Computational Aspects of Problems on Mahler's Measure

Michael Mossinghoff

Davidson College

June 2003

1. Notation.

$$f(x) = \sum_{k=0}^{d} a_k x^k = a_d \prod_{k=1}^{d} (x - \beta_k) \, ,$$

$$L(f) = \sum_k |a_k| \ ,$$

$$H(f) = \max_k |a_k| \ ,$$

$$\|f\|_p = \left(\int_0^1 \left| f(e^{2\pi i t}) \right|^p \, dt \right)^{1/p} ,$$

$$
\begin{aligned}
M(f) &= |a_d| \prod_{k=1}^{d} \max\{1, |\beta_k|\} \\
&= \exp\left(\int_0^1 \log \left| f\left(e^{2\pi i t}\right) \right| \, dt \right) \\
&= \lim_{p \to 0^+} \|f\|_p \,,
\end{aligned}
$$

$$
\begin{aligned}
\ell(x) &= x^{10} + x^9 - x^7 - x^6 \\
&\quad - x^5 - x^4 - x^3 + x + 1\,,
\end{aligned}
$$

$$
f^*(x) = x^d f(1/x)\,.
$$

2. Essentials.

- $M(f) = M(f(x^n)) = M(f^*)$.

- Kronecker: For $f \in \mathbf{Z}[x]$, $M(f) = 1 \iff f(x)$ is a product of cyclotomic polynomials and x.

- Smyth (1971): If $f \neq \pm f^*$ and $f(0) \neq 0$ then $M(f) \geq M(x^3 - x - 1) = 1.324717\ldots$.

- Dobrowolski (1979): If f is irreducible and noncyclotomic with degree d then

$$M(f) \geq 1 + c\left(\frac{\log\log d}{\log d}\right)^3.$$

3. Exhaustive Searches.

- $M(f) \le \|f\|_2 \le \|f\|_\infty \le L(f) \le 2^d M(f)$.
  - $a_k/a_d = \pm e_{d-k}(\beta_1, \ldots, \beta_d)$, so
  - $|a_k| \le \binom{d}{k} M(f)$.

- Hence given d and M, there exist only finitely many $f \in \mathbf{Z}[x]$ with $\deg f = d$ and $M(f) \le M$.

- Yields trivial algorithm for finding all f with $\deg f = d$ and $M(f) \le M$.

- With $f = f^*$, this tests $O((2M)^{d/2} e^{d^2/4})$ polys.

Boyd's Algorithm (1980).

(1) Improved Bounds.

- If $M(f) \leq M$ then
$$|a_k| \leq \binom{d}{k} + \binom{d-2}{k-1}\left(M^2 + M^{-2} - 2\right).$$

- Stronger inequality under certain other conditions.

- Example: $d = 10$, $M = 1.3$.
  - Trivial algorithm: $\approx 2 \cdot 10^{10}$ polynomials.
  - Boyd algorithm: 1826 polynomials.

- $O(\exp(d^2 \log M/4))$ polynomials.

(2) Method for Screening Polynomials.

- Graeffe Root-Squaring Algorithm.
  - Write $f(x) = a(x^2) + xb(x^2)$.
  - Define $Gf(x) = a(x)^2 - xb(x)^2$.
  - $Gf(x^2) = f(x)(a(x^2) - xb(x^2))$.
  - Roots of Gf: $\beta_1^2, \ldots, \beta_d^2$.
  - $M(Gf) = M(f)^2$.

- Since
$$M(G^k f) \le L(G^k f) \le 2^d M(G^k f)$$
then
$$M(f) \le L(G^k f)^{2^{-k}} \le 2^{d/2^k} M(f),$$
so
$$\lim_{k\to\infty} L(G^k f)^{2^{-k}} = M(f).$$

- Method: Test coefficients of $G^k f$ for $k \le m$, for fixed parameter m.

- Fast and exact.

Example: $M = 1.3$.

