Three Highly Computational Problems somewhere between Diophantine Number Theory and Combinatorics

Peter Borwein

-

http://www.cecm.sfu.ca/~pborwein.

MAY 2003

Abstract: A number of classical and not so classical problems in number theory concern finding polynomials with integer coefficients that are of small norm. These include old chestnuts like the Merit Factor problem, Lehmer's Conjecture and Littlewood's (other) Conjecture.

Let

$$\mathcal{Z}_n := \left\{ \sum_{i=0}^{n} a_i z^i : a_i \in \mathbb{Z} \right\}$$

denote the set of algebraic polynomials of degree at most n with integer coefficients and let $\mathcal{Z}$ denote the union.

Let

$$\mathcal{L}_n := \left\{ \sum_{i=0}^{n} a_i z^i : a_i \in \{-1, 1\} \right\}$$

denote the set of polynomials of degree at most n with coefficients from $\{-1, 1\}$. Call such polynomials **Littlewood polynomials**.

The **supremum norm** of a polynomial p on a set A is defined as

$$\|p\|_A := \sup_{z \in A} |p(z)|.$$

For positive α, the L_α norm on the boundary of the unit disk is defined by

$$\|p\|_\alpha := \left(\frac{1}{2\pi} \int_0^{2\pi} \left| p\left(e^{i\theta}\right) \right|^\alpha d\theta \right)^{1/\alpha}.$$

For

$$p(z) := a_n z^n + \cdots + a_1 z + a_0$$

the L_2 norm on D is also given by

$$\|p\|_2 = \sqrt{|a_n|^2 + \cdots + |a_1|^2 + |a_0|^2}.$$

The two interesting limiting cases give

$$\lim_{\alpha \to \infty} \|p\|_\alpha = \|p\|_D =: \|p\|_\infty$$

and

$$\lim_{\alpha \to 0} \|p\|_\alpha = \exp\left(\frac{1}{2\pi}\int_0^{2\pi} \log\left|p\left(e^{i\theta}\right)\right| \, d\theta\right).$$

The latter is the **Mahler measure** denoted by $M(p)$. Jensen's theorem for

$$p_n(z) := a(z-\alpha_1)(z-\alpha_2)\cdots(z-\alpha_n)$$

gives

$$M(p_n) = |a| \prod_{|\alpha_i| \geq 1} |\alpha_i|.$$

Mahler's measure is multiplicative:

$$M(p\,q) = M(p)M(q)$$

Problem 1. Littlewood's Problem in L_∞ (1950?). *Find the polynomial in $\mathcal{L}_n$ that has smallest possible supremum norm on the unit disk.*

Show that there exist positive constants c_1 and c_2 so that for any n is it is possible to find $p_n \in \mathcal{L}_n$ with

$$c_1\sqrt{n} \le |p_n(z)| \le c_2\sqrt{n}$$

for all complex z with $|z| = 1$.

Littlewood, in part, based his conjecture on computations of all such polynomials up to degree twenty.

Odlyzko has now done 200 MIPS years of computing on this problem

A Related Erdős's Problem in L_∞. *Show that there exists a positive constant c_3 so that for all n and all $p_n \in \mathcal{L}_n$ we have $\|p_n\|_D \geq (1 + c_3)\sqrt{n}$.*

Merit Factor Problems (1950?). The L_4 norm computes algebraically. If

$$p(z) := \sum_{k=0}^{n} a_k z^k$$

has real coefficients then

$$p(z)p(1/z) = \sum_{k=-n}^{n} c_k z^k$$

where the **acyclic autocorrelation coefficients**

$$c_k = \sum_{j=0}^{n-k} a_j a_{j+k} \quad \text{and} \quad c_{-k} = c_k$$

and

$$\|p(z)\|_4^4 = \|p(z)p(1/z)\|_2^2 = \sum_{k=-n}^{n} c_k^2.$$

The **merit factor** is defined by

$$MF(p) = \frac{\|p\|_2^4}{\|p|_4^4 - \|p\|_2^4}$$

or equivalently

$$MF(p) = \frac{n+1}{2\sum_{k>0} c_k^2}.$$

The merit factor is a useful normalization. It tends to give interesting sequences integer limits and makes the expected merit factor of a polynomial with ± 1 coefficients 1.

The Rudin-Shapiro polynomials have merit factors that tend to 3.

Problem 2. Merit Factor Problem.

Find the polynomial in $\mathcal{L}_n$ that has smallest possible L_4 norm on the unit disk.

Show that there exists a positive constant c_4 so that for all n and all $p_n \in \mathcal{L}_n$ we have

$$L_4(p_n) \geq (1 + c_4)\sqrt{n}.$$

Equivalently show that the Merit Factor is bounded above.

The Related Barker Polynomial Problem. *For* $n > 12$ *and* $p_n \in \mathcal{L}_n$ *show that*

$$L_4(p_n) > ((n+1)^2 + 2n)^{1/4}.$$

Equivalently show that at least one non trivial autocorrelation coefficient is strictly greater than 1 in modulus.

