THE TRACE PROBLEM FOR TOTALLY POSITIVE ALGEBRAIC INTEGERS

JULIÁN AGUIRRE AND JUAN CARLOS PERAL,
WITH AN APPENDIX BY JEAN-PIERRE SERRE

ABSTRACT. Suppose that $P(x) = x^d + a_1 x^{d-1} + \cdots + a_d$ is a polynomial with integer coefficients, irreducible, and with all roots real and positive. In a remarkable paper of 1918, I. Schur proved that if $c < \sqrt{e}$, then there are only finitely many such polynomials for which the average of the roots, equal to $-a_1/d$, is less than c. The Schur-Siegel-Smyth trace problem asks for the largest value of c for which the same conclusion holds. In this paper we give an account of the history of the problem, the latest results, and its relations with other problems in number theory.

1. INTRODUCTION

An *algebraic number* is a complex number α that satisfies a polynomial equation

$$a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n = 0,$$

where the coefficients $a_k \in \mathbb{Z}$, the ring of integers. If the leading coefficient a_0 equals 1, then α is said to be an *algebraic integer*. The set of all algebraic numbers is a field, while the set of all algebraic integers, that we shall denote by $\mathbb{A}$, is a ring. Given $\alpha \in \mathbb{A}$ there is a unique monic polynomial $P \in \mathbb{Z}[x]$, the ring of all polynomials in one indeterminate with integer coefficients, such that both $P(\alpha) = 0$, and also if $Q \in \mathbb{Z}[x]$ is such that $Q(\alpha) = 0$, then P divides Q in $\mathbb{Z}[x]$. This polynomial P is irreducible, and is called the *minimal polynomial* of α; its degree is called the *degree* of α.

Let α be an algebraic integer of degree d and let $P(x) = x^d + a_1 x^{d-1} + \cdots + a_d$ be its minimal polynomial. Then P has d different roots $\alpha_1, \ldots, \alpha_d$, which are called the *conjugates* of α. We have

$$P(x) = (x - \alpha_1) \ldots (x - \alpha_d).$$

If all the conjugates of $\alpha \in \mathbb{A}$ are real, then α is said to be *totally real*; if they are all positive, then α is said to be *totally positive*. The set of all totally positive algebraic integers will be denoted by $\mathbb{A}_+$.

2000 *Mathematics Subject Classification.* 11R06.

Key words and phrases. Totally positive algebraic integers, Schur-Siegel-Smyth trace problem.

J. Aguirre supported by grant 9/UPV127.310-15969/2004 of the Universidad del País Vasco.

Associated with $\alpha \in \mathbb{A}$ there are several quantities of interest in algebraic number theory, among them the *trace*

$$\mathrm{Trace}(\alpha) = \sum_{k=1}^{d} \alpha_k = -a_1,$$

the *norm*

$$\mathrm{Norm}(\alpha) = \prod_{k=1}^{d} \alpha_k = (-1)^d a_d,$$

and the *discriminant*

$$\mathrm{Disc}(\alpha) = \Delta(\alpha_1, \ldots, \alpha_d),$$

where Δ is the function defined by

$$\Delta(x_1, \ldots, x_d) = \prod_{1 \le i < j \le d} (x_i - x_j)^2. \tag{1}$$

For a monic polynomial $P \in \mathbb{Z}[x]$, $\mathrm{Trace}(P)$, $\mathrm{Norm}(P)$ and $\mathrm{Disc}(P)$ are defined as $\mathrm{Trace}(\alpha)$, $\mathrm{Norm}(\alpha)$ and $\mathrm{Disc}(\alpha)$, where α is any root of P. It is clear that the trace and the norm are integers, and it turns out that so is the discriminant. The *resultant* of two polynomials $P(x) = a_0 x^n + \cdots + a_n$ of degree n and $Q(x) = b_0 x^m + \cdots + b_m$ of degree m is defined as

$$\mathrm{Resultant}(P, Q) = a_0^m \prod_{P(x)=0} Q(x),$$

that is, a_0^m times the product of the values of Q on the roots of P. If P and Q have integer coefficients, then $\mathrm{Resultant}(P, Q)$ is also an integer. Moreover, $\mathrm{Resultant}(P, Q) = 0$ if and only if P and Q have a common root. In particular, if $P, Q \in \mathbb{Z}[x]$ are coprime, then $\big|\mathrm{Resultant}(P, Q)\big| \ge 1$. All the above facts about algebraic integers can be found in any text on algebraic number theory, for instance [3].

