

## ON THE COMPLEXITY OF NUMERICAL ANALYSIS\*

ERIC ALLENDER<sup>†</sup>, PETER BÜRGISSE<sup>‡</sup>, JOHAN KJELDGAARD-PEDERSEN<sup>§</sup>, AND  
PETER BRO MILTERSEN<sup>¶</sup>

**Abstract.** We study two quite different approaches to understanding the complexity of fundamental problems in numerical analysis: (a) the Blum–Shub–Smale model of computation over the reals; and (b) a problem we call the “generic task of numerical computation,” which captures an aspect of doing numerical computation in floating point, similar to the “long exponent model” that has been studied in the numerical computing community. We show that both of these approaches hinge on the question of understanding the complexity of the following problem, which we call PosSLP: Given a division-free straight-line program producing an integer  $N$ , decide whether  $N > 0$ . In the Blum–Shub–Smale model, polynomial-time computation over the reals (on discrete inputs) is polynomial-time equivalent to PosSLP when there are only algebraic constants. We conjecture that using transcendental constants provides no additional power, beyond *nonuniform* reductions to PosSLP, and we present some preliminary results supporting this conjecture. The generic task of numerical computation is also polynomial-time equivalent to PosSLP. We prove that PosSLP lies in the counting hierarchy. Combining this with work of Tiwari, we obtain that the Euclidean traveling salesman problem lies in the counting hierarchy—the previous best upper bound for this important problem (in terms of classical complexity classes) being PSPACE. In the course of developing the context for our results on arithmetic circuits, we present some new observations on the complexity of the arithmetic circuit identity testing (ACIT) problem. In particular, we show that if  $n!$  is not ultimately easy, then ACIT has subexponential complexity.

**Key words.** Blum–Shub–Smale model, arithmetic circuits, counting hierarchy, BPP, sum of square roots problem, straight-line programs

**AMS subject classifications.** 68Q15, 68Q17

**DOI.** 10.1137/070697926

**1. Introduction.** The original motivation for this paper comes from a desire to understand the complexity of computation over the reals in the Blum–Shub–Smale model. In section 1.1 we give a brief introduction to this model, and we introduce the problem PosSLP and explain its importance in understanding the Blum–Shub–Smale model.

In section 1.2 we present yet another reason to be interested in PosSLP. We isolate a computational problem that lies at the root of the task of designing numerically stable algorithms. We show that this task is computationally equivalent to PosSLP. The material in sections 1.1 and 1.2 provides motivation for studying PosSLP and for attempting to place it within the framework of traditional complexity classes.

In section 1.3 we discuss our main technical contributions: proving upper and

\*Received by the editors July 23, 2007; accepted for publication (in revised form) September 5, 2008; published electronically January 14, 2009.

<http://www.siam.org/journals/sicomp/38-5/69792.html>

<sup>†</sup>Department of Computer Science, Rutgers University, Piscataway, NJ 08854-8019 (allender@cs.rutgers.edu). The first author’s work was supported by NSF grants CCF-0514155, CCF-0830133, and CCF-0832787.

<sup>‡</sup>Institute of Mathematics, Paderborn University, DE-33095 Paderborn, Germany (pbuerg@upb.de). This author’s research was supported by DFG grant BU 1371.

<sup>§</sup>Decision Sciences Practice, PA Consulting Group, Tuborg Blvd. 5, DK 2900 Hellerup, Denmark (johan.kjeldgaard-pedersen@paconsulting.com).

<sup>¶</sup>Department of Computer Science, University of Aarhus, IT-parken, DK 8200 Aarhus N, Denmark (bromille@cs.au.dk). This author’s research was supported by SNF grants 21-04-0551 and 272-07-0440 and by the Center for Algorithmic Game Theory, funded by the Carlsberg Foundation.

lower bounds on the complexity of PosSLP. In section 1.4 we present applications of our main result with respect to the Euclidean traveling salesman problem and the sum-of-square-roots problem.

**1.1. Polynomial time over the reals.** The Blum–Shub–Smale model of computation over the reals provides a very well-studied complexity-theoretic setting in which to study the computational problems of numerical analysis. We refer the reader to Blum et al. [12] for detailed definitions and background material related to this model; here, we will recall only a few salient facts. In the Blum–Shub–Smale model, each machine computing over the reals has associated with it a finite set  $S$  of real *machine constants*. The inputs to a machine are elements of  $\bigcup_n \mathbb{R}^n = \mathbb{R}^\infty$ , and thus each polynomial-time machine over  $\mathbb{R}$  accepts a “decision problem”  $L \subseteq \mathbb{R}^\infty$ . The set of decision problems accepted by polynomial-time machines over  $\mathbb{R}$  using only constants from  $S \cup \{0, 1\}$  is denoted  $P_{\mathbb{R}}^S$ . The union of the classes  $P_{\mathbb{R}}^S$  over all  $S$  is called *polynomial time over  $\mathbb{R}$*  and is denoted  $P_{\mathbb{R}}$ . The subclass  $P_{\mathbb{R}}^0$  of “constant-free polynomial time” is commonly denoted by  $P_{\mathbb{R}}^0$ ; cf. Bürgisser and Cucker [20].

