THEORY OF COMPUTING, Volume 9 (10), 2013, pp. 403–411
www.theoryofcomputing.org

On the Real τ-Conjecture and the Distribution of Complex Roots*

Pavel Hrubeš

Received December 4, 2012; Revised April 11, 2013; Published May 21, 2013

Abstract: Koiran's real τ-conjecture asserts that if a non-zero real polynomial can be written as $f = \sum_{i=1}^{p} \prod_{j=1}^{q} f_{ij}$, where each f_{ij} contains at most k monomials, then the number of distinct real roots of f is polynomially bounded in pqk. We show that the conjecture implies quite a strong property of the complex roots of f: their arguments are uniformly distributed except for an error which is polynomially bounded in pqk. That is, if the conjecture is true, f has degree n and $f(0) \neq 0$, then for every $0 < \alpha - \beta < 2\pi$

$$\left| N_{\alpha,\beta}(f) - \frac{(\alpha-\beta)}{2\pi} n \right| \leq (pqk)^c ,$$

where c is an absolute constant and $N_{\alpha,\beta}(f)$ is the number of roots of f of the form $re^{i\phi}$, with $r > 0$ and $\beta < \phi < \alpha$, counted with multiplicities. In particular, if the real τ-conjecture is true, it is also true when multiplicities of non-zero real roots are included.

ACM Classification: F.1.m

AMS Classification: 03D15, 68Q17

Key words and phrases: arithmetic circuits, lower bounds, roots

1 Introduction

The Shub-Smale τ-conjecture [11, 12] is a conjecture in arithmetic circuit complexity, asserting that a polynomial which is computable by a small arithmetic circuit has a small number of integer roots. If true, it gives a lower bound on the circuit complexity of the permanent polynomial [1]. One drawback

*A preliminary version of this paper appeared in ECCC 2012/121.

DOI: 10.4086/toc.2013.v009a010

of the conjecture is that, by referring to *integer* roots, it leads one to the area of number theory which is notorious for its hard problems. It would be desirable to have a hypothesis relating circuit complexity and the number of real, or even complex, roots. Such a conjecture was put forward by Koiran [6], who calls it the "real τ-conjecture." Since τ-conjecture is false when we merely replace "integer root" by "real root", the real τ-conjecture counts the number of real roots of a polynomial computed by a restricted circuit. As shown by Koiran, it nevertheless gives lower bounds for general circuits.[1]

The real τ-conjecture can be stated without reference to circuits or computation. Let us call a real (or later complex) polynomial $\left(\sum_{i=0}^{n} a_i x^i\right)$ *k-sparse* if at most k of the coefficients $a_0,\ldots,a_n$ are non-zero. Let f be a polynomial of the form

$$f=\sum_{i=1}^{p}\prod_{j=1}^{q} f_{ij}\,,\ \text{where each } f_{ij} \text{ is } k\text{-sparse}\ . \tag{1.1}$$

Conjecture 1.1 (The real τ-conjecture). *Let f be a non-zero polynomial as in (1.1) with every $f_{ij}\in\mathbb{R}[x]$. Then the number of distinct real roots of f is at most $(pqk)^c$, where c is an absolute constant.*

Apart from the absence of a counterexample, the conjecture's motivation is the following corollary of Descartes' rule of signs:

Theorem 1.2 (Weak rule of signs). *A non-zero k-sparse polynomial has at most $k-1$ positive real roots.*

In particular, Conjecture 1.1 is true if $p=1$ and, in general, f has at most $O(pk^q)$ real roots. A remarkable aspect of the weak rule of signs is that the number of real roots can be bounded by the number of terms of a polynomial, rather than the degree. This suggests that in the real setting, sparsity of a polynomial has a role similar to the notion of degree in the complex setting. Indeed, this analogy was developed by Khovanskii in his theory of fewnomials [5]. Most notably, he gives a real version of Bezout's theorem where the number of solutions of a system of polynomial equations is bounded by a function of the number of terms in the equations (and the number of equations). It is an intriguing question whether the quantitative bounds Khovanskii obtains are asymptotically tight and hence how far can the analogy between degree and the number of terms be pushed. In this perspective, the real τ-conjecture is an interesting question from a purely mathematical point of view.

