On integer Chebyshev Polynomials

Bruno Salvy
INRIA Rocquencourt

January 29, 1996

[summary by Xavier Gourdon]

Abstract

We deal with the problem of minimizing the supremum norm on $[0,1]$ of non zero polynomials of degree at most n with integer coefficients.

1. Introduction

We consider the supremum norm on polynomials $\|P\|_\infty = \max_{[0,1]} |P(t)|$. We denote by $\mathbb{Z}_k[x]$ the set of polynomials with integer coefficients of degree $\le k$. We consider the polynomials P_k in $\mathbb{Z}_k[x]$ and the quantities C_k such that

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

According to [1], the polynomials P_k are called integer Chebyshev polynomials in $[0,1]$. These polynomials appeared in the literature because as we discuss below, it was thought that they could be used to obtain an elementary proof of prime number theorem. Aparicio showed that in fact, one cannot prove the prime number theorem in this way. However, the problem of finding the polynomials P_k is interesting in itself. According to Borwein and Erdélyi, "Even computing low-degree examples is difficult".

2. The prime number theorem

Let d_n denote the lowest common multiple of $1, 2, \ldots, n$. Proving the prime number theorem can be elementary reduced to proving the inequality

$$\liminf_{n \to \infty} \frac{\log d_n}{n} \ge 1.$$

An idea to obtain this result is to use the fact that $P \in \mathbb{Z}_m[x]$ implies $\int_0^1 P(x)\,dx \in \mathbb{Z}/d_{m+1}$. Applying this to the polynomial P_k^{2n} leads to

$$\|P_k\|_\infty^{2n} \ge \int_0^1 P_k^{2n}(x)\,dx \ge \frac{1}{d_{2kn+1}}, \qquad \text{thus} \qquad \liminf_{n \to \infty} \frac{\log d_n}{n} \ge -\frac{\log \|P_k\|_\infty}{k} = C_k .$$

Therefore, if we had $\limsup_{k \to \infty} C_k = 1$, one could prove the prime number theorem in this way. Indeed, it appears that this is not the case. The sequence (C_k) converges to a limit C, and Borwein and Erdélyi [1] showed that $C \in (0.8586616, 0.8657719)$. Thanks to our new results, we improve the lower bound on C.

3. Related problems

3.1. Integer transfinite diameter. Our problem can be stated in terms of *integer transfinite diameter*. The transfinite diameter of a set S of complex numbers is defined by

$$t(S) := \lim_{n\to\infty} \sup_{z_1,\ldots,z_n\in S} \prod_{i<j} |z_i - z_j|^{1/\binom{n}{2}}.$$

A theorem of Fekete states that

$$t(S) = \inf_{P\in\mathbb{C}[x], P \text{ monic}} \max_{x\in S} |P(x)|^{1/\deg(P)}.$$

The *integer transfinite diameter* of a subset S of $\mathbb{R}$ is defined by

$$t_{\mathbb{Z}}(S) = \inf_{P\in\mathbb{Z}[x], \deg(P)>0} \max_{x\in S} |P(x)|^{1/\deg(P)}.$$

Thus, our problem can be rephrased as: finding the integer transfinite diameter of the interval $[0,1]$. If I is the interval $[a,b]$ with $a<b$, it is known that $t(I) = |I|/4$, with $|I| = b-a$. If $|I|\geq 4$, we have the equality $t_{\mathbb{Z}}(I) = t(I)$. For $|I|<4$, the best known result is due to Fekete and states that $t(S) \leq t_{\mathbb{Z}}(S) \leq \sqrt{t(S)}$.