- Let $f(x) = x^8 - x^7 + x^6 + x^5 + x^3 + x^2 - x + 1$ ($M(f) \approx 1.771$).

- $a(x) = x^4 + x^3 + x + 1$,
$b(x) = -x^3 + x^2 + x - 1$.

- $Gf(x) = a(x)^2 - xb(x)^2$
$= x^8 + x^7 + 3x^6 + 3x^5 + 3x^3 + 3x^2 + x + 1.$

- $\boldsymbol{G^2 f(x) = x^8 + 5x^7 + 3x^6 - 9x^5 - 9x^3 + 3x^2 + 5x + 1.}$

- $\boldsymbol{G^3 f(x) = x^8 - 19x^7 + 99x^6 + 15x^5 - 192x^4 + 15x^3 + 99x^2 - 19x + 1.}$

- $\boldsymbol{a_{1,3} = -19}$, but require $\left|\boldsymbol{a_{1,3}}\right| \le \mathbf{14}$. Reject $\boldsymbol{f}$.

```
void Polynomial::Graeffe() {
    int s=1, t, j, k;
    for (k=0; k<=d; k++) w[k] = c[k];
    for (k=0; k<=d; k++) {
        c[k] *= w[k]; t = -s;
        if (s < 0) c[k] = -c[k];
        for (j=1; j<=imin(k,d-k); j++) {
            u=w[k-j]; u*=w[k+j]; u<<=1;
            if (t<0) u=-u; c[k]+=u; t=-t;
        }
        s = -s;
    }
}
```

Searches Performed.

- Boyd (1980): $\boldsymbol{d \leq 16}$, $\boldsymbol{M = 1.3}$.
- Boyd (1989): $\boldsymbol{d \leq 20}$, $\boldsymbol{M = 1.3}$.
- M. (1995): $\boldsymbol{d \leq 24}$, $\boldsymbol{M = 1.3}$.
- New algorithm: G. Rhin (June 23).

4. Height 1 Search.

Theorem: If $f \in \mathbf{Z}[x]$ has $M(f) < 2$ then there exists $g \in \mathbf{Z}[x]$ with $H(fg) = 1$.

- So if one can bound the multiplicity of a noncyclotomic factor of a height 1 polynomial then Lehmer's problem follows.

- Proof: Use Siegel's Lemma.

  - For f irreducible: Box principle.

- Degree of auxiliary g can be bounded, but no bound known on $M(g)$.

- Often, g exists with small degree and $M(g) = 1$.

- If true, need only test $O(\sqrt{3}^d)$ polynomials.

- Searches performed ($M = 1.3$).
  - Boyd (1989): $d \leq 32$.
  - M. (1995): $d \leq 40$.

- Finds all from exhaustive search by $d = 28$.

5. Perturbed Cyclotomic Products.

- M., Pinner, Vaaler (1998).
- $\ell(x) = \Phi_1^2(x)\Phi_2^2(x)\Phi_3^2(x)\Phi_6(x) - x^5$.
- Algorithm. Given M, $d = 2e$.
  - Construct all $g \in \mathbf{Z}[x]$ with $M(g) = 1$, $g(0) = 1$, $\deg g = d$.
  - (Restrict multiplicity of cyclotomic factors.)
  - Test $g(x) \pm x^e$ (and similar perturbations).

- Complexity.
  - Boyd, Montgomery (1988): Number of cyclotomic products of degree d is

$$\sim \frac{A\exp(B\sqrt{d})}{d\sqrt{\log d}},$$

$$A = \sqrt{105\zeta(3)}/4\pi^2 e^{\gamma/2} \approx 0.2132,$$

$$B = \sqrt{105\zeta(3)}/\pi \approx 3.576.$$

  - Multiplicity ≤ 2:

$$0.2187\exp(2.920\sqrt{d})/d^{3/4}.$$

- Results of search through $d = 64$.
  - Finds 88% of polynomials with $M(f) < 1.3$ and $\deg f \leq 32$.
  - Finds all known measures less than 1.23.
  - 241 different representations found for $M(\ell)$.