It is the author's conviction that if the real τ-conjecture is true, it is true by virtue of some deeper phenomenon pertaining to the structure of complex roots. This is because complex roots give a complete description of a polynomial (up to a multiplicative factor), and complex analysis provides a more powerful perspective of the world of the reals. Certainly, the real τ-conjecture as stated above has a rather arbitrary feeling about it. As an extension of the weak rule of signs, it could apparently state much more. The rule holds also when *multiplicities* of non-zero real roots are included. Moreover, it implies that the multiplicity of every non-zero *complex* root is at most $k-1$, and the rule is also valid when we consider polynomials with complex coefficients. In a less direct manner, it can be shown (see [8, 4]) that the rule applies also to the number of complex roots lying close to the real axis.

An interesting generalisation of the weak rule of signs, which subsumes the above observations, is the following. Let α,β be real numbers such that $0<\alpha-\beta<2\pi$, and let f be a complex polynomial. Denote $N_{\alpha,\beta}(f)$ the number of complex roots lying in the sector defined by the angles α,β: i. e., let

[1] That is, *constant-free* circuits of unbounded depth.

$$\begin{aligned} S(\alpha,\beta) &:= \{re^{\imath\phi} \in \mathbb{C} : r > 0 \text{ and } \beta < \phi < \alpha\} \\ N_{\alpha,\beta}(f) &:= \text{the number of roots of } f \text{ in } S(\alpha,\beta) \text{ counted with multiplicities.} \end{aligned}$$

Hayman [3] (see also Proposition 11.2.4 in [9]) proves the following theorem:

Theorem 1.3 (Hayman)**.** *Let f be a complex k-sparse polynomial of degree n with $f(0) \neq 0$. Then for every* $0 < \alpha - \beta < 2\pi$

$$\left| N_{\alpha,\beta}(f) - \frac{\alpha-\beta}{2\pi} n \right| \leq k - 1\,.$$

The term $(\alpha-\beta)n/(2\pi)$ denotes the number of roots in the sector $S(\alpha,\beta)$, assuming the arguments of the roots are distributed uniformly. So the theorem says that the angles of roots of f are distributed uniformly except for an error which depends linearly on the number of terms of f. The motivating example is of course $f = x^n - 1$, where the roots are perfectly spread on the unit circle. Theorem 1.3 gives, for example, that every sector with $\alpha - \beta > 2\pi(k-1)/n$ contains a root of f. Also, one obtains the weak rule of signs by letting $\alpha \to 0_+, \beta \to 0_-$. One can compare Hayman's theorem with the Erdös-Turán theorem [2] which estimates the distribution of roots in terms of the sizes of coefficients of f, rather than their number.

In this note, we apparently strengthen Conjecture 1.1 so that, instead of counting the number of real roots, we measure the discrepancy from uniformity á la Theorem 1.3. This is done only to show that the two versions of the conjecture are actually equivalent. That is, if the real τ-conjecture is true then the arguments of the complex roots of a polynomial f are uniformly distributed with an error polynomial in pqk. In particular, if the conjecture is true, it is also true when the multiplicities of the non-zero roots are included.

Of course, the real τ-conjecture may turn out to be false. This note can also be used to extend the sphere of possible counterexamples. In order to disprove Conjecture 1.1, it is now enough to construct a polynomial f which can be succinctly written as (1.1) but whose roots lie in the negative half-plane; or to construct such an f which has a complex root with multiplicity superpolynomial in pqk—perhaps already $(x+1)^n$ is a good candidate.

2 Modifications of the conjecture

An apparent detail is whether Conjecture 1.1 should refer to the number of distinct roots, or to the number of non-zero roots including their multiplicities. Arguments can be made in both directions. The original Shub-Smale conjecture is inevitably about the number of distinct integer roots, and this suggests to also exclude multiplicities in Conjecture 1.1. Several applications of Khovanskii's theory require counting distinct roots—let us mention Risler's theorem [10], which relates the number of real roots of a polynomial and the number of addition gates needed to compute it. Koiran himself seems to believe that it is important to exclude multiplicities: in [7], Koiran et al. consider polynomials of the form

$$f = \sum_{i=1}^{p} \prod_{j=1}^{q} f_{ij}^{n_{ij}}\,.$$

They give an upper-bound on the number of real roots of f which is independent on the exponents n_{ij}. They call it a "step towards the real τ-conjecture," which clearly assumes that multiplicities are ignored. On the other hand, we note in Observation 3.4 that if the polynomial $(x+1)^n$ can be written as (1.1) with small pqk then Conjecture 1.1 is false. This suggests that multiplicities of non-zero roots cannot be neglected and that counting roots with multiplicities is indeed the correct way of counting:

Conjecture 2.1. *Let f be a non-zero polynomial as in (1.1) with every $f_{ij} \in \mathbb{R}[x]$. Then the number of non-zero real roots of f,* counted with multiplicities*, is at most $(pqk)^c$, where c is an absolute constant.*

Another detail is whether it is important for the polynomial f in Conjecture 1.1 to be real. This will be addressed in Corollary 2.5 where it is shown that we can allow the f_{ij}'s to have complex coefficients. Finally, inspired by the generalisation of the weak rule of signs given in Theorem 1.3, let us consider the following:

Conjecture 2.2. *Let f be a polynomial as in (1.1) with every $f_{ij} \in \mathbb{C}[x]$. Assume that f has degree n and $f(0) \neq 0$. Then for every $0 < \alpha - \beta < 2\pi$,*

$$\left| N_{\alpha,\beta}(f) - \frac{(\alpha-\beta)}{2\pi} n \right| \leq (pqk)^c ,$$

where c is an absolute constant.

The assumption $f(0) \neq 0$ is necessary in order to avoid zero roots. If $f(0) = 0$ and zero is a root of multiplicity m, Conjecture 2.2 implies

$$\left| N_{\alpha,\beta}(f) - \frac{(\alpha-\beta)}{2\pi} (n-m) \right| \leq O((pqk)^c)$$

This is shown by considering the polynomial $f+\varepsilon$ for a small enough ε. The $n-m$ non-zero roots of f change only slightly, whereas the zero root of f splits into m distinct roots of $f+\varepsilon$ which are almost uniformly distributed around a circle of radius $O(\varepsilon^{1/m})$.

Each Conjecture 1.1, 2.1 and 2.2 seems to be strictly stronger than the previous one. However, we show that this is in fact not the case:

Theorem 2.3. *Conjectures 1.1, 2.1 and 2.2 are equivalent.*

This allows one to formulate the following consequences of the real τ-conjecture. Each of them can be potentially used to construct a counterexample.

Corollary 2.4. *Assume Conjecture 1.1. Let f be a complex polynomial as in (1.1) with $s := pqk$. Then*

1. *the multiplicity of every non-zero root of f is polynomial in s;*
2. *if the real part of every root of f is negative (such an f is called* Hurwitz polynomial*) then $s = \Omega(n^c)$, for a constant $c > 0$.*

Corollary 2.5. *If Conjecture 1.1 is true then both Conjecture 1.1 and 2.1 are true even when we allow the f_{ij}'s in (1.1) to be complex (while still counting real roots).*

Proof of Corollary 2.4 and 2.5. Let f be as in (1.1) with $f_{ij} \in \mathbb{C}[x]$. Let $s := pqk$ and n be the degree of f. By Theorem 2.3, we can replace Conjecture 1.1 by Conjecture 2.2, and we will assume the latter.

If $re^{\imath\phi}, r > 0$, is a root of f with multiplicity m, consider the sector $S = S(\phi + \pi/n, \phi - \pi/n)$. Assuming $f(0) \neq 0$, Conjecture 2.2 implies that the number of roots in S is at most $s^c + 1$ and so $m \leq s^c + 1$ (we count all roots with their multiplicities). If $f(0) = 0$, take the polynomial $f + \varepsilon$ for a small ε. The roots vary continuously with ε and S is an open set, hence $f + \varepsilon$ has at least as many roots in S as f does. $f + \varepsilon$ is of the form $\sum_{i=1}^{p'} \prod_{j=1}^{q} f_{ij}$ where $p' = p + 1$ and the f_{ij}'s are k-sparse. Conjecture 2.2 gives that the number of roots of $f + \varepsilon$ in S is at most $(p'qk)^c + 1 \leq (2s)^c + 1$ and so $m \leq (2s)^c + 1$.

If f is a Hurwitz polynomial then $N_{3\pi/2,\pi/2}(f) = n$ and Conjecture 2.2 gives that $n/2 \leq s^c$.

For Corollary 2.5, it is enough to show that the number of non-zero real roots of f is bounded by a polynomial in s. Consider the two sectors $S(\alpha, -\alpha)$ and $S(\pi + \alpha, \pi - \alpha)$ with $\alpha = \pi/n$. If $f(0) \neq 0$, Conjecture 2.2 gives that the number of roots in each sector is at most $s^c + 1$. If $f(0) = 0$, take the polynomial $f + \varepsilon$ as above. $\square$

3 Proof of Theorem 2.3

The proof has two simple parts. The first, Proposition 3.1, is a general statement about angular distribution of roots. The second, Proposition 3.3, is a property of depth-three arithmetic circuits which allows to efficiently compute the real part of a complex polynomial f, provided f itself can be so computed.

