paper, we first prove two lemmas that halve the degree of the polynomials we need to look for. This step enables us to compute polynomials of larger degree but we cannot guarantee to find them all anymore. We then describe several techniques to derive an efficient algorithm for computing these polynomials for moderate degree. We give a table of these polynomials for degree up to 75 and use a value from this table (P_{70}) to answer an open problem from [BE95] and improve the lower bound on C.

2. STRUCTURE OF THE POLYNOMIALS

The set

$$E_k = \{P \in \mathbb{Z}_k[X] \ : \ P(1 - X) = (-1)^k P(X)\}$$

is related to our problem by the following two lemmas.

Lemma 1. *For any nonnegative integer k, we have*

$$E_{2k} = \mathbb{Z}_k[X(1 - X)] \qquad and \qquad E_{2k+1} = (1 - 2X)\mathbb{Z}_k[X(1 - X)].$$

Proof. We first show by induction on k that $E_{2k} = \mathbb{Z}_k[X(1 - X)]$. The case $k = 0$ is trivial: $E_0 = \mathbb{Z} = \mathbb{Z}_0[X(1 - X)]$. Let k be a positive integer and let P be in E_{2k}. The polynomial $P(X) - P(0)$ vanishes when X equals 0, and when X equals 1, by symmetry. Therefore the quotient $Q(X) = \frac{P(X) - P(0)}{X(1 - X)}$ is a polynomial in X of degree at most $2k - 2$. Besides, the polynomial Q belongs to E_{2k-2}. Applying the induction hypothesis to Q then gives the desired result for P.

If P belongs to E_{2k+1}, we have $P(1/2) = -P(1/2) = 0$, which shows that $1 - 2X$ divides $P(X)$. The polynomial $Q(X) = P(X)/(1 - 2X)$ then belongs to E_{2k} and we can use the first part to complete the proof of the lemma.   □

Lemma 2. *For any positive integer k, there exists an element F of degree k in E_k for which*

$$C_k = -\frac{1}{k} \log \|F\|_\infty.$$

Proof. Let k be a positive integer and P a polynomial of degree less than or equal to k, with integral coefficients such that $C_k = -\log \|P\|_\infty / k$. Let us define two polynomials Q_1 and Q_2 with integral coefficients by

$$(3) \qquad Q_1(X) = XP(X) + (-1)^k(1 - X)P(1 - X),$$

$$(4) \qquad Q_2(X) = (1 - X)P(X) + (-1)^k XP(1 - X).$$

By construction, we have $Q_i(X) = (-1)^k Q_i(1 - X)$, for $i = 1, 2$. For any element t in $[0, 1]$, notice that

$$|Q_i(t)| \leq t \|P\|_\infty + (1 - t) \|P\|_\infty = \|P\|_\infty,$$

which implies that $\|Q_i\|_\infty \leq \|P\|_\infty$, for $i = 1, 2$.

At least one of the polynomials Q_i is non-zero, since otherwise $P(X)$ would be solution of a linear system with determinant $(-1)^k(2X - 1) \neq 0$, which would imply $P = 0$. We then take $F = Q_i$ to complete the proof of the lemma.   □

3. Computation of minimal polynomials

We now describe the techniques we use to compute a polynomial P_k of degree k satisfying (2) for k up to 75. The outline of the algorithm is as follows:

1. Find a good upper bound for $\|P_k\|_\infty$;
2. Use this bound to deduce polynomials that are necessarily factors of P_k;
3. Perform an exhaustive search for the missing factors.

We now review these stages in detail.

3.1. First upper bound. A good bound is given by

$$c_k = \min_{0<p<k} \|P_p P_{k-p}\|_\infty.$$

For 56 out of the first 75 polynomials, c_k turns out to be optimal, which means that a minimal polynomial of degree k has been found. However, we do not have this information a priori.

3.2. Bounds and factors. The second stage of the algorithm is iterative. Each step attempts to prove the existence of a factor of P_k starting from c_k and a known factor F of P_k. Initially, $F = 1$ if k is even and $F = 2X - 1$ otherwise. By Lemmas 1 and 2, we concentrate on finding factors of a polynomial $G \in \mathbb{Z}[X]$, such that $P_k(X) = F(X)G(X(1 - X))$. We denote by g the degree of G.