1.176280	$\Phi_1^2\Phi_2^2\Phi_3^2\Phi_6 - x^5$
1.188368	$\Phi_1^2\Phi_2^2\Phi_3^2\Phi_4\Phi_6\Phi_9 + x^9$
1.200026	$\Phi_1^2\Phi_2^2\Phi_4\Phi_6\Phi_7 + x^7$
1.201396	$(\Phi_1^2\Phi_5^2\Phi_7\Phi_{10} + x^{10})/\Phi_6$
1.202616	$\Phi_1^2\Phi_2^2\Phi_3\Phi_4\Phi_6\Phi_{12} + x^7$
1.205019	$(\Phi_2^2\Phi_{10}\Phi_{16}\Phi_{26} - x^{13})/\Phi_{12}$
1.207950	$\Phi_1^2\Phi_2^2\Phi_3\Phi_4\Phi_6\Phi_7\Phi_9\Phi_{18} + x^{14}$
1.212824	$(\Phi_1^2\Phi_3\Phi_8\Phi_9\Phi_{13} + x^{13})/\Phi_{14}$
1.214995	$\Phi_1^2\Phi_2^2\Phi_3\Phi_5^2\Phi_6\Phi_{10} + x^{10}$
1.216391	$\Phi_1^2\Phi_2^2\Phi_3\Phi_4\Phi_6 + x^5$
1.218396	$(\Phi_1^2\Phi_3^2\Phi_4\Phi_6\Phi_7\Phi_{12}^2 + x^{12})/\Phi_{10}$
1.218855	$\Phi_1^2\Phi_2^2\Phi_3\Phi_4\Phi_6\Phi_7\Phi_{10}\Phi_{12} + x^{12}$
1.219057	$(\Phi_1^2\Phi_3\Phi_4\Phi_5\Phi_{44} + x^{15})/\Phi_{14}$
1.219446	$\Phi_1^2\Phi_2^2\Phi_3^2\Phi_4^2\Phi_6\Phi_{12} + x^9$
1.219720	$\Phi_1^2\Phi_2^2\Phi_3\Phi_4\Phi_8\Phi_9 + x^9$

6. A Problem of J. Vaaler.

- Given $f \in \mathbf{Z}[x]$, monic, with $M(f) > 1$, and $k \geq 1$. Find $A, B \in \mathbf{Z}[x]$ with $M(A) = M(B) = 1$ so that
$$f^k(x) = rA(x) + sB(x)$$
with $r, s \in \mathbf{Z}$.

- May assume $\deg A = k \deg f$ so $r = 1$.

- Algorithm.
  - Construct all A with $M(A) = 1$ and $A(0) \neq 0$.
  - For each A, test if $f^k - A = sB$ with $M(B) = 1$.

- Fast cyclotomic detector: Graeffe algorithm.
- Note $G\Phi_n = \begin{cases} \Phi_n, & n \text{ odd}, \\ \Phi_{n/2}, & n/2 \text{ odd}, \\ \Phi_{n/2}^2, & n/2 \text{ even}. \end{cases}$
- Algorithm.
  - If $|a_k| > \binom{d}{k}$ for some k then **no**.
  - If $Gf = f$ then **yes**.
  - Set $f := Gf$ and repeat.
  - If more than $\lceil \log_2 d \rceil$ iterations then **no**.

$$\begin{aligned}\ell^2 &= \Phi_2^2\Phi_8\Phi_{16}\Phi_{18} - x^3\Phi_3\Phi_5\Phi_{30}\\ &= \Phi_7^2\Phi_{20} - x^2\Phi_2^4\Phi_3\Phi_6\Phi_{24}\\ &= \Phi_3^2\Phi_{20}\Phi_{30} - x\Phi_2^2\Phi_8\Phi_{42}\\ &= \Phi_{30}\Phi_{42} - x^5\Phi_1^2\Phi_2^4\Phi_3^2.\end{aligned}$$