We shall also use the family of measures defined by

$$M_p(\alpha) = \Big(\frac{1}{d} \sum_{k=1}^{d} |\alpha_k|^p \Big)^{1/p}, \quad p > 0.$$

If $\alpha \in \mathbb{A}_+$, then $\mathrm{Trace}(\alpha) = d \cdot M_1(\alpha)$. It follows from the inequality between the arithmetic and the geometric means that

$$M_p(\alpha) \ge \big|\mathrm{Norm}(\alpha)\big|^{1/d},$$

and thus that $M_p(\alpha) > 1$ unless $\alpha = 0$ or $\alpha = \pm 1$. The spectrum of the measure M_p is defined as the set

$$\mathcal{T}_p = \{\, M_p(\alpha) : \alpha \in \mathbb{A}_+, \alpha \ne 1 \,\}.$$

For each positive integer n, $\theta_n = 4\cos^2\bigl(\pi/(2\,n)\bigr) \in \mathbb{A}_+$. Its minimal polynomial is a factor of

$$P_n(x) = x^{[n/2]} + \sum_{k=1}^{[n/2]} (-1)^k \frac{n}{k} \binom{n-k-1}{k-1} x^{[n/2]-k}$$
$$= x^{[n/2]} - n\,x^{[n/2]-1} + \frac{n(n-3)}{2}\,x^{[n/2]-2} - \cdots \pm a_{[n/2]},$$

where $[\,\cdot\,]$ is the integer part function, $a_{[n/2]} = \pm 2$ if n is even, and $a_{[n/2]} = \pm n$ if n is odd. Eisenstein's irreducibility criterion implies that if n is an odd prime or a power of two, then P_n is irreducible. It follows that $M_1(\theta_p) = 2\,p/(p-1)$ if p is an odd prime, and $M_1(\theta_{2^n}) = 2$ for all positive integers n. Thus 2 is a limit point of $\mathcal{T}_1$, and there is an infinite number of totally positive algebraic integers, of different degree, for which the value of M_1 is 2. The Schur-Siegel-Smyth trace problem, as stated by Peter Borwein in [4], is the following.

Schur-Siegel-Smyth Trace Problem. *Given any $\epsilon > 0$, prove that the set*

$$\{\,\alpha \in \mathbb{A}_+ : M_1(\alpha) < 2 - \epsilon\,\}$$

is finite, and if possible, find all its elements.

In other words, the problem asks whether 2 is in fact the smallest limit point of $\mathcal{T}_1$. A more general form of the problem is to find the structure of $\mathcal{T}_1$. Of course the same problem can be posed for each of the sets $\mathcal{T}_p$, $p > 0$, but our main concern will be with the case $p = 1$.

Sometimes the problem is stated for the class of totally real algebraic integers instead of for the class of totally positive algebraic integers. However both problems are equivalent, since if α is totally real, then $\alpha^2 \in \mathbb{A}_+$ and $M_p(\alpha^2) = \bigl(M_{2p}(\alpha)\bigr)^2$.

The rest of the paper is divided into four sections and two appendices. Section 2 is devoted to the work of I. Schur, C.L. Siegel and C.J. Smyth on the trace problem. In Section 3 we explain the method of auxiliary functions and give the best results known. Section 4 deals with the relation between the trace problem and the integer Chebyshev problem, and Section 5 is dedicated to the special case of cyclotomic algebraic integers. Appendix A gives the best result, as far as we know, for the trace problem. Appendix B contains a letter from J.-P. Serre to C. Smyth.