For a complex polynomial $f = \sum_{i=0}^{n} a_i x^i$, let

$$\Re(f) = \sum_{i=0}^{n} \Re(a_i) x^i \, , \; \Im(f) = \sum_{i=0}^{n} \Im(a_i) x^i \, ,$$

where $\Re(a)$, $\Im(a)$ are the real and the imaginary part of the complex number a, respectively. If $\Re(a_0) \neq 0$ and $\alpha \in \mathbb{R}$, let $M_\alpha(f)$ be the number of distinct positive roots of the real polynomial $f_\alpha(x) := \Re(f(xe^{\imath\alpha}))$. Furthermore, let

$$M(f) := \max_{\alpha \in [0,2\pi)} M_\alpha(f) \, .$$

Proposition 3.1. *Let f be a complex polynomial of degree n with $\Re(f(0)) \neq 0$. Then for every $0 < \alpha - \beta < 2\pi$*

$$\left| N_{\alpha,\beta}(f) - \frac{(\alpha - \beta)}{2\pi} n \right| \leq M(f) + 1/2 \, .$$

Proof. This follows from Theorem 11.2.1 in [9] where the quantity $N_{\alpha,\beta}(f)$ is determined exactly. The regularity assumption of the Theorem can always be guaranteed by considering $S(\alpha', \beta')$ with α', β' ε-close to α, β. $\square$

The proof of Theorem 11.2.1 in [9] relies chiefly on the argument principle, which relates the number of roots of f inside a domain with the behavior of f on its boundary. For the sake of a reader who is either curious, or does not want to look for [9], let us give a sketch of an elementary proof of Proposition 3.1. Consider the family of polynomials $f + \imath t$, where $t \geq 0$ is a real parameter. The main point is that the n complex roots of $f + \imath t$ depend continuously on t. If t is sufficiently large, $f + \imath t$ has n distinct roots which are almost completely uniformly distributed around the circle with radius $O(t^{1/n})$. Hence the sector $S(\alpha,\beta)$ contains $(\alpha-\beta)n/2\pi + c$ roots, with $|c|<1$. As t decreases, the only way how the number of roots in $S(\alpha,\beta)$ can change, is that the roots pass through the boundary of the sector. Hence one must estimate the number of roots of the form $x = re^{\imath\phi}$, with $r > 0$ and $\phi \in \{\alpha,\beta\}$, which are roots of $f+\imath t$ for some $t \geq 0$. If $re^{\imath\phi}$ is a root of $f(x)+\imath t$ then r is a root of $\Re(f(xe^{\imath\phi})+\imath t)$. However, $\Re(f(xe^{\imath\phi})+\imath t) = \Re(f(xe^{\imath\phi}))$ does not depend on t and has $M_\phi(f)$ positive roots. In addition, considering the imaginary part gives $\Im(f(re^{\imath\phi}))+t = 0$ and t is uniquely determined by r. So we have reached

$$\left|N_{\alpha,\beta}(f) - \frac{(\alpha-\beta)}{2\pi}n\right| \leq M_\alpha(f) + M_\beta(f) + 1 \leq 2M(f)+1\,.$$

There are few details to correct. First, since $M_\alpha(f)$ counts distinct roots, one should better assume that neither f_α nor f_β have multiple real roots—but this can always be achieved by changing α,β by a small ε. Second, we have missed the bound of Proposition 3.1 by a factor of two—which can be improved by considering the direction in which the roots pass through the boundary of the sector.

For the purpose of the following lemma, we extend the definition of $\Re(f)$ to the case when f is a multivariate complex polynomial, in the obvious way.

Lemma 3.2.

$$\Re\Big(\prod_{i=1}^{n}(x_i+\imath y_i)\Big) = \sum_{j=1}^{n+1} b_j \prod_{i=1}^{n}(x_i + a_j y_i)\,,$$

where the a_j, b_j are some real constants.