This is much weaker than the Merit Factor Problem.

• Find sequences that have analysable Merit Factors

Theorem . *For q an odd prime, the Turyn type polynomials*

$$R_q(z) := \sum_{k=0}^{q-1} \left(\frac{k + [q/4]}{q} \right) z^k$$

where $[\cdot]$ denotes the nearest integer, satisfy

$$\|R_q\|_4^4 = \frac{7q^2}{6} - q - \frac{1}{6} - \gamma_q$$

and

$$\gamma_q := \begin{cases} h(-q)\big(h(-q) - 4\big) & \text{if } q \equiv 1, 5 \pmod 8, \\ 12\big(h(-q)\big)^2 & \text{if } q \equiv 3 \pmod 8, \\ 0 & \text{if } q \equiv 7 \pmod 8. \end{cases}$$

Thus these polynomials have merit factors asymptotic to 6.

Golay, Høholdt and Jensen, and Turyn (and others) show that the merit factors of cyclically permuted character polynomials associated with non-principal real characters (the Legendre symbol) vary asymptotically between 3/2 and 6.

Several authors have conjectured this is best possible. For example in 1983 Golay wrote:

> "[Six] is the highest merit factor obtained so far for systematically synthesized binary sequences, and the eventuality must be considered that no systematic synthesis will ever be found which will yield higher merit factors."

And in 1988 Høholdt and Jensen wrote:

> "We therefore make a new conjecture concerning the merit factor problem, namely, that asymptotically the maximum value of the merit factor is 6 and hence that offset Legendre sequences are optimal."

A really interesting observation made by Tony Kirilusha and Ganesh Narayanaswamy as summer students at the University of Richmond of Jim Davis suggested that one should try building on Turyn's construction by appending the initial part of Turyn's sequence to the end.

Their suggestion was wrong but the intuition was good. To see what is happening one needs to look at sequences of length 100,000 or greater.

We conjecture there exist sequences of Turyn type polynomials (with modification) that have merit factors growing like 6.3. (Joint work with Choi and Jedwab).

Basically one rotates the Fekete polynomials by 22 percent and adds 5.7 percent of the initial terms to the end.

The numbers are compelling!!

Merit Factor Problem Restated.

For a sequence of length n+1

$$\{a_0, a_1, a_2, \dots, a_n\} \quad a_k = \pm 1$$

the **acyclic autocorrelation coefficients**

$$c_k := \sum_{j=0}^{n-k} a_j a_{j+k} \quad \text{and} \quad c_{-k} = c_k$$

and the **Merit factor**

$$MF := \frac{n+1}{2\sum_{k>0} c_k^2}.$$

For any (all) n, **maximize this!**

- This has been called the "hardest combinatorial optimization problem known."

• Best merit factors have been computed up to length 59. This is by variations on branch and bound algorithms (with huge effort).

• The “landscape” for best merit factors is very irregular. We suspect that most hueristics are wrong.

• All Golay pairs are known up to length 100.

• Barker polynomials (all autocorrelations of size at most 1) are known not to exist up to 10^{20} – far past computational rangs.

- One ambition is to map out the best merit factor space probabilistically up to degree 100 or so.

- This is done with a mix of hill climbing and simulated annealing. (And a lot of cluster computing.)

- It works surprisingly well. (Joint with Ferguson and Knauer).

Problem 3. Lehmer's Problem (1933). *Show that a (non-cyclotomic) polynomial p with integer coefficients has Mahler measure at least* 1.1762.... *(This latter constant is the Mahler measure of* $1 + z - z^3 - z^4 - z^5 - z^6 - z^7 + z^9 + z^{10}$*.)*

A conjecture of similar flavour (implied by the above) is

Conjecture of Schinzel and Zassenhaus (1965). *There is a constant c so that any non-cyclotomic polynomial p_n of degree n with integer coefficients has at least one root of modulus at least c/n.*

The best partials are due to Smyth.

If p is a non-reciprocal polynomial of degree n then at least one root ρ satisfies

$$\rho \geq 1 + \frac{\log \phi}{n}$$

where $\phi = 1.3247\ldots$ is the smallest Pisot number, namely the real root of $z^3 - z - 1$.

The number ϕ is also the smallest measure of a non-reciprocal polynomial.