3.2. Trace of totally positive algebraic integers. Let α_1 be an algebraic integer of d, $\alpha_2,\ldots,\alpha_d$ its conjugates. We say that α_1 is *totally positive* if all the α_i are real and positive. Siegel has proved in 1945 that except for finitely many exceptions, we have the following lower bound on totally positive algebraic integers

$$\frac{\alpha_1+\cdots+\alpha_d}{d} \geq 1.733.$$

A general result states that this problem is related to the integer transfinite diameter:

THEOREM 1 (BORWEIN, ERDÉLYI). *Let m be a positive integer.*

$$\text{If} \quad t_{\mathbb{Z}}\left(\left[0,\frac{1}{m}\right]\right) < \frac{1}{m+\delta} \quad \text{then} \quad \frac{\alpha_1+\cdots+\alpha_d}{d} \geq \delta$$

for totally positive algebraic integers, with finitely many exceptions.

4. 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 lemma [2].

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

$$E_{2k} = \mathbb{Z}_k[x(1-x)] \quad \text{and} \quad E_{2k+1} = (1-2x)\mathbb{Z}_k[x(1-x)],$$

and there exists an element F of degree k in E_k for which

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

5. Computation of minimal polynomials

The previously known integer Chebyshev polynomials had small degrees. We now briefly describe the techniques used to compute a polynomial P_k of degree k satisfying (1) for k up to 75. The outline of the algorithm goes as follows:

(1) Find a good upper bound for $\|P_k\|_\infty$;
(2) Repeat
  – use this bound to determine factors of P_k,
  – use these factors to improve the bound,
  until no more factors are found;
(3) Perform an exhaustive search for the missing factors.

5.1. First upper bound. A good bound is given by $c_k = \min_{0<\ell<k} \|P_\ell P_{k-\ell}\|_\infty$.

5.2. Bounds and factors. We use the following facts to find factors of $G \in \mathbb{Z}_g[x]$.

– If $q^g|G(p/q)| < 1$ then $(qx - p)$ is a factor of G.
– This technique extends to multiple factors via Markov's inequality:

$$\max_{a\le x\le b} |G^{(r)}(x)| \le \frac{2^r}{(b-a)^r} \frac{n^2(n^2-1^2)\cdots(n^2-(r-1)^2)}{1\cdot 3\cdots(2r-1)} \max_{a\le x\le b} |G(x)|.$$

– At $x = 0$, we have a better bound due to Borwein and Erdélyi:

$$G(x) = x^{g-p}Q(x) \qquad \Longrightarrow \qquad |Q(0)| \le \sqrt{2p+1}\binom{g+p+1}{g-p}\|G\|_\infty.$$

– More generally, we can find higher degree factors. Let $F = a_0x^n + \cdots + a_n \in \mathbb{Z}[x]$ be irreducible, $\alpha_1, \ldots, \alpha_n$ its roots. The expression $R = a_0^g G(\alpha_1)\cdots G(\alpha_n)$ is an integer (it is a resultant). If $|R| < 1$, then F is a factor of G.

Once factors have been obtained in this way, we have $P_k(x) = F(x)G(x(1-x))$, where F is known and G unknown. Bounds on $G(x)$ at a given x can be obtained using the fact that $|F(u(x))G(x)| \le \|P_k\|_\infty \le c_k$ with $u(x) = \frac{1}{2}(1-\sqrt{1-4x})$. This enables to find other factors. This technique provides all the integer Chebyshev polynomials of degree ≤ 12.

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

$$G(x) = \sum_{i=0}^{g} G(x_i)\prod_{j\ne i}\frac{x-x_j}{x_i-x_j} \quad \text{thus} \quad |G(x)| \le c_k \sum_{i=0}^{g}\frac{1}{|F(u(x_i))|}\prod_{j\ne i}\left|\frac{x-x_j}{x_i-x_j}\right|.$$

This gives a bound on $|G(x)|$, which can be further improved by finding a set $\{x_0, \ldots, x_g\}$ which minimizes the right-hand side of the inequality. By this technique, all Chebyshev of degree ≤ 30 are found.