Proof. This is a standard interpolation argument. Introduce a new variable z and consider the polynomial $f(z) = \prod_{i=1}^{n}(x_i + zy_i))$, which is now a real polynomial in $2n+1$ variables. Then

$$f(z) = f_0 + f_1 z + \cdots + f_n z^n\,,$$

where the polynomials f_i do not depend on z. Choosing $n+1$ distinct real numbers $a_1,\ldots,a_{n+1}$, we obtain

$$f(a_i) = f_0 + f_1 a_i + \cdots + f_n a_i^n\,,\, i \in \{1,\ldots,n+1\}\,,$$

which can be written as

$$(f(a_1),\ldots,f(a_{n+1}))^t = V(a_1,\ldots,a_{n+1})\cdot(f_0,\ldots,f_n)^t\,,$$

where $V(a_1,\ldots,a_{n+1})$ is $(n+1)\times(n+1)$ Vandermonde matrix. The matrix is invertible and hence the polynomials $f_0,\ldots,f_n$ are real linear combinations of the polynomials $f(a_1)\ldots f(a_{n+1})$. Finally,

$$\Re(\prod_{i=1}^{n}(x_i+\imath y_i)) = \sum_{2j\in\{0,\ldots,n\}} (-1)^j f_{2j}$$

and so $\Re(\prod_{i=1}^{n}(x_i+\imath y_i)) = b_1 f(a_1) + \cdots + b_{n+1} f(a_{n+1})$ for some $b_1,\ldots,b_{n+1} \in \mathbb{R}$. □

Proposition 3.3. *Let $f = \sum_{i=1}^{p} \prod_{j=1}^{q} f_{ij}$ where each f_{ij} is a complex k-sparse polynomial. Then*

$$\Re(f) = \sum_{i=1}^{p(q+1)} \prod_{j=1}^{q} g_{ij}\,,$$

where each g_{ij} is a real k-sparse polynomial.

Proof. Write

$$\Re(f) = \sum_{i=1}^{p} \Re\Big(\prod_{j=1}^{q} (\Re(f_{ij}) + \imath \cdot \Im(f_{ij}))\Big)$$

and apply the previous lemma to $\Re\big(\prod_{j=1}^{q} (\Re(f_{ij}) + \imath \cdot \Im(f_{ij}))\big)$ for each $i \in \{1, \dots, p\}$. Note that if f_{ij} is complex k-sparse then $a \cdot \Re(f_{ij}) + b \cdot \Im(f_{ij})$ is real k-sparse for any $a, b \in \mathbb{R}$. $\square$

Let us note that Proposition 3.3 by itself implies:

Observation 3.4. Assume that $f(x) = (x+1)^n$ can be written as $\sum_{i=1}^{p} \prod_{j=1}^{q} f_{ij}$ where f_{ij} are complex k-sparse polynomials. If Conjecture 1.1 is true then $pqk = \Omega(n^c)$ for some $c > 0$.

In order to see this, consider the complex polynomial

$$f(\imath x) + f(-\imath x) = (\imath x + 1)^n + (-\imath x + 1)^n\,.$$

Its degree is either n, if n is even, or $n-1$, if it is odd. The roots are of the form

$$\imath \frac{1-\omega}{1+\omega}\,,$$

where ω is an n-th root of -1 with $\omega \neq -1$. There are again either n or $n-1$ such roots, depending on the parity of n, and they are all distinct. Furthermore, since $|\omega| = 1$,

$$\imath \frac{1-\omega}{1+\omega} = \imath \frac{(1-\omega)(1+\overline{\omega})}{|1+\omega|^2} = \imath \frac{1 - |\omega|^2 + \overline{\omega} - \omega}{|1+\omega|^2} = \imath \frac{\overline{\omega} - \omega}{|1+\omega|^2} = \frac{2\Im(\omega)}{|1+\omega|^2}$$

is real. The roots of $f(\imath x) + f(-\imath x)$ must also be the roots of the non-zero real polynomial $\Re(f(\imath x) + f(-\imath x))$. Conjecture 1.1 in conjunction with Proposition 3.3 then implies that $n = O((pqk)^{c'})$ for some constant $c' > 0$.

Proof of Theorem 2.3. Clearly, Conjecture 2.1 implies Conjecture 1.1. That Conjecture 2.2 implies Conjecture 2.1 was explained in the proof of Corollary 2.5.

It remains to prove Conjecture 2.2 assuming Conjecture 1.1. Let f be a complex polynomial as in Conjecture 2.2. We have $f(0) \neq 0$ and we can also assume that $\Re(f(0)) \neq 0$ – otherwise multiply f by $\imath$. By Proposition 3.1, we have

$$\Big|N_{\alpha,\beta}(f) - \frac{(\alpha-\beta)}{2\pi} n\Big| \leq M(f) + 1/2\,,$$

where $M(f)$ is the maximum number of distinct positive roots of $\Re(f(xe^{i\phi}))$, for $\phi \in [0, 2\pi)$. Proposition 3.3 gives that for a fixed ϕ

$$\Re(f(xe^{i\phi})) = \sum_{i=1}^{p'} \prod_{j=1}^{q} g_{ij}\,,$$

where all of g_{ij} are real k-sparse and $p' = p(q+1)$. Conjecture 1.1 then implies that the number of positive roots of $\Re(f(xe^{i\phi}))$ is polynomial in $p'qk = O((pqk)^2)$ and so Conjecture 2.2 follows by taking c large enough. □