No representations for ℓ^k for $3 \le k \le 7$.

$$(1+x-x^2+x^3+x^4)^3 = \Phi_4^3\Phi_9 + 3x\Phi_6\Phi_{12}^2.$$

$$(1+x-x^3-x^7+x^9+x^{10})^3 =$$
$$\Phi_5\Phi_{22}\Phi_{30}^2 + x\Phi_3\Phi_{12}^2\Phi_{18}\Phi_{28}.$$

7. Two-Variable Polynomials.

$$\log M(f(x,y)) = \int_0^1 \int_0^1 \log |f(e(s), e(t))| \, ds \, dt,$$

where $e(s) = e^{2\pi i s}$.

- Boyd, Lawton: $\lim_{n \to \infty} M(f(x, x^n)) = M(f(x,y))$.

- Algorithm.
  - Find small limit point.
  - Specialize $y = x^n$.

- Specialization with smallest known measures generates most known $f(x)$ with small measure.

- Four $f(x, y)$ known with $1 < M(f) < 1.3247$.

- Smallest known limit of two-variable measures: $M(1 + x + y) = 1.38135\ldots$.

- Boyd (1978): Multivariable version of Kronecker.

  $M(f(x, y)) = 1$ iff $f(x, y) = \prod_k \Phi_k^{n_k}(x^{a_k} y^{b_k})$.

- Boyd conjecture (1981): The set

$$L = \bigcup_{n \geq 1} \{M(f) : f \in \mathbf{Z}[x_1, \ldots, x_n]\}$$

  is closed.

  - Suppose so, and suppose $1 \in L'$.
  - Then $\overline{L} = [1, \infty)$, so $L = [1, \infty)$.
  - But L is countable, so $1 \notin L'$.

Searching for Small Two-Variable Measures.

Boyd, M. (2002).

(1) Patterns in Coefficients of One-Variable Measures.

- Example:

$$x^{28} + x^{20} + x^{17} - x^{16} + x^{15} + x^{8} + 1,$$

$$x^{48} + x^{35} + x^{27} - x^{26} + x^{25} + x^{13} + 1,$$

$$x^{60} + x^{44} + x^{33} - x^{32} + x^{31} + x^{16} + 1.$$

- Suggests

$$x^{4n} + x^{3n-1} + x^{2n+3} - x^{2n+2} + x^{2n+1} + x^{n+1} + 1.$$

- Substituting y for x^n yields $f(x, y) =$

$$xy^4 + y^3 + x^4y^2 - x^3y^2 + x^2y^3 + x^2y + 1,$$

- $M(f) = 1.309098\ldots.$

(2) Sparse Multiples of Sporadic Polynomials.

- $f(x) = x^{44} - x^{42} + x^{35} - x^{33} + x^{31} - x^{29} + x^{26} - x^{24} + x^{22} - x^{20} + x^{18} - x^{15} + x^{13} - x^{11} + x^{9} - x^{2} + 1$ has $M(f) = 1.291273\ldots$

- Let $g_0(x) = x^m$, $g_k(x) = x^{m+k} + x^{m-k}$, $1 \le k \le m$.

- Use LLL on lattice spanned by half coefficients of $f(x)g_k(x)$.