There has been considerable interest in relating computation over  $\mathbb{R}$  to the classical Boolean complexity classes such as  $P$ ,  $NP$ ,  $PSPACE$ , etc. This is accomplished by considering the *Boolean part* of decision problems over the reals. That is, given a problem  $L \subseteq \mathbb{R}^\infty$ , the Boolean part of  $L$  is defined as  $BP(L) := L \cap \{0, 1\}^\infty$ . (Here, we follow the notation of [12];  $\{0, 1\}^\infty = \bigcup_n \{0, 1\}^n$ , which is identical to  $\{0, 1\}^*$ .) The Boolean part of  $P_{\mathbb{R}}$ , denoted  $BP(P_{\mathbb{R}})$ , is defined as  $\{BP(L) \mid L \in P_{\mathbb{R}}\}$ .

By encoding the advice function in a single real constant as in Koiran [44], one can show that  $P/\text{poly} \subseteq BP(P_{\mathbb{R}})$ . The best upper bound on the complexity of problems in  $BP(P_{\mathbb{R}})$  that is currently known was obtained by Cucker and Grigoriev [27]:

$$(1.1) \quad BP(P_{\mathbb{R}}) \subseteq PSPACE/\text{poly}.$$

There has been *no* work pointing to lower bounds on the complexity of  $BP(P_{\mathbb{R}})$ ; nobody has presented any compelling evidence that  $BP(P_{\mathbb{R}})$  is not equal to  $P/\text{poly}$ . There has also been some suggestion that perhaps  $BP(P_{\mathbb{R}})$  is equal to  $PSPACE/\text{poly}$ . For instance, certain variants of the RAM model that provide for unit-cost arithmetic can simulate all of  $PSPACE$  in polynomial time [10, 37]. Since the Blum–Shub–Smale model also provides for unit-time multiplication on “large” numbers, Cucker and Grigoriev [27] mention that researchers have raised the possibility that similar arguments might show that polynomial-time computation over  $\mathbb{R}$  might be able to simulate  $PSPACE$ . Cucker and Grigoriev also observe that certain naïve approaches to providing such a simulation must fail.

One of our goals is to provide evidence that  $BP(P_{\mathbb{R}})$  lies properly between  $P/\text{poly}$  and  $PSPACE/\text{poly}$ . Towards this goal, it is crucial to understand a certain decision problem PosSLP: *Decide, for a given division-free straight-line program, whether it represents a positive integer*. More generally, for a fixed finite subset  $S \subset \mathbb{R}$ ,  $\text{PosSLP}(S)$  is the problem of deciding for a given division-free straight-line program, using constants from  $S \cup \{0, 1\}$ , whether the real number represented by it is positive. (For precise definitions, see the next section.)

The immediate relationship between the Blum–Shub–Smale model and the problems  $\text{PosSLP}(S)$  is given by the proposition below.

**PROPOSITION 1.1.** *We have  $P^{\text{PosSLP}(S)} = BP(P_{\mathbb{R}}^S)$  for all finite subsets  $S \subset \mathbb{R}$ . In particular,  $P^{\text{PosSLP}} = BP(P_{\mathbb{R}}^0)$ .*

*Proof.* It is clear that  $\text{PosSLP}(S)$  is in  $BP(P_{\mathbb{R}}^S)$ , since we can implement a standard SLP (straight-line program) interpreter in the real Turing machine framework

and evaluate the result in linear time using unit-cost instructions. The result is then obtained by one sign test. To show the other direction, assume that we have a polynomial-time machine over  $\mathbb{R}$  using only the constants in  $S \cup \{0, 1\}$ . By a usual argument (separate computation of numerator and denominator), we may assume without loss of generality that the machine does not use divisions. Given a bit string as input, we simulate the computation by storing the straight-line program representation of the intermediate results instead of their values. Branch instructions can be simulated by using the oracle  $\text{PosSLP}(S)$  to determine if the contents of a given register (represented by a straight-line program) are greater than zero.  $\square$

Symbolic  
execution  
+ PosSLP oracle

It was shown by Chapuis and Koiran [24] that algebraic constants do not help. More specifically,  $\mathcal{P}_{\mathbb{R}}^0$  is equal to the class of decision problems over the reals decided by polynomial-time Blum–Shub–Smale machines using real algebraic numbers as constants.

As already mentioned, by encoding the advice function in a single real constant, one can show that  $\mathcal{P}/\text{poly} \subseteq \text{BP}(\mathcal{P}_{\mathbb{R}})$ . The proof in fact shows even  $\mathcal{P}^{\text{PosSLP}}/\text{poly} \subseteq \text{BP}(\mathcal{P}_{\mathbb{R}})$ . The real constant encoding the advice function, will, of course, in general be transcendental. Thus, there is a strong relationship between nonuniformity in the classical model of computation and the use of transcendental constants in the Blum–Shub–Smale model. We conjecture that this relationship can be further strengthened, as follows.

CONJECTURE 1.  $\mathcal{P}^{\text{PosSLP}}/\text{poly} = \text{BP}(\mathcal{P}_{\mathbb{R}})$ .

In section 3 we present some preliminary results toward proving this conjecture. For instance, we prove that  $\text{BP}(\mathcal{P}_{\mathbb{R}}^{\{\alpha\}}) \subseteq \mathcal{P}^{\text{PosSLP}}/\text{poly}$  for almost all  $\alpha \in \mathbb{R}$ , in the sense of Lebesgue measure. We also show that  $\text{BP}(\mathcal{P}_{\mathbb{R}}^{\{\alpha\}}) \subseteq \mathcal{P}^{\text{PosSLP}}/1$  (one bit of advice) if  $\alpha$  is the value of an elementary function on a rational number. This is the case, for instance, for the well-known transcendental numbers  $e$  or  $\pi$ .