Since $|P_k(x)|$ is bounded by c_k on $[0, 1]$, it follows that for all $x \in [0, 1/4]$,

$$(5) \qquad |G(x)| \cdot |F(u(x))| \leq c_k, \qquad \text{with} \qquad u(x) = \frac{1 - \sqrt{1 - 4x}}{2}.$$

As G has integer coefficients, this inequality can often be used to prove the existence of factors of the form $qX - p$ (p and q integers, $0 \leq p/q \leq 1/4$) when $F(u(p/q)) \neq 0$, for then it is sufficient to check that

$$c_k < \frac{|F(u(p/q))|}{q^g},$$

which implies $q^g|G(p/q)| < 1$. This technique extends to multiple factors via Markov's inequality on the r-th derivative of any polynomial P of degree n with real coefficients:

$$\max_{a \leq x \leq b} |P^{(r)}(x)| \leq \frac{2^r}{(b-a)^r} \frac{n^2(n^2 - 1^2) \cdots (n^2 - (r-1)^2)}{(2r-1)!!} \max_{a \leq x \leq b} |P(x)|,$$

where $(2i + 1)!! = 1 \cdot 3 \cdot 5 \cdots (2i + 1)$.

In practice, we use these bounds with $p/q \in \{1/4, 1/5\}$ to find factors $(4X - 1)^a$, $(5X - 1)^b$ of G, corresponding to factors $(2X - 1)^{2a}$, $(5X^2 - 5X + 1)^b$ of the polynomial P_k. This technique also applies to $p/q = 0$, yielding factors $X^c(1-X)^c$ of P_k, but we rather use another bound derived from [BE95]. If $P_k(X) =$

$X^{k-p}Q(X)$ with $Q(0) \neq 0$, then

$$|Q(0)| \leq \sqrt{2p+1}\binom{k+p+1}{k-p}c_k.$$

This yields factors $X^c(1-X)^c$ by Lemmas 1 and 2.

The advantage of the bounds above is that their computation can be performed rather efficiently. However, they generally fail to yield all the factors of P_k. One reason for this is that they do not really take into account the known factor F, except for its value at $u(p/q)$. To get tighter bounds on the value of G at a given x, we then turn to *Lagrange interpolation*. If $x_0, \ldots, x_g$ are $g+1$ distinct points in $[0, 1/4]$, then

$$G(x) = \sum_{i=0}^{g} G(x_i) \prod_{j \neq i} \frac{x - x_j}{x_i - x_j}.$$

If the points x_j are chosen so that $F(u(x_j)) \neq 0$ for $j = 0, \ldots, g$, it follows that

(6) $$|G(x)| \leq c_k \sum_{i=0}^{g} \frac{1}{|F(u(x_i))|} \prod_{j \neq i} \left| \frac{x - x_j}{x_i - x_j} \right|.$$

This gives a bound on $|G(x)|$ for any $x \in \mathbb{C}$, which can be further improved by finding a set $\{x_0, \ldots, x_g\}$ which minimizes the right-hand side of (6). It turns out that it is not necessary to spend much time finding a global minimum, but that a few iterations of an optimizing scheme produce excellent results.

More generally, bounds on values of the polynomial help find factors of G of any degree. If $A(X) = a_0 X^n + \cdots + a_n$ is an irreducible polynomial with integer coefficients, a necessary and sufficient condition for A to be a factor of G is that the resultant of A and G be zero. Since this resultant is an integer, denoting $\alpha_1, \ldots, \alpha_n$ the roots of A, this condition is equivalent to

(7) $$|a_0|^g |G(\alpha_1)| \cdots |G(\alpha_n)| < 1.$$

Thus for each irreducible polynomial $A(X)$ such that $A(X(1-X))$ occurs as a factor of one of the P_p's, $p < k$, we compute its roots $\alpha_1, \ldots, \alpha_n$ numerically and bound the left-hand side of (7) using Lagrange interpolation as above for each $|G(\alpha_i)|$. In practice, this works well for $A(X) = 29X^2 - 11X + 1$ which occurs frequently.

During this stage of the algorithm, every time a factor is found, F and g are updated, leading to better estimates in the inequalities above, and the whole process is started over again, until no more factors are found.

3.3. **Exhaustive search.** For 25 out of the first 75 polynomials, the quest for factors described above is sufficient to determine all the factors of P_k. In the other cases, we still have to determine a missing factor. By plugging values of x in (5), we get linear inequalities satisfied by the coefficients of the factor G. Sufficiently many of these inequalities define a polyhedron whose interior integer points we have to determine. We have not found any reference to an efficient algorithm for doing so (except [KNA94] in dimension 2).