- Detects

$$x^{52} + x^{51} + x^{39} + x^{38} + x^{26} + x^{14} + x^{13} + x + 1,$$

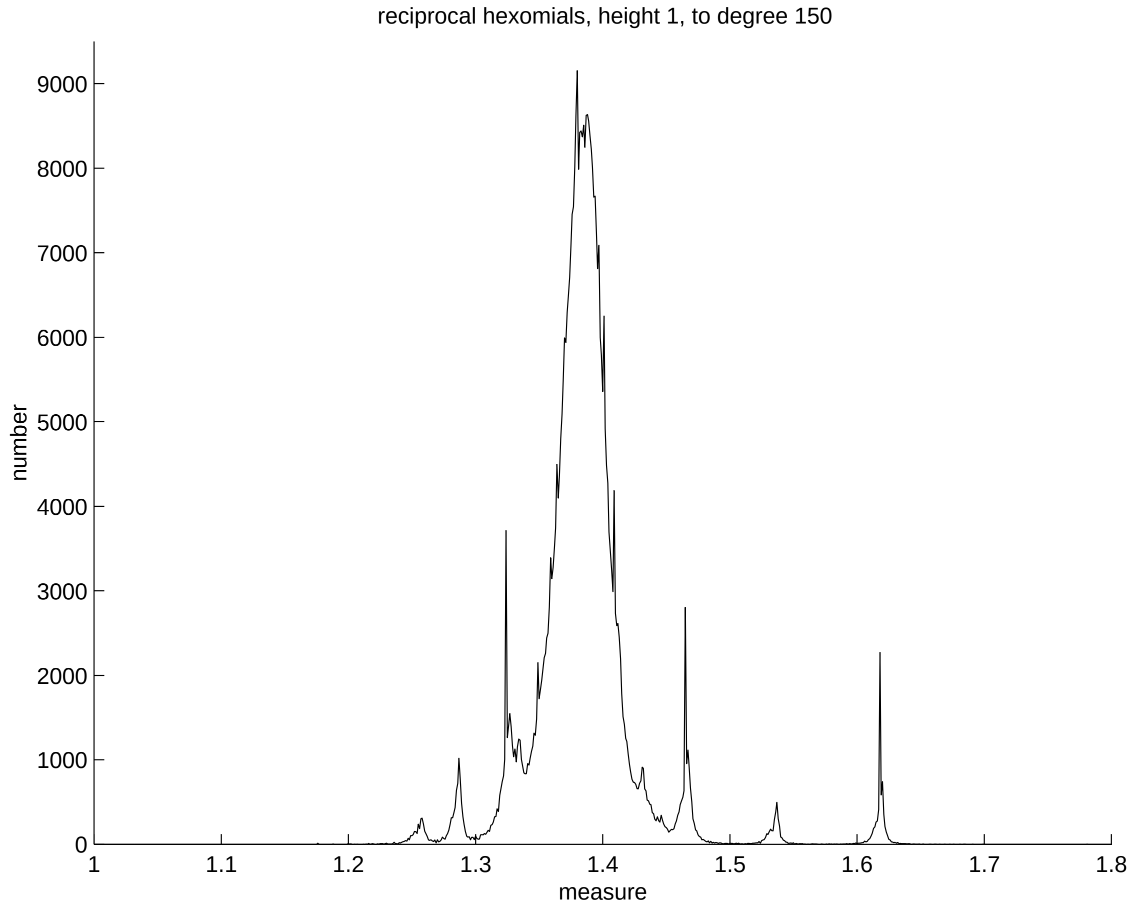
- Suggesting

$$f(x, y) = xy^4 + y^4 + xy^3 + y^3 + xy^2 + x^2y + xy + x^2 + x.$$

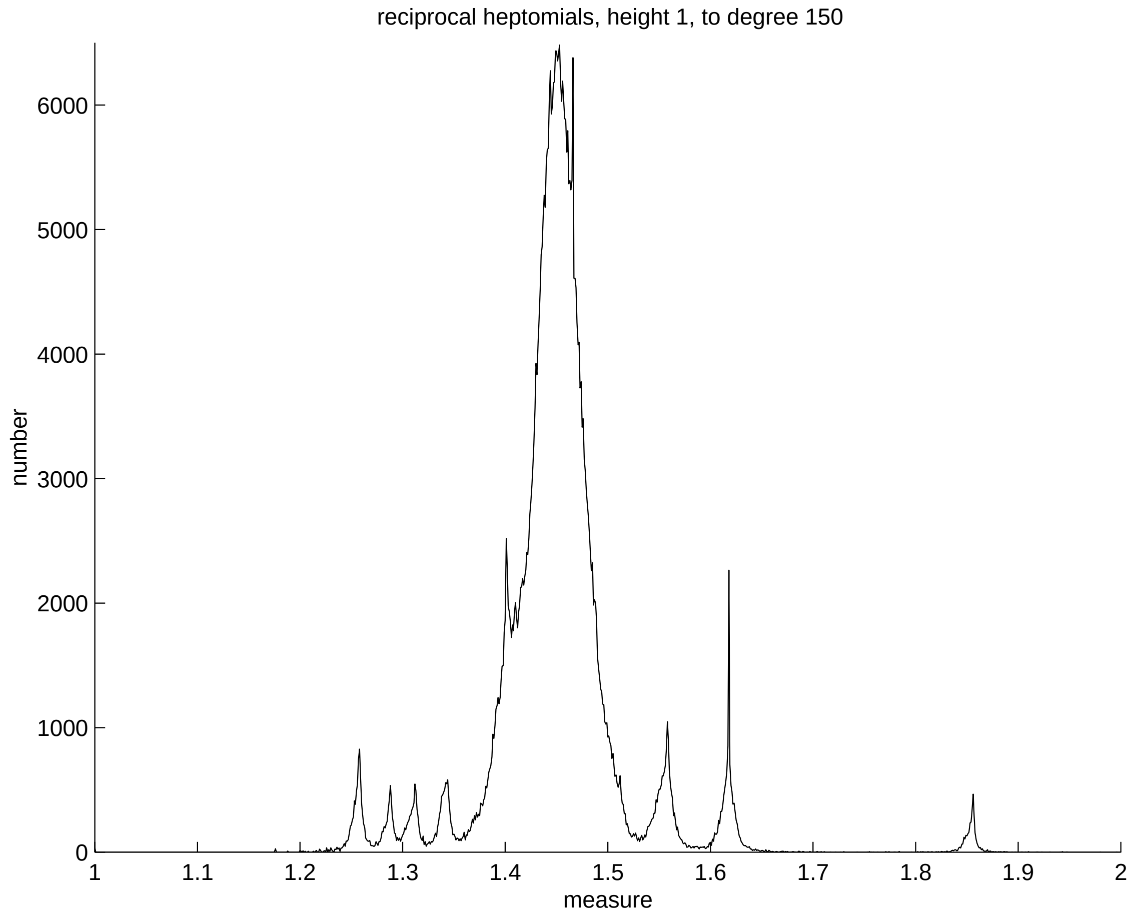
- $M(f) = 1.332051\ldots$

(3) Clustering of Measures of Sparse Polynomials.

- Reciprocal hexomials with height 1.



• Reciprocal heptomials with height 1.



(4) Systematic Searches.

- Reciprocal f with $H(f) = 1$, $\deg_x(f) \leq 9$, and $\deg_y(f) = 2$.

- Symmetric, reciprocal f with $H(f) = 1$, $\deg_x(f) \leq 6$.

- Families of reciprocal hexomials with limiting measure $M(1 + x + y)$.

- $P_{a,b} = (x^a - 1) + (x^b - 1)y + x^{b-a}(x^a - 1)y^2.$

- $Q_{a,b} = 1 + x^a + (1 + x^b)y + x^{b-a}(1 + x^a)y^2.$

- $R_{a,b} = 1 + x^a + (1 - x^b)y - x^{b-a}(1 + x^a)y^2.$

- $S_{a,b,\epsilon} = 1 + (x^a + \epsilon)(x^b + \epsilon)y + x^{a+b}y^2.$

- $T_f = f(x)y + f^*(x)$, with $f(x) = 1 \pm x^a \pm x^b$.