**1.2. The task of a numerical analyst.** The Blum–Shub–Smale model is a very elegant one, but it does not take into account the fact that actual numerical computations have to deal with *finitely* represented values. We next observe that even if we take this into account, the PosSLP problem still captures the complexity of numerical computation.

Let  $u \neq 0$  be a dyadic rational number. The *floating point* representation of  $u$  is obtained by writing  $u = v2^m$ , where  $m$  is an integer and  $\frac{1}{2} \leq |v| < 1$ . The floating point representation is then given by the sign of  $v$  and the usual binary representations of the numbers  $|v|$  and  $m$ . The floating point representation of 0 is the string 0 itself. We shall abuse notation and identify the floating point representation of a number with the number itself, using the term “floating point number” for the number as well as its representation.

Let  $u \neq 0$  be a real number. We may write  $u$  as  $u = u'2^m$ , where  $\frac{1}{2} \leq |u'| < 1$  and  $m$  is an integer. Then, we define a *floating point approximation of  $u$  with  $k$  significant bits* to be a floating point number  $v2^m$  so that  $|v - u'| \leq 2^{-(k+1)}$ .

We will focus on one part of the job that is done by numerical analysts: the design of numerically stable algorithms. In our scenario, the numerical analyst starts out with a known function  $f$ , and the task is to design a “good” algorithm for it. When we say that the function  $f$  is “known,” we mean that the analyst starts out with some method of computing (or at least approximating)  $f$ ; we restrict attention to the “easy” case where the method for computing  $f$  uses only the arithmetic operations  $+$ ,  $-$ ,  $*$ ,  $\div$ , and thus the description of  $f$  that the analyst is given can be presented as an arithmetic circuit with operations  $+$ ,  $-$ ,  $*$ ,  $\div$ . Usually, the analyst also has to worry about the

problems that are caused by the fact that the inputs to  $f$  are not known precisely but are only given as floating point numbers that are approximations to the “true” inputs—but again we will focus on the “easy” case where the analyst will merely try to compute a good approximation for  $f(x_1, \dots, x_n)$  on the exact floating point numbers  $x_1, \dots, x_n$  that are presented as input, as follows.

THE GENERIC TASK OF NUMERICAL COMPUTATION (GTNC). *Given a straight-line program  $P$  (with  $\div$ ), and given inputs  $x_1, \dots, x_n$  for  $P$  (as floating point numbers) and an integer  $k$  in unary, along with a promise that  $P(x_1, \dots, x_n)$  neither evaluates to zero nor does division by zero, compute a floating point approximation of the value of the output  $P(x_1, \dots, x_n)$  with  $k$  significant bits.*

The traditional approach that numerical analysts have followed in trying to solve problems of this sort is to study the numerical stability of the algorithm represented by the circuit and, in case of instability, to attempt to devise an equivalent computation that is numerically stable. Although stable algorithms have been found for a great many important functions, the task of devising such algorithms frequently involves some highly nontrivial mathematics and algorithmic ingenuity. There seems to be no expectation that there will ever be a purely automatic way to solve this problem, and indeed there seems to be no expectation that a numerically stable algorithm will exist in general. To summarize, there is substantial empirical evidence that the generic task of numerical computation is intractable. It would be of significant practical interest if, contrary to expectation, it should turn out to be very easy to solve (say, solvable in linear time).

We show that the generic task of numerical computation is equivalent in power to PosSLP.

PROPOSITION 1.2. *The GTNC is polynomial-time Turing equivalent to PosSLP.*

*Proof.* We first reduce PosSLP to the GTNC. Given a division-free straight-line program representing the number  $N$ , we construct a straight-line program computing the value  $v = 2N - 1$ . The only inputs 0, 1 of this program can be considered to be floating point numbers, and this circuit clearly satisfies the promise of the GTNC. Then  $N > 0$  if  $v \geq 1$ , and  $N \leq 0$  if  $v \leq -1$ . Determining an approximation of  $v$  to one significant bit is enough to distinguish between these cases.

Conversely, suppose we have an oracle solving PosSLP. Given a straight-line program with inputs being floating point numbers, we first convert it to a straight-line program having only input 1; it is easy to see that this can be done in polynomial time. By standard techniques we move all  $\div$  gates to the top, so that the program computes a value  $v = v_1/v_2$ , where  $v_1, v_2$  are given by division-free straight-line programs. We can use the oracle to determine the signs of  $v_1$  and  $v_2$ . Without loss of generality assume that  $v$  is positive. Next we use the oracle to determine whether  $v_1 \geq v_2$ . Suppose that this is indeed the case (the opposite case is handled similarly).

We then find the least  $r$  so that  $2^{r-1} \leq v < 2^r$ , by first comparing  $v_1$  with  $v_2 2^{2^i}$  for  $i = 0, 1, 2, 3, \dots$ , using the oracle, thus finding the minimum  $i$  so that  $v < 2^{2^i}$ , and afterwards doing a binary search, again using the oracle to compare  $v_1$  to  $v_2 2^r$  for various values of  $r$ . This takes polynomial time.