We solve this problem by using a simplex method to compute bounds on each coordinate. Then if the size of the bounding polyrectangle is not too large, we

check each of its points to see whether it belongs to the polyhedron. For larger polyrectangles, we select the variable with least variation and apply recursively the same technique for each of its possible values. Empirically, it appears that it is better to compute the coefficients of the reciprocal polynomials in the basis 1, $(X-4), (X-4)(X-5), \ldots$ instead of the coefficients of the polynomials themselves.

4. A NEW FACTOR AND ITS CONSEQUENCES

Table 1 shows the first 75 integer Chebyshev polynomials. For each degree we give only one polynomial, even when several exist. The notations are

$$A_1 = X(1 - X), \quad A_2 = 1 - 2X, \quad A_3 = 5X^2 - 5X + 1,$$

$$A_4 = 6X^2 - 6X + 1, \quad A_5 = 29X^4 - 58X^3 + 40X^2 - 11X + 1,$$

$$A_6 = (13X^3 - 20X^2 + 9X - 1)(13X^3 - 19X^2 + 8X - 1),$$

$$A_7 = (31X^4 - 63X^3 + 44X^2 - 12X + 1)(31X^4 - 61X^3 + 41X^2 - 11X + 1),$$

$$A_8 = 4921X^{10} - 24605X^9 + 53804X^8 - 67586X^7 + 53866X^6$$
$$-28388X^5 + 9995X^4 - 2317X^3 + 338X^2 - 28X + 1.$$

When expressed in the variable $u = X(1 - X)$, these polynomials become

$$A_1 = u, \quad A_2^2 = 4u - 1, \quad A_3 = 5u - 1, \quad A_4 = 6u - 1, \quad A_5 = 29u^2 - 11u + 1,$$

$$A_6 = 169u^3 - 94u^2 + 17u - 1, \quad A_7 = 961u^4 - 712u^3 + 194u^2 - 23u + 1,$$

$$A_8 = 4921u^5 - 4594u^4 + 1697u^3 - 310u^2 + 28u - 1.$$

Almost all these factors were already known to occur in integer Chebyshev polynomials. The most surprising result is the factor A_8 which divides P_{70}. This factor gives a negative answer to the following open problem from [BE95]:

> Do the integer Chebyshev polynomials on $[0, 1]$ have all their zeros in $[0, 1]$?

The polynomial P_{70} has four non-real zeros. The derivative of A_8 however has all its zeros in $[0, 1]$.

The factor A_8 can also be used to improve the bound on C. Following the lines of [BE95], we use a simplex method to compute $\alpha_1, \ldots, \alpha_{10}$ and c such that: the system

$$\sum_{i=1}^{10} \alpha_i \log |A_i(x_j)| \le c, \qquad j = 1, \ldots, n,$$

is satisfied; c is minimal; the α_i's are nonnegative and constrained by

$$\sum_{i=1}^{10} \alpha_i \deg(A_i) = 1;$$

the polynomial A_9 is taken from [BE95]:

$$941[X(1 - X)]^4 - 703[X(1 - X)]^3 + 193[X(1 - X)]^2 - 23X(1 - X) + 1;$$

TABLE 1. Integer Chebyshev polynomials of degree up to 75

k	C_k	Polynomial	k	C_k	Polynomial
0	$-\infty$	1	38	.8400137109	$A_1^{14}A_2^6A_3^2$
1	0	A_2	39	.8488877225	$A_1^{13}A_2^5A_3^2A_5$
2	.6931471805	A_1	40	.8404640658	$A_1^{13}A_2^6A_3^2A_5$
3	.7803552046	A_1A_2	41	.8465081502	$A_1^{14}A_2^5A_3^2A_5$
4	.6931471805	A_1^2	42	.8440344532	$A_1^{14}A_2^6A_3^2A_5$
5	.8047189562	$A_1^2A_2$	43	.8449879864	$A_1^{14}A_2^5A_3^3A_5$
6	.7803552047	$A_1^2A_2^2$	44	.8455791880	$A_1^{15}A_2^6A_3^2A_5$
7	.7991843140	$A_1^3A_2$	45	.8398268629	$A_1^{15}A_2^7A_3^2A_5$
8	.8010279578	$A_1^3A_2^2$	46	.8468722310	$A_1^{16}A_2^6A_3^2A_5$
9	.8316158874	$A_1^3A_2A_3$	47	.8430715282	$A_1^{15}A_2^5A_3^2A_5^2$
10	.8047189567	$A_1^4A_2^2$	48	.8491690644	$A_1^{16}A_2^6A_3^3A_5$
11	.8109727374	$A_1^4A_2A_3$	49	.8457300825	$A_1^{16}A_2^7A_3^2A_4A_5$
12	.8235466006	$A_1^4A_2^2A_3$	50	.8448129844	$A_1^{16}A_2^6A_3^2A_5^2$
13	.8090328223	$A_1^4A_2A_3^2$	51	.8473273518	$A_1^{17}A_2^7A_3^3A_5$
14	.8405593722	$A_1^5A_2^2A_3$	52	.8464778545	$A_1^{17}A_2^8A_3^2A_4A_5$
15	.8163003367	$A_1^5A_2^3A_3$	53	.8494236563	$A_1^{18}A_2^7A_3^3A_5$
16	.8268434981	$A_1^6A_2^2A_3$	54	.8441650118	$A_1^{18}A_2^8A_3^3A_5$
17	.8311026953	$A_1^6A_2^3A_3$	55	.8469319238	$A_1^{19}A_2^7A_3^3A_5$
18	.8316158595	$A_1^6A_2^2A_3^2$	56	.8457325337	$A_1^{19}A_2^8A_3^3A_5$
19	.8400137111	$A_1^7A_2^3A_3$	57	.8464270507	$A_1^{19}A_2^7A_3^3A_4^4A_5$
20	.8288579250	$A_1^6A_2^2A_3A_5$	58	.8471145416	$A_1^{20}A_2^8A_3^3A_5$
21	.8303936176	$A_1^8A_2^3A_3$	59	.8468162432	$A_1^{19}A_2^7A_3^3A_5^2$
22	.8322820522	$A_1^8A_2^4A_3$	60	.8483301990	$A_1^{21}A_2^8A_3^3A_5$
23	.8385504326	$A_1^8A_2^3A_3^2$	61	.8462840938	$A_1^{20}A_2^7A_3^3A_5^2$
24	.8378960676	$A_1^9A_2^4A_3$	62	.8488367522	$A_1^{21}A_2^8A_3^4A_5$
25	.8448129844	$A_1^8A_2^3A_3A_5$	63	.8463191193	$A_1^{20}A_2^7A_3^3A_5A_6$
26	.8338173096	$A_1^9A_2^4A_3^2$	64	.8477264811	$A_1^{21}A_2^8A_3^3A_5^2$
27	.8434645771	$A_1^9A_2^3A_3A_5$	65	.8478630743	$A_1^{22}A_2^9A_3^4A_5$
28	.8405595853	$A_1^{10}A_2^4A_3^2$	66	.8489400289	$A_1^{22}A_2^{10}A_3^3A_4A_5$
29	.8356309576	$A_1^{11}A_2^5A_3$	67	.8492102067	$A_1^{23}A_2^9A_3^4A_5$
30	.8398858116	$A_1^{10}A_2^4A_3A_5$	68	.8468222183	$A_1^{23}A_2^{10}A_3^3A_4A_5$
31	.8358028746	$A_1^{11}A_2^5A_3^2$	69	.8471956204	$A_1^{22}A_2^9A_3^3A_5A_6$
32	.8412151163	$A_1^{11}A_2^4A_3A_5$	70	.8467991413	$A_1^{22}A_2^8A_3^2A_5A_8$
33	.8406807538	$A_1^{12}A_2^5A_3^2$	71	.8472585205	$A_1^{24}A_2^{11}A_3^3A_4A_5$
34	.8461748302	$A_1^{11}A_2^4A_3^2A_5$	72	.8499040059	$A_1^{23}A_2^8A_3^4A_5A_6$
35	.8388555719	$A_1^{11}A_2^5A_3A_4A_5$	73	.8499191960	$A_1^{24}A_2^9A_3^4A_5^2$
36	.8409740145	$A_1^{12}A_2^4A_3^2A_5$	74	.8486911214	$A_1^{23}A_2^8A_3^4A_5A_7$
37	.8431610719	$A_1^{12}A_2^5A_3^2A_5$	75	.8487246297	$A_1^{24}A_2^9A_3^4A_5A_6$

the polynomial A_{10} is

$$34X^4 - 68X^3 + 46X^2 - 12X + 1,$$

which was found by considering polynomials with small coefficients in the basis $1, (X - 4), (X - 4)(X - 5), \ldots$; and the x_j's are (numerous) points in $[0, 1/2]$. After further optimization starting from the result of the simplex method, we obtain