Theorem 1 (Hare, Mossinghoff and PB) *Suppose* f *is a monic, nonreciprocal polynomial with integer coefficients satisfying* $f \equiv \pm f^*$ *mod* m *for some integer* $m \geq 2$. *Then*

$$M(f) \geq \frac{m + \sqrt{m^2 + 16}}{4}, \tag{1}$$

and this bound is sharp when m *is even.*

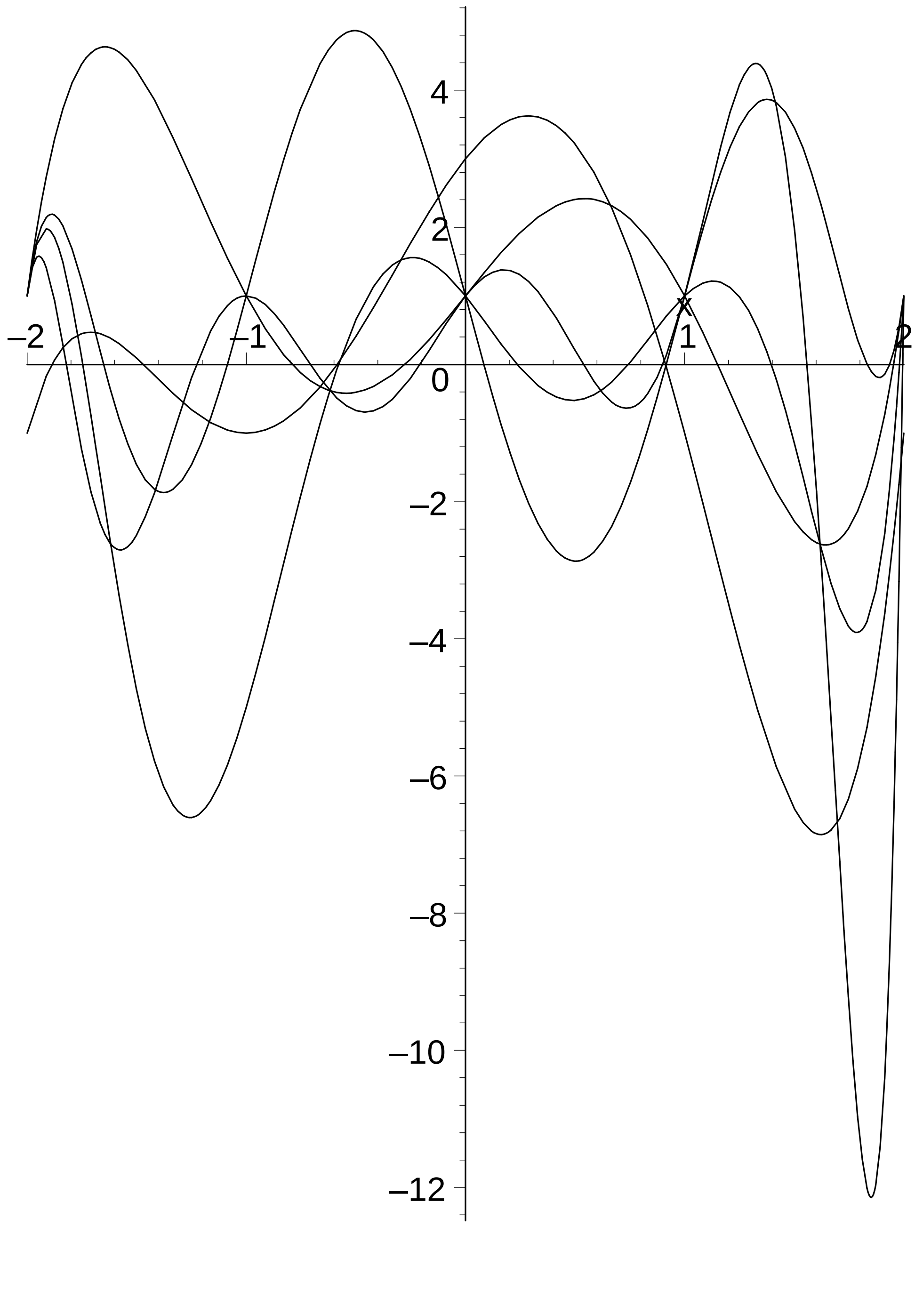
Corollary 1 *If* f *is a monic, nonreciprocal polynomial whose coefficients are all odd integers, then*

$$M(f) \geq M(x^2 - x - 1) = (1 + \sqrt{5})/2.$$

Theorem 2 (Dobrowolski, Mossinghoff and PB) *Suppose f is a monic polynomial with all odd integer coefficients of degree that does not have measure 1.*

a] *Schinzel and Zassenhaus holds for this class with at least one root of modulus at least* $(1 + .31/n)$.

b] *If f is irreducible then Lehmer's conjecture holds for this class and the measure must be at least* 1.495.



4
2
0
–2
–4
–6
–8
–10
–12
–2
–1
1
2
x

A Related Problem of Mahler's. *For each n find the polynomials in $\mathcal{L}_n$ that have largest possible Mahler measure. Analyse the asymptotic behaviour as n tends to infinity.*

Multiplicity of Zeros of Height One Polynomials. *What is the maximum multiplicity of the vanishing at 1 of a height 1 polynomial ?*

Multiplicity of Zeros in $\mathcal{L}_n$. *What is the maximum multiplicity of the vanishing at 1 of a polynomial in $\mathcal{L}_n$?*