1.	$\mathbf{1.25543386626660}$	$P_{2,3}$
2.	$\mathbf{1.28573486429198}$	$P_{1,3}$ or $P_{2,1}$
3.	$\mathbf{1.30909838065232}$	++000|+0−0+
4.	$\mathbf{1.31569270298664}$	$P_{3,5}$
5.	$\mathbf{1.32471795724474}$	T_{1+x-x^3}
6.	$\mathbf{1.32537249730758}$	$P_{3,4}$
7.	$\mathbf{1.33205110543741}$	$P_{2,5}$
8.	$\mathbf{1.33239612945871}$	$S_{1,3,+}$
9.	$\mathbf{1.33813743193884}$	$P_{3,2}$
10.	$\mathbf{1.33999992173818}$	$P_{4,7}$
11.	$\mathbf{1.34050688293084}$	$P_{3,1}$
12.	$\mathbf{1.34971610466969}$	$T_{1+x^2+x^7}$
13.	$\mathbf{1.35001483216301}$	$P_{3,7}$
14.	$\mathbf{1.35031697905986}$	$S_{1,4,-}$
15.	$\mathbf{1.35114589566970}$	$P_{4,5}$

16. $\mathbf{1.35246806251886}$ $\boldsymbol{P_{5,9}}$

17. $\mathbf{1.35369764946263}$ $\boldsymbol{Q_{1,6}}$

18. $\mathbf{1.35674810514560}$ $\boldsymbol{P_{4,3}}$

19. $\mathbf{1.35678598845264}$ $\boldsymbol{P_{5,8}}$

20. $\mathbf{1.35812963240441}$ ++00000|+0−−−0+

21. $\mathbf{1.35854559039605}$ $\boldsymbol{P_{4,1}}$

22. $\mathbf{1.35920806869955}$ $\boldsymbol{P_{4,9}}$

23. $\mathbf{1.35981177528194}$ $\boldsymbol{P_{6,11}}$

24. $\mathbf{1.35981589898774}$ $\boldsymbol{S_{1,6,+}}$

25. $\mathbf{1.35991414938211}$ $\boldsymbol{T_{1+x+x^8}}$

30. $\mathbf{1.36443581178063}$

$\boldsymbol{1 + x^2(1+x)y + (1+x)y^2 + x^3y^3}$

39. $\mathbf{1.36688307085922}$ $\boldsymbol{R_{1,5}}$

Computing Measures.

- Let $\beta_i(t)$ denote roots in y of $f(e(t), y) = 0$ for $0 \leq t \leq 1$.

- Jensen's formula:

$$\log M(f(x,y)) = 2 \sum_i \int_{\substack{|\beta_i(t)|>1 \\ 0\leq t\leq 1/2}} \log |\beta_i(t)| \, dt.$$

- Usually for each t only one branch has $|\beta_i(t)| > 1$.

- Numerical integrator + Root finder (Maple, PARI).

Example.

$$f(x,y) = (1+x+x^2) + y(1+x+x^2+x^3) \\ + xy^2(1+x+x^2).$$

$$f(e(t),y) = e(t)s(t) + 2ye(3t/2)r(t) + y^2 e(2t)s(t),$$

where

$$r(t) = \cos 3\pi t + \cos \pi t,$$
$$s(t) = 2\cos 2\pi t + 1.$$

Roots of discriminant: $t_1 \approx .301$, $t_2 \approx .388$.

$$\int_{t_1}^{t_2} \log\left(\sqrt{r(t)^2 - s(t)^2} - r(t)\right) dt \approx -.0106005.$$

$$\begin{aligned}\int_{t_1}^{t_2} \log|s(t)|\,dt = (t_2 - z)\log|s(t_2)| \\ + (z - t_1)\log|s(t_1)| \\ + \int_{t_1}^{t_2} (z-t)\frac{s'(t)}{s(t)}\,dt \approx -.151447,\end{aligned}$$

with $z = 1/3$.

$$M(f(x,y)) \approx \exp(2(.1514 - .0106)) = 1.32537.$$

Faster Screening.