$(\alpha_1, \ldots, \alpha_{10})$
$$= (.3185482277, .1173845553, .0387135327, .0015952503, .0151308163,$$
$$.0056051138, .0023845110, .0004709314, .0057932925, .0001539332).$$

From this computation we deduce a polynomial

$$Q = A_1^{3185482277} \cdot A_2^{1173845553} \cdot A_3^{387135327} \cdot A_4^{15952503}$$
$$\cdot A_5^{151308163} \cdot A_6^{56051138} \cdot A_7^{23845110} \cdot A_8^{4709314} \cdot A_9^{57932925} \cdot A_{10}^{1539332}$$

of degree $d = 10^{10} - 5$ such that

$$-\frac{1}{d} \log \|Q\|_\infty \approx 0.8592502805249817173754836.$$

Then since $\|P_{nd}\|_\infty \leq \|Q^n\|_\infty$, we get the following improvement on the known lower bound 0.8591282.

Theorem 1. *The constant C satisfies*

$$C > 0.85925028.$$

5. CONCLUSION

All the computations have been performed using the computer algebra system Maple. By implementing the same techniques in C, one would probably find at most ten more polynomials, at the expense of a much longer programming time. However, it is clearly much more effective to look for better algorithms.

Currently, the bottleneck of the computation is the last part, which is hopeless if the degree of the missing factor is too high (our limit is 24, corresponding to thirteen undeterminate coefficients in $X(1 - X)$). Sophisticated techniques from integer linear programming might help.

Also, it is crucial to find as many factors as possible before this stage. In practice, we almost always know what the best polynomial is, the problem lies in proving it. In particular, in almost all cases, the use of bounds as described in this paper is not sufficient to determine the maximal exponent of the factor $X(1 - X)$. Further work on this part should help.

REFERENCES

[BE95]   Peter Borwein and Tamás Erdélyi, *The integer Chebyshev problem*, Mathematics of Computation **65** (1996), 661–681. MR **96g**:11077

[Ber67] Emiliano Aparicio Bernardo, *Sobre la aproximación de las funciones mediante polinomios de coeficientes enteros*, Actas de la Octava Reunión Anual de Matemáticos Españoles (Madrid), 1967, pp. 21–33. MR **41**:4066

[Ber88] Emiliano Aparicio Bernardo, *On the asymptotic structure of the polynomials of minimal diophantic deviation from zero*, Journal of Approximation Theory **55** (1988), 270–278. MR **90b**:41010

[Fla95] Valérie Flammang, *Sur le diamètre transfini entier d'un intervalle à extrémités rationnelles*, Annales de l'Institut Fourier **45** (1995), no. 3, 779–793. MR **96i**:11083

[FRS95] V. Flammang, G. Rhin, and C. J. Smyth, *The integer transfinite diameter of intervals and totally real algebraic integers*, Tech. Report MS-95-033, Department of Mathematics and Statistics, University of Edinburgh, 1995.

[KNA94] Naoyoshi Kanamaru, Takao Nishizeki, and Tetsuo Asano, *Efficient enumeration of grid points in a convex polygon and its application to integer programming*, International Journal of Computational Geometry & Applications **4** (1994), no. 1, 69–85. MR **95b**:90060

[Mon94] Hugh L. Montgomery, *Ten lectures on the interface between analytic number theory and harmonic analysis*, CBMS Regional Conference Series in Mathematics, vol. 84, AMS, October 1994. MR **96i**:11002

[Nai82] M. Nair, *On Chebyshev-type inequalities for primes*, American Mathematical Monthly **89** (1982), no. 2, 126–129. MR **83f**:10043

LABORATOIRE D'ALGORITHMIQUE ARITHMÉTIQUE, CNRS UMR 9936, UNIVERSITÉ BORDEAUX 1, 351 COURS DE LA LIBÉRATION, F-33405 TALENCE CEDEX, FRANCE
    E-mail address: `habsiege@math.u-bordeaux.fr`

INRIA ROCQUENCOURT, DOMAINE DE VOLUCEAU, B.P. 105, F-78153 LE CHESNAY CEDEX, FRANCE
    E-mail address: `Bruno.Salvy@inria.fr`