5.3. Exhaustive search. By plugging values of x in the inequality $|F(u(x))| \cdot |G(x)| \le c_k$, we get linear inequalities satisfied by the coefficients of the factor G. These inequalities define a polyhedron whose interior integer points we have to determine. 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. In this way, we test a finite set of polynomials. This technique is reasonable for $n \le 13$ (i.e., degree 24).

5.4. A detailed example: P_{37}. We show how to find P_{37} using our algorithm.
A first upper bound is obtained from the previous polynomials

$$\|P_{37}\|_\infty \le c_{37} = \min_\ell \|P_\ell P_{37-\ell}\|_\infty = 0.283\,10^{-13}.$$

We then look for factors of P_{37}. At each stage, we have $P_{37}(x) = F(x)G(x(1-x))$ with F known and G unknown, $g = \deg(G)$.

- Since 37 is odd, a factor is $F = 1 - 2x$ by lemma 1 ($g = 18$).
- We have $5^{18}c_{37} < |F(u(1/5))|$ thus $5^{18}|G(1/5)| < 1$, and a factor is $F := F \cdot (5x^2 - 5x + 1)$ ($g = 17$).
- Using the Borwein-Erdélyi bound, we find the factor $F := F \cdot x^9(1-x)^9$ ($g = 8$).
- Using Lagrange interpolation, we find $|G(0)| < 1$, thus a factor is $F := F \cdot x(1-x)$ ($g = 7$).
- The same technique applied with the new factor F gives $|G(0)| < 1$, thus a factor is $F := F \cdot x(1-x)$ ($g = 6$).
- The same technique gives $4^6|G(1/4)| < 1$, thus $F := F \cdot (4x^2 - 4x + 1)$ ($g = 5$).
- The same technique gives
$$29^5 \left| G\left(\frac{11+\sqrt{5}}{58}\right) G\left(\frac{11-\sqrt{5}}{58}\right) \right| < 1$$
thus $F := F \cdot (29x^4 - 58x^3 + 40x^2 - 11x + 1)$ ($g = 3$).
- The same technique gives $|G(0)| < 1$ thus $F = F \cdot x(1-x)$ ($g = 2$).
- The same technique gives $4^2|G(1/4)| < 1$, thus $F := F \cdot (4x^2 - 4x + 1)$ ($g = 1$).

The step of exhaustive search finally yields 6 solutions, and only one has the right $\|\cdot\|_\infty$. Eventually, we find

$$P_{37}(x) = x^{12}(1-x)^{12}(1-2x)^5(5x^2-5x+1)^2(29x^4-58x^3+40x^2-11x+1).$$

6. A new factor

The only factors of all the 75 first polynomials are the following, expressed in the variable $u = x(1-x)$,

$$A_1 = u, \quad A_2 = 4u - 1, \quad A_3 = 5u - 1, \quad A_4 = 6u - 1, \quad A_5 = 29u^2 - 11u + 1,$$
$$A_6 = 169u^3 - 94u^2 + 17u - 1, \quad A_7 = 961u^4 - 712u^3 + 194u^2 - 23u + 1,$$
$$A_8 = 4921u^5 - 4594u^4 + 1697u^3 - 310u^2 + 28u - 1.$$

The factor A_8 is a new one, and it has four non real root, which gives a negative answer to an open problem from [1]: Do all the integer Chebyshev polynomials on $[0,1]$ have all their zeros in $[0,1]$?

Thanks to this new factor we can improve the bound on C. Following the lines of [1], we use a simplex method to compute a polynomial $Q = A_1^{\beta_1}A_2^{\beta_2}\cdots$ of degree $d = 10^{10} - 9$ such that $-\frac{1}{d}\log\|Q\|_\infty = 0.8591978$, thus $C > 0.8591978$.

Bibliography

[1] Borwein (Peter) and Erdélyi (Tamás). – The integer Chebyshev problem. *Mathematics of Computation*, 1995. – To appear.

[2] Habsieger (Laurent) and Salvy (Bruno). – On integer Chebyshev polynomials. *Mathematics of Computation*, 1996. – To appear.