4 A comment about the proof

The proof of Theorem 2.3 relies mainly on the fact that if a complex polynomial f can be succinctly represented as (1.1) then so can $\Re(f)$, and the theorem will go through for any computational model with this property. For example, consider the following strengthening of the real τ-conjecture:

Conjecture 4.1. *Let $A(x_1,\dots,x_n)$ be an arithmetic formula of size s over $\mathbb{R}$. Let $f \in \mathbb{R}[x]$ be the polynomial computed by $A(x^{k_1},\dots,x^{k_n})$ where $k_1,\dots,k_n$ are some natural numbers. If f is non-zero then the number of distinct real roots of f is at most s^c, for some constant c.*

The author is not aware of a counterexample to this statement. As in Theorem 2.3, one can show:

Theorem 4.2. *Let f be as above but with A allowed to use complex numbers. Assume that $f(0) \neq 0$ and f has degree n. If Conjecture 4.1 is true then for every $0 < \alpha - \beta < 2\pi$,*

$$\left| N_{\alpha,\beta}(f) - \frac{(\alpha-\beta)}{2\pi} n \right| \leq s^c\,,$$

with an absolute constant c.

References

[1] PETER BÜRGISSER: On defining integers and proving arithmetic circuit lower bounds. *Comput. Complexity*, 18(1):81–103, 2009. Preliminary version in STACS'07. [doi:10.1007/s00037-009-0260-x] 403

[2] PAUL ERDŐS AND PÁL TURÁN: On the distribution of roots of polynomials. *Ann. of Math.*, 51(1):105–119, 1950. JSTOR. 405

[3] WALTER K. HAYMAN: Angular value distribution of power series with gaps. *Proc. London Mathematical Society*, s3-24(4):590–624, 1972. [doi:10.1112/plms/s3-24.4.590] 405

[4] AUBREY J. KEMPNER: On the complex roots of algebraic equations. *Bull. Amer. Math. Soc.*, 41(12):809–843, 1935. [doi:10.1090/S0002-9904-1935-06201-9] 404

[5] ASKOLD G. KHOVANSKII: *Fewnomials*. Volume 88 of *Translations of Mathematical Monographs*. Amer. Math. Soc., 1991. 404

[6] PASCAL KOIRAN: Shallow circuits with high-powered inputs. In *Proc. 2nd Symp. Innovations in Computer Science (ICS'11)*, pp. 309–320. Tsinghua University Press, 2011. ICS'11. 404

[7] PASCAL KOIRAN, NATACHA PORTIER, AND SÉBASTIEN TAVENAS: A Wronskian approach to the real τ-conjecture. Preprint, 2012. [arXiv:1205.1015] 405

[8] NIKOLA OBRESCHKOFF: Über die Wurzeln algebraischer Gleichungen. *Jahresbericht der Deutschen Mathematiker-Vereinigung*, 33:52–64, 1925. DigiZeitschriften. 404

[9] QAZI I. RAHMAN AND GERHARD SCHMEISSER: *Analytic Theory of Polynomials*. Oxford Univ. Press, 2002. 405, 407

[10] JEAN-JACQUES RISLER: Additive complexity and zeros of real polynomials. *SIAM J. Comput.*, 14(1):178–183, 1985. [doi:10.1137/0214014] 405

[11] MICHAEL SHUB AND STEVE SMALE: On the intractability of Hilbert's Nullstellensatz and an algebraic version of "$NP \neq P$?". *Duke Mathematical Journal*, 81(1):47–54, 1995. [doi:10.1215/S0012-7094-95-08105-8] 403

[12] STEVE SMALE: Mathematical problems for the next century. *The Mathematical Intelligencer*, 20(2):7–15, 1998. [doi:10.1007/BF03025291] 403

AUTHOR

Pavel Hrubeš
postdoctoral fellow
University of Washington, Seattle, WA
pahrubes@gmail.com

ABOUT THE AUTHOR

PAVEL HRUBEŠ graduated from Charles University in Prague in 2008, and he has been touring the world ever since. His supervisor was Pavel Pudlák. He is interested in computational complexity and logic.