Acknowledgements

We wish to thank C.J. Smyth for providing us with a copy of J.-P. Serre's letters, and for several suggestions that have resulted in an improvement of the paper. We also wish to thank J.-P. Serre for kindly giving permission to publish his letter to Smyth as Appendix B, as well as for his suggestions for putting it into context.

2. Earlier results

In this section we describe the results obtained by I. Schur, C.L. Siegel and C.J. Smyth.

The work of I. Schur. The first result on the trace problem appears in I. Schur's 1918 paper [15], and is based on the following inequality for the function Δ defined in (1):

Theorem (Schur [15, Satz II]). *The maximum of $\Delta(x_1,\dots,x_d)$ over the set of real n-tuples $(x_1,\dots,x_d)$ such that $x_1^2+\cdots+x_d^2\le 1$ is*

$$\mu_d = (d^2-d)^{-\frac{1}{2}(d^2-d)} \prod_{k=2}^{d} k^k.$$

It follows from Euler's summation formula that

$$\prod_{k=2}^{d} k^k = e^{\sum_{k=2}^{d} k\log k} = O\big(d^{\frac{1}{2}(d^2+d)+\frac{1}{12}}\, e^{-\frac{d^2}{4}}\big),$$

and then

$$\mu_d = O\big(d^{\frac{1}{2}(3d-d^2)+\frac{1}{12}}\, e^{-\frac{1}{4}(2d-d^2)}\big). \tag{2}$$

Schur considers next totally real algebraic integers α of degree d, with minimal polynomial $x^d+a_1x^{d-1}+\cdots+a_d$, and such that $\alpha_1^2+\cdots+\alpha_d^2\le\gamma\, d$ for some $\gamma>0$. The definition of the discriminant implies that $\mathrm{Disc}(\alpha)>0$, and since the discriminant is an integer, we have

$$1\le \mathrm{Disc}(\alpha)\le (\gamma\, d)^{\frac{1}{2}(d^2-d)}\mu_d = O\big(e^{\frac{d}{4}}\, d^{d+\frac{1}{12}}\, (e^{-\frac{1}{2}}\gamma)^{\frac{1}{2}(d^2-d)}\big). \tag{3}$$

If $\gamma<\sqrt{e}=1.648721\dots$, then the right hand side of (3) converges to zero as d goes to infinity. Since on the other hand $\mathrm{Disc}(\alpha)\ge 1$, there exists a positive integer d_0 such that $d\le d_0$. Moreover, $|\alpha_k|\le\sqrt{\gamma\, d}$ for $1\le k\le d$. Thus

$$|a_k| = \sum_{1\le i_1<i_2<\cdots<i_k\le d} \alpha_{i_1}\alpha_{i_2}\dots\alpha_{i_k} \le \binom{d}{k}(\gamma\, d)^{\frac{k}{2}}.$$

This concludes the proof of the following:

Theorem (Schur [15, Satz VIII]). *Let γ be a positive constant such that $\gamma<\sqrt{e}$. Then the number of totally real algebraic integers α such that*

$$a_1^2-a_2 = \frac{\alpha_1^2+\cdots+\alpha_d^2}{d}\le\gamma$$

is finite.

Finally, using the observation made in the introduction, this theorem is restated as:

Theorem (Schur [15, Satz XI]). *Let γ be a positive constant such that $\gamma < \sqrt{e}$. Then the number of totally positive algebraic integers α such that*

$$\frac{\alpha_1 + \cdots + \alpha_d}{d} \le \gamma$$

is finite.