The desired output is a floating point number  $u = u'2^r$ , where  $|v - u'| \leq 2^{-(k+1)}$ . To obtain  $u'$  we first want to find the integer  $w$  between  $2^k$  and  $2^{k+1} - 1$  so that  $w/2^{k+1} \leq v/2^r < (w+1)/2^{k+1}$ . Since  $w/2^{k+1} \leq v/2^r < (w+1)/2^{k+1}$  iff  $w2^r v_2 \leq v_1 2^{k+1} < (w+1)2^r v_2$ , we can determine this by another binary search, using  $O(k)$  calls to the oracle. We then output the sign of  $v$ , the binary representation of the rational  $w/2^{k+1}$ , and the binary representation of  $r$ , together forming the desired floating point approximation of  $v$ .  $\square$

The reader may wonder how GTNC fits into the numerical analysis literature. The long exponent model (LEM) of Demmel [31, 30] offers the closest parallel. Demmel considers the classic problem of computation of the determinant, and he identifies three ways of modeling the problem, which he calls the traditional model, the short exponent model (SEM), and the LEM. Computing determinants is easy in the SEM, while in the LEM the problem is equivalent to a special case of GTNC. Namely, it is equivalent to instances of GTNC where the circuit  $C$  that is provided as input is the polynomial-size SLP for determinants given by Berkowitz [9].

Demmel goes so far as to conjecture that, in the LEM, the problem of deciding whether the determinant is zero is NP-hard [31]. Since this problem is actually a special case of EquSLP and thus lies in BPP, Demmel's conjecture is almost certainly false. However, we agree with his underlying intuition, in that we believe that the problem of deciding whether the determinant is *positive* in the LEM very likely is intractable (even if we see no evidence that it is NP-hard) [57]. That is, this special case of PosSLP is recognized as a difficult problem by the numerical analysis community.

$$\begin{aligned} \mathbb{RP} &\subseteq \mathbb{BPP} \\ \text{CoRP} &\subseteq \mathbb{BPP} \end{aligned}$$

**1.3. The complexity of PosSLP.** We consider Proposition 1.2 to be evidence for the computational intractability of PosSLP. If PosSLP is in P/poly, then there is a polynomial-sized “cookbook” that can be used in place of the creative task of devising numerically stable computations. This seems unlikely.

We wish to emphasize that the generic task of numerical computation models the *discrete* computational problem that underlies an important class of computational problems. Thus it differs quite fundamentally from the approach taken in the Blum–Shub–Smale model.

We also wish to emphasize that, in defining the generic task of numerical computation, we are *not* engaging in the debate over which real functions are “efficiently computable.” There is by now a large literature comparing and contrasting the relative merits of the Blum–Shub–Smale model with the so-called bit model of computing, and there are various competing approaches to defining what it means for a real-valued function to be feasible to compute; see [13, 17, 16, 67, 68] among others. Our concerns here are orthogonal to that debate. We are not trying to determine which real-valued functions are feasible; we are studying a discrete computational problem that is relevant to numerical analysis, with the goal of proving upper and lower bounds on its complexity.

The generic task of numerical computation is one way of formulating the notion of what is feasible to compute in a world where *arbitrary precision* arithmetic is available for free. In contrast, the Blum–Shub–Smale model can be interpreted as formulating the notion of feasibility in a world where *infinite precision* arithmetic is available for free. According to Proposition 1.2, both of these approaches are *equivalent* (and captured by  $\mathbf{P}^{\text{PosSLP}}$ ) when only algebraic constants are allowed in the Blum–Shub–Smale model. Conjecture 1 claims that this is also true when allowing arbitrary real constants.

As another demonstration of the computational power of PosSLP, we show in section 2 that the problem of determining the total degree of a multivariate polynomial over the integers given as a straight-line program reduces to PosSLP.

The above discussion suggests that PosSLP is not an easy problem. Can more formal evidence of this be given? Although it would be preferable to show that PosSLP is hard for some well-studied complexity class, the best that we can do is observe that a somewhat stronger problem (BitSLP) is hard for  $\#P$ . This will be done in section 2.

The above discussion also suggests that nontrivial upper bounds for PosSLP are

of great interest. Prior to this paper, the best upper bound was PSPACE. Our main technical result is an improved upper bound: We show, based on results on the uniform circuit complexity of integer division and the relationship between constant depth circuits and subclasses of PSPACE [6, 39], that PosSLP lies in the counting hierarchy CH, a well-studied subclass of PSPACE that bears more or less the same relationship to  $\#P$  as the polynomial hierarchy bears to NP [64, 66].

CH  $\subseteq$  PSPACE

THEOREM 1.3. PosSLP is in  $P^{PPP^{PP}}$ . *even in  $PH^{PP^{PP}}$*

third level  $C_3$  of the counting hierarchy

Another interesting upper bound for PosSLP was recently discovered by Tarasov and Vyalii [61], who give a reduction from PosSLP to the semidefinite feasibility problem (SDFP), i.e., the feasibility version of the optimization problem semidefinite programming. Their result can be seen as a lower bound for SDFP. SDFP is known to reduce to its complement and to lie in  $NP_{\mathbb{R}}$  [54]; also it is easy to see that SDFP reduces to the existential theory of the reals (for instance, see the discussion in [54]), and thus  $SDFP \in PSPACE$ .

We suspect that PosSLP lies at an even lower level of CH. Note that, in presenting our upper bound, we do not exploit some powerful techniques that have been proved useful in computing certain bits of exponentially large numbers [40]. We leave as major open problems the question of providing better upper bounds for PosSLP and the question of providing any sort of hardness theorem, reducing a supposedly intractable problem to PosSLP.