- Simple probabilistic method.
  - Select θ and $n_1, \ldots, n_m$.
  - Reject f if mean of $M(f(x, x^{n_i})) > \theta$.
  - Repeat.

- Analogue of root-squaring.
  - $M(f) < M \implies$ bounds on coefficients of $f(x,y)$ with fixed support.
  - Define

$$\begin{aligned} Tf = & f(x^{1/2}, y^{1/2}) f(-x^{1/2}, y^{1/2}) \\ & f(x^{1/2}, -y^{1/2}) f(-x^{1/2}, -y^{1/2}). \end{aligned}$$

  - $M(Tf) = M(f)^4$.
  - Boyd (1998): $L(T^k f)^{4^{-k}} \to M(f)$.
  - Unwieldy.

8. Other Searches.

(1) Sparse Polynomials.

- Height 1, reciprocal, with fixed number of terms, $\boldsymbol{n}$.
- $\boldsymbol{O(d^{\lceil n/2 \rceil})}$.
- Finds all polynomials from previous searches with $\boldsymbol{M(f) < 1.3}$.
- M. (1998). $\boldsymbol{n \le 7}$: $\boldsymbol{d \le 181}$; $\boldsymbol{n \le 9}$: $\boldsymbol{d \le 131}$, etc.
- Lisonek (2000): A few more with $\boldsymbol{174 \le d \le 180}$.

(2) Newman Polynomials.

- Reciprocal polynomials with $\{0, 1\}$ coefficients.
- $O(2^{d/2})$.
- Test through $d = 70$.
- Smallest 33 known measures (< 1.2305) found.
- Does there exist $M_0 > 1$ so that if $M(f) < M_0$ then there exists g such that $M(fg)$ has $\{0, 1\}$ coefficients?
- Can we demand $M(g) = 1$?

d	Measure	n_{70}	d_1	Half of Coefficients
10	1.17628	7500	13	++000+
18	1.18836	69	55	++++++0+000000000+000000000
14	1.20002	1534	28	+00+0+00000000
18	1.20139	872	19	+00+0++++
14	1.20261	2567	20	++0000000+
22	1.20501	1051	23	++++0+00+0+
28	1.20795	346	34	+0+000000000000+0
20	1.21282	1247	24	++00000+00+0
20	1.21499	481	34	+0+0+000000+0+000
10	1.21639	4819	18	++0000000
20	1.21839	661	22	+000++0++++
24	1.21885	849	42	+++++0000000++0000000
24	1.21905	419	37	+00+0+0++0+0+00000
18	1.21944	312	47	++++++000+0000000000000
18	1.21972	460	46	++000++0000+00000000000
34	1.22028	0	95	++++++++++++++0+++++++++000000000+00000000000000
38	1.22344	173	44	+00+000000000000000+00
26	1.22377	21	59	++++++++000000000+00000000000
16	1.22427	3573	18	+0000000+
18	1.22550	2459	22	+000+000000
30	1.22561	341	30	+0+0000000000+0
30	1.22581	0	74	++++++++++000+0000000++00000000000+000
26	1.22609	861	26	+00+000000+00
36	1.22649	20	52	+000000000000000000+++++++
20	1.22699	755	24	+000000000++
12	1.22778	4841	20	+0+0000+00
30	1.22814	296	36	+0000+0000000+0000
36	1.22948	0	78	+++++++++0000000000000++++00000000000000
22	1.22956	660	30	+0000+0+0000000
34	1.22999	85	61	++++++00000000000+++++00000000

9. Web Site on Lehmer's Problem.

- Presently at www.math.ucla.edu/∼mjm/lc.
  Will move in the near future!
  - Small measures to degree 180.
  - Small Salem numbers.
  - Small measures of $\{-1, 1\}$ polynomials.
  - Small values of $M(f(x, y))$.
  - References. Additions welcome!