The work of C.L. Siegel. The next advance is due to C.L. Siegel in his 1945 paper [16]. The first result in the paper is an improvement of the classical inequality between the arithmetic and the geometric means involving the function Δ. Given an integer $d \ge 2$ define a polynomial P and a rational function Q by

$$P(t) = \frac{1}{d!}\prod_{k=0}^{d-2}\Big(\frac{t+k}{d-k}\Big)^{d-k-1}, \qquad Q(t) = \prod_{k=1}^{d-1}\Big(1 + \frac{d-k}{t+k-1}\Big).$$

Theorem (Siegel [16, Theorem I]). *Let $x_1, \dots, x_d$ be positive real numbers such that $\Delta(x_1, \dots, x_d) \ne 0$, and let μ be the unique positive solution of the algebraic equation*

$$P(\mu) = \frac{(x_1 \dots x_d)^{d-1}}{\Delta(x_1, \dots, x_d)};$$

then

$$\Big(\frac{x_1 + \cdots + x_d}{d}\Big)^d \ge Q(\mu)\, x_1 \dots x_d. \tag{4}$$

The polynomial P has positive coefficients and $P(0) = 0$, so that μ is well defined. Since moreover $Q(\mu) > 1$, (4) is in fact an improvement of the arithmetic-geometric inequality. If $\alpha \in \mathbb{A}_+$, (4) can be rewritten as

$$\big(M_1(\alpha)\big)^d \ge Q(\mu)\,\mathrm{Norm}(\alpha),$$

where μ is the unique positive solution of $P(\mu) = \mathrm{Norm}(\alpha)^{d-1}/\,\mathrm{Disc}(\alpha)$. Since $\mathrm{Norm}(\alpha)$ is positive, it follows that

$$\big(M_1(\alpha)\big)^{d(d-1)} \ge \mathrm{Disc}(\alpha) P(\mu) Q^{d-1}(\mu). \tag{5}$$

This inequality is the starting point for the proof of the following two theorems dealing with the trace problem.

Theorem (Siegel [16, Theorem II]). *Let ϑ be the positive root of the transcendental equation*[†]

$$(1+\vartheta)\log(1+\vartheta^{-1}) + \frac{\log\vartheta}{1+\vartheta} = 1,$$

and let $\lambda_0 = e(1+\vartheta^{-1})^{-\vartheta} = 1.7336\dots$. Then for any $\lambda \in (1, \lambda_0)$ the set

$$\{\, \alpha \in \mathbb{A}_+ : M_1(\alpha) < \lambda \,\}$$

is finite.

[†]There is a misprint in the paper. The '−' on the left hand side should be a '+'.

Theorem (Siegel [16, Theorem III]). *The only $\alpha \in \mathbb{A}_+$ with $M_1(\alpha) \le 3/2$ are $\alpha = 1$ and $\alpha = (3 \pm \sqrt{5})/2$, the roots of the polynomial $x^2 - 3x + 1$.*

These theorems imply in particular that $3/2$ is the smallest point in $\mathcal{T}_1$ and that it is isolated. Siegel finds remarkable that they imply a refinement of Minkowski's inequality between the discriminant and the degree of totally real algebraic fields of sufficiently large degree.

The work of C.J. Smyth. Stimulated by McAuley's Master Thesis [12], C.J. Smyth carries out in his 1984 paper [19] a detailed analysis, both theoretical and numerical, of the structure of the sets $\mathcal{T}_p$ for $p > 0$ (defined in terms of totally real instead of totally positive algebraic integers). His main result for the case $p = 1$, translated to the language we have been using, is as follows.

Theorem (Smyth [19, Theorem 1]).

(1) *The smallest three elements of $\mathcal{T}_1$ are isolated, and are the only elements of $\mathcal{T}_1$ in the interval $(1, 1.7719)$:*

$$(1, 1.7719) \cap \mathcal{T}_1 = \left\{ \frac{3}{2}, \frac{5}{3}, \frac{7}{4} \right\}.$$

These values are $M_1(\alpha)$, where $\alpha \in \mathbb{A}_+$ is a root of one of the polynomials $x^2 - 3x + 1$, $x^3 - 5x^2 + 6x - 1$, $x^4 - 7x^3 + 13x^3 - 7x + 1$, $x^4 - 7x^3 + 14x^3 - 8x + 1$.