Theorem 1.3, together with Proposition 1.1, implies that  $BP(P_{\mathbb{R}}^0) \subseteq CH$ . It is reasonable to conjecture that  $BP(P_{\mathbb{R}}) \subseteq CH/\text{poly}$ —and indeed that would follow from Conjecture 1—but as yet we are not able to improve the upper bound of  $BP(P_{\mathbb{R}}) \subseteq PSPACE/\text{poly}$  that was presented by Cucker and Grigoriev [27].

We believe that it would be very interesting to verify Conjecture 1, as this would give a characterization of  $BP(P_{\mathbb{R}})$  in terms of classical complexity classes. But in fact, it would be equally interesting to refute it under some plausible complexity-theoretic assumption, as this would give evidence that the power of using transcendental constants in the sequential Blum–Shub–Smale model goes beyond the power of nonuniformity in classical computation.

**1.4. Applications.** The sum-of-square-roots problem is a well-known problem with many applications to computational geometry and elsewhere. The input to the problem is a list of integers  $(d_1, \dots, d_n)$  and an integer  $k$ , and the problem is to decide whether  $\sum_i \sqrt{d_i} \geq k$ . The complexity of this problem is posed as an open question by Garey, Graham, and Johnson [36] in connection with the Euclidean traveling salesman problem, which is not known to be in NP but which is easily seen to be solvable in NP relative to the sum-of-square-roots problem. See also O'Rourke [53, 52] and Etessami and Yannakakis [34] for additional information. Although it has been conjectured [51] that the problem lies in P, it seems that no classical complexity class smaller than PSPACE has been known to contain this problem. On the other hand, by observing that one can construct a polynomial-sized straight-line program with division that approximates the square root of any given integer with exponentially high precision, using Newton iteration, Tiwari [62] showed that this problem can be decided in polynomial time on an “algebraic random-access machine.” In fact, it is easy to see that the set of decision problems decided by such machines in polynomial time is exactly  $BP(P_{\mathbb{R}}^0)$ . Thus by Proposition 1.1 we see that the sum-of-square-roots problem reduces to PosSLP. Theorem 1.3 thus yields the following corollary.

COROLLARY 1.4. The sum-of-square-roots problem and the Euclidean traveling salesman problem are in CH.

**2. Preliminaries.** Our definitions of arithmetic circuits and straight-line programs are standard. An arithmetic circuit is a directed acyclic graph with input nodes labeled with the constants 0, 1 or with indeterminates  $X_1, \dots, X_k$  for some  $k$ . Internal nodes are labeled with one of the operations  $+$ ,  $-$ ,  $*$ ,  $\div$ . A straight-line program is a sequence of instructions corresponding to a sequential evaluation of an arithmetic circuit. If it contains no  $\div$  operation, it is said to be division-free. Unless otherwise stated, all the straight-line programs considered will be division-free. Thus straight-line programs can be seen as very compact representations of a polynomial over the integers. In many cases, we will be interested in division-free straight-line programs using no indeterminates, which thus represent an integer.

with division

By the  $n$ -bit binary representation of an integer  $N$  such that  $|N| < 2^n$  we understand a bit string of length  $n + 1$  consisting of a *sign bit* followed by  $n$  bits encoding  $|N|$  (padded with leading zeroes, if needed).

We consider the following problems:

EquSLP. Given a straight-line program representing an integer  $N$ , decide whether  $N = 0$ .

ACIT. Given a straight-line program representing a polynomial  $f \in \mathbb{Z}[X_1, \dots, X_k]$ , decide whether  $f = 0$ .

DegSLP. Given a straight-line program representing a polynomial  $f \in \mathbb{Z}[X_1, \dots, X_k]$  and given a natural number  $d$  in binary, decide whether  $\deg f \leq d$ .

PosSLP. Given a straight-line program representing  $N \in \mathbb{Z}$ , decide whether  $N > 0$ .

BitSLP. Given a straight-line program representing  $N$ , and given  $n, i \in \mathbb{N}$  in binary, decide whether the  $i$ th bit of the  $n$ -bit binary representation of  $N$  is 1.

It is not clear that any of these problems is in P, since straight-line program representations of integers can be exponentially smaller than ordinary binary representation.

There is an immediate relationship between the Blum-Shub-Smale model over the complex numbers  $\mathbb{C}$  and the problem EquSLP. Let  $P_{\mathbb{C}}^0$  denote the class of decision problems over  $\mathbb{C}$  decided by polynomial-time Blum-Shub-Smale machines using only the constants 0, 1. Similarly as for Proposition 1.1 one can show that  $P^{\text{EquSLP}} = \text{BP}(P_{\mathbb{C}}^0)$ . On the other hand, it is known that constants can be eliminated in this setting [11, 45], and hence  $\text{BP}(P_{\mathbb{C}}) = \text{BP}(P_{\mathbb{C}}^0)$ . We therefore have the following result.