(2) *The set $\mathcal{T}_1$ is dense in $[2, +\infty)$.*

From this theorem we see that the structure of $\mathcal{T}_1$ is undetermined only in the interval $(1.7719, 2)$. Let us remark again that Smyth proves similar results for all $p > 0$.

The ideas for proving the above theorem had already been developed by Smyth in [17, 18] to treat the corresponding problem for the measure

$$\Omega(\alpha) = \Big(\prod_{k=1}^{d} \max\big(1, |\alpha_k|\big) \Big)^{1/d}.$$

The methods for proving (1) and (2) are quite different. We will explain with some detail in the next section the method used to prove (1), known as the method of auxiliary functions, which can be applied to a large class of problems in the theory of polynomials with integer coefficients. Whereas Schur's and Siegel's results were based on inequalities for the discriminant of an algebraic integer, the method of auxiliary functions exploits an inequality for the resultant of two polynomials, one of them being the minimal polynomial of an algebraic integer.

3. The method of auxiliary functions

Suppose that somehow we are able to find a polynomial $Q \in \mathbb{Z}[x]$ and real constants $y > 0$, c such that

$$x - y \log |Q(x)| \geq c \quad \text{for all } x > 0. \tag{6}$$

If $\alpha \in \mathbb{A}_+$ has conjugates $\alpha_1, \ldots, \alpha_d$, then

$$\alpha_k - y \log |Q(\alpha_k)| \geq c, \quad 1 \leq k \leq d.$$

Adding these inequalities and dividing by d we get

$$M_1(\alpha) \geq c + y \log \Big| \prod_{k=1}^{d} Q(\alpha_k) \Big| = c + y \log |\operatorname{Resultant}(P, Q)|,$$

where P is the minimal polynomial of α. If $Q(\alpha) \neq 0$, then

$$|\operatorname{Resultant}(P, Q)| \geq 1$$

and $M_1(\alpha) \geq c$. Thus inequality (6) implies that

$$(1, c) \cap \mathcal{T}_1 \subset \{ M_1(\alpha) : Q(\alpha) = 0 \},$$

and in particular that $(1, c) \cap \mathcal{T}_1$ is finite. Define the constant $\mathcal{K}$ as

$$\mathcal{K} = \sup_{Q \in \mathbb{Z}[x],\, Q \neq 0,\, y > 0} \Big\{ \inf_{x > 0} \Big(x - y \log |Q(x)| \Big) \Big\}. \tag{7}$$

Reasoning as above, it is easy to see that

$$(1, c) \cap \mathcal{T}_1 \text{ is finite for all } c < \mathcal{K}.$$

What Smyth did to prove the first part of his theorem is to compute explicitly a polynomial $Q \in \mathbb{Z}[x]$ and a constant $y > 0$ such that

$$x - y \log |Q(x)| \geq 1.7719$$

for all $x > 0$, proving that $\mathcal{K} > 1.7719$.

How does one find such Q and a? In practice, one chooses N irreducible polynomials $Q_i \in \mathbb{Z}[x]$ and solves the optimization problem

$$\sup \Big\{ \min_{x > 0} \Big(x - \sum_{k=1}^{N} c_k \log |Q_k(x)| \Big) \Big\}, \tag{8}$$

where the supremum is taken over all N-tuples $(c_1, \ldots, c_N) \in \mathbb{R}^N$ with $c_k > 0$ for $1 \leq k \leq N$. The function $x - \sum_{k=1}^{N} c_k \log |Q_k(x)|$ is called an *auxiliary function*. The method can be adapted to study other measures. For instance, if we change x to x^p, $p > 0$, then we obtain results about the sets $\mathcal{T}_p$; changing x to $\max(0, \log x)$ will provide information on the spectrum of the Mahler measure. It should be noted that in Smyth's original approach, (8) appears as the dual of another optimization problem on the set of all probability measures on $(0, +\infty)$.