**PROPOSITION 2.1.**  $P^{\text{EquSLP}} = \text{BP}(P_{\mathbb{C}})$ .

Clearly, EquSLP is a special case of ACIT. Schönhage [57] showed that EquSLP is in coRP, using computation modulo a randomly chosen prime. Ibarra and Moran [41], building on DeMillo and Lipton [29], Schwartz [58], and Zippel [69], extended this to show that ACIT lies in coRP. In the spirit of Adleman's observation [1], Heintz and Schnorr [38] established the existence of nonuniform polynomial-time algorithms for an algebraic variant of the ACIT problem (allowing any field elements as constants). The problem ACIT has recently attracted much attention due to the work of Kabanets and Impagliazzo [42] who showed that a deterministic algorithm for ACIT would yield circuit lower bounds. (See [47] for some progress on finding deterministic algorithms for certain versions of the problem.) As far as we know, although the proof technique that we use in Proposition 2.2 is well known and has been applied various times over the years [3, 60], it has not been pointed out before that ACIT is actually polynomial-time equivalent to EquSLP. In other words, disallowing indeterminates in the straight-line program given as input does not make ACIT easier. Or more optimistically: It is enough to find a deterministic algorithm for this special case in order to have circuit lower bounds.

PTIME equivalent

$\text{EquSLP} \subseteq \text{coRP}$   
 $\uparrow \text{PTIME}$   
 $\text{ACIT} \subseteq \text{coRP}$



PROPOSITION 2.2. *ACIT is polynomial-time equivalent to EquSLP.*

*Proof.* We are given a straight-line program of size  $n$  with  $m$  indeterminates  $X_1, \dots, X_m$ , computing the polynomial  $p(X_1, \dots, X_m)$ . Define  $B_{n,i} = 2^{2^{in^2}}$ . Straight-line programs computing these numbers using iterated squaring can easily be constructed in polynomial time, so given a straight-line program for  $p$ , we can easily construct a straight-line program for  $p(B_{n,1}, \dots, B_{n,m})$ . We shall show that for  $n \geq 3$ ,  $p$  is identically zero iff  $p(B_{n,1}, \dots, B_{n,m})$  evaluates to zero.

To see this, first note that the “only if” part is trivial, so we only have to show the “if” part. Thus, assume that  $p(X_1, \dots, X_m)$  is not the zero-polynomial. Let  $q(X_1, \dots, X_m)$  be the largest monomial occurring in  $p$  with respect to inverse lexicographic order,<sup>1</sup> and let  $k$  be the number of monomials. We can write  $p = \alpha q + \sum_{i=1}^{k-1} \alpha_i q_i$ , where  $(q_i)_{i=1, \dots, k-1}$  are the remaining monomials. An easy induction in the size of the straight-line program shows that  $|\alpha_i| \leq 2^{2^{2n}}$ ,  $k \leq 2^{2^n}$  and that the degree of any variable in any  $q_i$  is at most  $2^n$ .

Now, our claim is that the absolute value  $|\alpha q(B_{n,1}, \dots, B_{n,m})|$  is strictly bigger than  $|\sum_{i=1}^{k-1} \alpha_i q_i(B_{n,1}, \dots, B_{n,m})|$ , and thus we cannot have that  $p(B_{n,1}, \dots, B_{n,m}) = 0$ .

Indeed, since the monomial  $q$  was the biggest in the inverse lexicographic ordering, we have that for any other monomial  $q_i$  there is an index  $j$  so that

$$\frac{q(B_{n,1}, \dots, B_{n,m})}{q_i(B_{n,1}, \dots, B_{n,m})} \geq \frac{2^{2^{jn^2}}}{\prod_{l=1}^{j-1} 2^{2^{ln^2} \cdot 2^n}} > 2^{2^{n^2-1}},$$

so we can bound

$$\begin{aligned} \left| \sum_{i=1}^{k-1} \alpha_i q_i(B_{n,1}, \dots, B_{n,m}) \right| &\leq 2^{2^n} 2^{2^{2n}} \left| \max_{i=1}^{k-1} q_i(B_{n,1}, \dots, B_{n,m}) \right| \\ &\leq 2^{2^n} 2^{2^{2n}} 2^{-2^{n^2-1}} |q(B_{n,1}, \dots, B_{n,m})| < q(B_{n,1}, \dots, B_{n,m}) \leq |\alpha q(B_{n,1}, \dots, B_{n,m})|, \end{aligned}$$

which proves the claim.  $\square$

We believe that Proposition 2.2 could be a useful tool for devising deterministic algorithms for ACIT. (See section 5 for one modest application in this direction.) Of course, it must also be acknowledged that multivariate polynomials exhibit a great deal of structure that is not so apparent in computation over the integers (as embodied by EquSLP), and algorithmic attacks on ACIT should also attempt to exploit this structure.

The problem DegSLP is not known to lie in BPP, even for the special case of univariate polynomials. Here, we show that it reduces to PosSLP.

PROPOSITION 2.3. DegSLP polynomial-time many-one reduces to PosSLP.

*Proof.* We first show the reduction for the case of univariate polynomials (i.e., straight-line programs with a single indeterminate), and afterwards we reduce the multivariate case to the univariate case.

Let  $f \in \mathbb{Z}[X]$  be given by a straight-line program of length  $n$ . To avoid having to deal with the zero polynomial of degree  $-\infty$  and to ensure that the image of the polynomial is a subset of the nonnegative integers, we first change the straight-line program computing  $f$  into a straight-line program computing  $f_1(X) = (Xf(X) + 1)^2$

<sup>1</sup>  $X_1^{\alpha_1} \dots X_m^{\alpha_m}$  is greater than  $X_1^{\beta_1} \dots X_m^{\beta_m}$  in this order iff the right-most nonzero component of  $\alpha - \beta$  is positive; cf. Cox, Little, and O’Shea [26, p. 59].



by adding a few extra lines. We can check whether the degree of  $f$  is at most  $d$  by checking whether the degree of  $f_1$  is at most  $D = 2(d+1)$  (except for  $d = -\infty$ , in which case we check whether the degree of  $f_1$  is at most  $D = 0$ ).

Let  $B_n$  be the integer  $2^{2^{n^2}}$ . As in the proof of Proposition 2.2, we can easily construct a straight-line program computing  $B_n$  and from this a straight-line program computing  $f_1(B_n)$ .

Now, suppose that  $\deg f_1 \leq D$ . Using the same bounds on sizes of the coefficients as in the proof of Proposition 2.2 and assuming without loss of generality that  $n \geq 3$ , we then have

$$f_1(B_n) \leq \sum_{i=0}^D 2^{2^{2n}} B_n^i < (2^n + 1) 2^{2^{2n}} B_n^D \leq (2^{2^n} + 1) 2^{2^{2n} - 2^{n^2}} B_n^{D+1} < \frac{B_n^{D+1}}{2}.$$

On the other hand, suppose that  $\deg f_1 \geq D+1$ . Then we have

$$f_1(B_n) \geq (B_n)^{D+1} - \sum_{i=0}^D 2^{2^{2n}} B_n^i \geq B_n^{D+1} - 2^{2^n} 2^{2^{2n}} 2^{-2^{n^2}} B_n^{D+1} > \frac{B_n^{D+1}}{2}.$$

Thus, to check whether  $\deg f_1 \leq D$ , we just need to construct a straight-line-program for  $2f_1(B_n) - B_n^{D+1}$  and check whether it computes a positive integer. This completes the reduction for the univariate case.

We next reduce the multivariate case to the univariate case. Thus, let  $f$  in  $\mathbb{Z}[X_1, \dots, X_m]$  be given by a straight-line program of length  $n$ . We define  $f^*$  in  $\mathbb{Z}[X_1, \dots, X_m, Y]$  by  $f^*(X_1, \dots, X_m, Y) = f(X_1 Y, \dots, X_m Y)$ . We claim that if we let  $B_{n,i} = 2^{2^{in^2}}$  as in the proof of Proposition 2.2, then, for  $n \geq 3$ , the degree of the univariate polynomial  $f^*(B_{n,1}, \dots, B_{n,m}, Y)$  is equal to the total degree of  $f$ . Indeed, we can write  $f^*$  as a polynomial in  $Y$  with coefficients in  $\mathbb{Z}[X_1, \dots, X_m]$ :

$$f^*(X_1, \dots, X_m, Y) = \sum_{j=0}^{d^*} g_j(X_1, \dots, X_m) Y^j,$$

where  $d^*$  is the degree of variable  $Y$  in the polynomial  $f^*$ . Note that this is also the total degree of the polynomial  $f$ . Now, the same argument as used in the proof of Proposition 2.2 shows that since  $g_{d^*}$  is not the zero-polynomial,  $g_{d^*}(B_{n,1}, B_{n,2}, \dots, B_{n,m})$  is different from 0.  $\square$

As PosSLP easily reduces to BitSLP, we obtain the chain of reductions

$$\text{EquSLP} \equiv \text{ACIT} \leq_m^P \text{DegSLP} \leq_m^P \text{PosSLP} \leq_m^P \text{BitSLP}.$$

$\in CH$

In section 4 we will show that all the above problems in fact lie in the counting hierarchy CH.

The complexity of BitSLP contrasts sharply with that of EquSLP.

PROPOSITION 2.4. BitSLP is hard for #P

*Proof.* A similar result is stated without proof in [31]. The proof that we present is quite similar to that of Bürgisser [22, Proposition 5.3], which in turn is based on ideas of Valiant [65]. We show that computing the permanent of matrices with entries from  $\{0,1\}$  is reducible to BitSLP.

Given a matrix  $X$  with entries  $x_{i,j} \in \{0,1\}$ , consider the univariate polynomial

$$f_n = \sum_i f_{n,i} Y^i = \prod_{i=1}^n \left( \sum_{j=1}^n x_{i,j} Y^{2^{j-1}} \right),$$

which can be represented by a straight-line program of size  $O(n^2)$ . Then  $f_{n,2^n-1}$  equals the permanent of  $X$ . Let  $N$  be the number that is represented by the straight-line program that results from replacing the indeterminate  $Y$  with  $2^{n^3}$ . It is easy to see that the binary representation of  $f_{n,2^n-1}$  appears as a sequence of consecutive bits in the binary representation of  $N$ .  $\square$

Triggered by an earlier version of this paper [5], Koiran and Perifel [43] studied the variant of the problem DegSLP for computations of polynomials over the finite field  $\mathbb{F}_p$ . They proved a considerably better upper bound on this problem than what is currently known for DegSLP. Also, Koiran and Perifel [43] investigated the problem *zero monomial coefficient* of deciding for a polynomial  $f$  given by a straight-line program and a given monomial  $x^\alpha$  whether the coefficient of this monomial in  $f$  equals zero. For computations of polynomials over the finite field  $\mathbb{F}_p$ , they managed to show that *zero monomial coefficient* is  $\text{Mod}_p P$  complete. However, for characteristic zero, no improvements upon the results in this paper were made in that respect.