When we apply the method of the auxiliary functions we are confronted with two different problems:

(1) Find appropriate polynomials Q_k.
(2) Once the polynomials have been chosen, find the values of the coefficients c_k that maximize (8).

The polynomials. To apply the method of auxiliary functions, one needs to choose the polynomials Q_k in (8). There are heuristic rules to select them:

- They should have positive roots.
- They should have *small* coefficients.
- They should have *small* trace. The reason for this is the following: to prove that $M_1(\alpha) < c$, all polynomials of degree d whose trace is smaller than $c \cdot d$ must appear in (8).

For small positive integers d and T, it is possible to give a complete list of all monic irreducible polynomials with integer coefficients, positive roots, degree d and trace T. In [20] a complete list of such $Q \in \mathbb{Z}[x]$ with

$$\mathrm{Trace}(Q) - \deg(Q) \leq 6$$

is given, and all $Q \in \mathbb{Z}[x]$ with $\deg(Q) = 10$ and $\mathrm{Trace}(Q) = 18$ are listed in [13]. Table 1 gives for each $1 \leq d \leq 10$ the smallest possible trace T of a totally positive algebraic integer of degree d, the corresponding value of M_1, and the number N_d of monic irreducible polynomials with positive roots having such degree and trace. Some of them appear in Table 2.

TABLE 1. Number of polynomials of a given degree and trace as small as possible

d	T	M_1	N_d
1	1	1.000	1
2	3	1.500	1
3	5	1.660	1
4	7	1.750	2
5	9	1.800	4
6	11	1.833	11
7	13	1.857	40
8	15	1.875	151
9	17	1.889	686
10	18	1.800	3

Smyth's theorem is used by O. Debarre in [7] to prove a result on curves on simple abelian varieties. He also conjectures that if $\alpha \in \mathbb{A}_+$ is of degree d, then $\mathrm{Trace}(\alpha) \geq 2\,d - 1$, and if equality holds, then $\mathrm{Norm}(\alpha) = 1$. The first

part of the conjecture is false, since by Corollary 3 in [14], for infinitely many d there exists $\alpha \in \mathbb{A}_+$ with

$$\deg(\alpha) = d \quad \text{and} \quad \operatorname{Trace}(d) \le 2\,d - \frac{1}{4}\,\frac{\log\log d}{\log\log\log d}\,.$$

The smallest d such that there exists $\alpha \in \mathbb{A}_+$ of degree d and

$$\operatorname{Trace}(\alpha) < 2\,d - 1$$

is $d = 10$. The second part of the conjecture does not hold either, as is shown by the polynomial

$$x^8 - 15\,x^7 + 89\,x^6 - 268\,x^5 + 438\,x^4 - 385\,x^3 + 169\,x^2 - 32\,x + 2.$$

The optimization algorithm. Once the polynomials Q_k have been chosen, it remains to find the coefficients c_k that maximize (8). This can be done by semi-infinite linear programing, as in [19], or by a variant of the second Remes algorithm, as in [1].

Latest results. New polynomials, better optimization algorithms and more powerful computers have produced a series of improvements in the trace problem:

- $\mathcal{K} > 1.7735$ (1997, Flammang, Grandcolas & Rhin [8]),
- $\mathcal{K} > 1.7783$ (2004, McKee & Smyth [13]),
- $\mathcal{K} > 1.7800$ (2006, Aguirre, Bilbao & Peral [1]),
- $\mathcal{K} > 1.7822$ (2006, Flammang, personal communication to C. Smyth),
- $\mathcal{K} > 1.7836$ (2006, Aguirre & Peral [2]).

The best current result as far as we know* is $\mathcal{K} > 1.784109$ and is due to the authors. It is included in Appendix A.

Considering for $\xi > 0$ the optimization problem

$$\sup\Big\{\min_{x>\xi}\Big(x - \sum_{k=1}^{N} c_k \log|Q_k(x)|\Big)\Big\} \tag{9}$$

instead of (8), it is possible to obtain a different type of inequality for the trace of $\alpha \in \mathbb{A}_+$ with conjugates $\alpha_1 < \alpha_2 < \cdots < \alpha_d$:

- $M_1(\alpha) > 1.60 + \alpha_1$ (1997, Flammang, Rhin & Smyth [9]),
- $M_1(\alpha) > 1.66 + \alpha_1$ (2006, Aguirre, Bilbao & Peral [1]).

These inequalities hold for all $\alpha \in \mathbb{A}_+$ except for 26 explicit exceptions and their integer translates.

*Added in proof: V. Flammang has proved recently that $\mathcal{K} > 1.78702$.

The limits of the method. How far is it possible to go with the method of auxiliary functions? Is it possible to solve the trace problem? Unfortunately the answer is no.

C. Smyth proved in [21] that $\mathcal{K} < 2 - 10^{-41}$. This was then improved by J.-P. Serre in a private letter (24 February 1998) to Smyth, whose contents appear as Appendix B. Serre proves that if Q is a polynomial with *real* coefficients with leading and constant coefficients of modulus at least 1, and if $y > 0$, $z > 0$, $c \in \mathbb{R}$ are constants such that

$$x - z \log x - y \log |Q(x)| \geq c \qquad \text{for all } x > 0, \tag{10}$$

then $c \leq 1.898302\ldots$. It follows that

$$\mathcal{K} \leq 1.898302\ldots. \tag{11}$$

Since Serre's result is for polynomials with real coefficients, it is possible that the inequality is in fact strict. We see from (11) that it is impossible to show using the method of auxiliary functions that $(1, c) \cap \mathcal{T}_1$ is finite for any $c \geq 1.898302\ldots$. Moreover, to prove for instance that $(1, 1.89) \cap \mathcal{T}_1$ is finite, the sum in (8) should include all the polynomials referred to in Table 1. We believe that the computational problem is intractable, and will remain so for a long time.

In a subsequent letter (31 March 1998) Serre proved that the upper bound for c is optimal. For any $c < 1.898302\ldots$ there exist constants $y > 0$, $z > 0$, and a polynomial

$$Q(x) = \prod_{k=1}^{n} (x - \lambda_k), \quad \lambda_k \in [a, b], \quad \prod_{k=1}^{n} \lambda_k \geq 1,$$

where $a = 0.08735\ldots$, $b = 4.41107\ldots$, such that (10) holds.

For optimal c, the corresponding values of y and z are $y = 1.628472\ldots$ and $z = 0.620741\ldots$. The extremal situation is described by a measure, giving the limiting density function of the zeroes of a sequence of real polynomials Q_n whose degrees go to infinity with n. This measure has support on the interval $[a, b]$, and is obtained by projecting the uniform probability measure on the unit circle to $[a, b]$. The result is that, with this optimal choice,

$$f_{\text{opt}}(x) = x - z \log x - \int_a^b \log |x - y| \, \frac{\sqrt{(y - a)(b - y)}}{\pi y} \, dy.$$

This function is constant on $[a, b]$, equal to $1.898302\ldots$, and increases to infinity both as $x \to 0$ and $x \to \infty$. See Figure 1, where f_{opt} is compared with the auxiliary function of Appendix A.

Serre's interest in the problem comes from its connection with the counting of points on curves over finite fields. For a curve $\mathcal{C}$ of genus g over a finite field $\mathbb{F}_q$, the number of points of $\mathcal{C}$ in $\mathbb{F}_q$ is given by Weil as $q + 1 - \text{trace}(P)$, where P is a monic integer polynomial of degree g having all its roots in the interval $[-2\sqrt{q}, 2\sqrt{q}]$. The roots of P are of the form $\pi + \bar{\pi}$, where the π, of