**3. Transcendental constants.** We present here some first results toward establishing our Conjecture 1.

Let  $S$  denote a fixed finite subset of  $\mathbb{R}$ . By an *SLP over  $S$*  we shall understand a division-free straight-line program using constants from  $S \cup \{0, 1\}$ . Recall the following problem:

**PosSLP( $S$ ).** Given an SLP over  $S$ , decide whether the real number represented by it is positive.

*Remark 1.* We could have defined a variant of  $\text{PosSLP}(S)$  by allowing divisions in the straight-line programs. However, this variant is easily seen to be polynomial-time equivalent to  $\text{PosSLP}(S)$ . Indeed, by computing separately with numerators and denominators we can transform an SLP representing  $\alpha$  into two division-free SLPs representing numbers  $A, B$  such that  $\alpha = A/B$ . Hereby, the length of the SLPs increases at most by a factor of four. Now  $\alpha$  is positive iff  $AB$  is positive.

A result by Chapuis and Koiran [24] implies that algebraic constants can be eliminated. It can be stated as follows.

**PROPOSITION 3.1.** *Let  $S \subseteq \mathbb{R}$  be finite and  $\alpha \in \mathbb{R}$  be algebraic over the field  $\mathbb{Q}(S)$ . Then  $\text{pPosSLP}(S \cup \{\alpha\}) = \text{pPosSLP}(S)$ .*

Our first goal is to prove that almost all transcendental constants can be eliminated.

**THEOREM 3.2.** *For all  $(\alpha_1, \alpha_2, \dots, \alpha_k) \in \mathbb{R}^k$  except in a subset of Lebesgue measure zero we have  $\text{pPosSLP}(\{\alpha_1, \dots, \alpha_k\})/\text{poly} = \text{pPosSLP}/\text{poly}$ .*

The proof will require some lemmas. The idea is to eliminate one by one the elements of such sets  $S$ , replacing each element with appropriate advice of polynomial size.

We denote by  $R_n^S \subset \mathbb{R}$  the set of all real numbers that occur as a root of some nonzero univariate polynomial that is computed by an SLP of size  $n$  that uses constants in  $S$ . Note that  $\mathbb{R} \setminus R_n^S$  consists of a collection of open intervals. Clearly, any univariate polynomial computed from  $S$  by an SLP of size  $n$  has constant sign on each of these intervals. For  $\alpha \in \mathbb{R} \setminus R_n^S$ , we denote by  $I_n^S(\alpha)$  the unique interval containing  $\alpha$ .

*Remark 2.* A real number  $\alpha$  is transcendental over  $\mathbb{Q}(S)$  iff  $\alpha \notin R_n^S$  for all  $n$  (or equivalently, for infinitely many  $n$ ).

**DEFINITION 3.3.** *We call a real number  $\alpha$  approximable with respect to  $S$  if either  $\alpha$  is algebraic over  $\mathbb{Q}(S)$  or else  $\alpha$  is transcendental over  $\mathbb{Q}(S)$  and satisfies the following condition: there exists a polynomial  $p$  such that for all sufficiently large*

$n \in \mathbb{N}$  the interval  $I_n^S(\alpha)$  contains an element  $x_n$  that can be represented by an SLP over  $S$  of size  $p(n)$ , possibly using divisions. (Note that this interval is well defined as  $\alpha \notin R_n^S$ ; cf. Remark 2.) We say that  $\alpha$  is approximable iff it is approximable with respect to the empty set.

LEMMA 3.4. *If  $\alpha \in \mathbb{R}$  is approximable with respect to  $S$ , then  $\mathbf{P}^{\text{PosSLP}(S \cup \{\alpha\})}/\text{poly} = \mathbf{P}^{\text{PosSLP}(S)}/\text{poly}$ .*

*Proof.* Suppose that  $\alpha \in \mathbb{R}$  is approximable with respect to  $S$ . By Proposition 3.1 we may assume that  $\alpha$  is transcendental over  $\mathbb{Q}(S)$ . Then, for all sufficiently large  $n$ , there exist  $x_n \in I_n^S(\alpha)$  computed by an SLP  $\Gamma_n$  over  $S$  (using divisions) of size polynomial in  $n$ .

It is sufficient to show that  $\text{PosSLP}(S \cup \{\alpha\})$  is contained in  $\mathbf{P}^{\text{PosSLP}(S)}/\text{poly}$ . Let  $C$  be an SLP (of size  $n$ ) over  $S \cup \{\alpha\}$  computing  $v \in \mathbb{R}$ . We want to decide whether  $v$  is positive. If we replace the constant  $\alpha$  by the variable  $X$ , then this SLP computes a polynomial  $f(X)$  and we have  $v = f(\alpha)$ . Since the sign of  $f$  is constant on the interval  $I_{p(n)}^S(\alpha)$ ,  $v$  has the same sign as  $f(x_{p(n)})$ .

We interpret the SLP  $\Gamma_n$  over  $S$  as an advice of polynomial size. By concatenating  $\Gamma_n$  with the SLP for  $f$ , we obtain an SLP over  $S$  that computes  $f(x_{p(n)})$ . We eliminate the divisions in the concatenated SLP according to Remark 1. Then the sign of this number is obtained by one oracle call to  $\text{PosSLP}(S)$ .  $\square$

LEMMA 3.5. *We have the following:*

1.  $|R_n^S| \leq (6(n + |S|))^n$ .
2. *The minimal distance between two different elements of  $R_n^\emptyset$  is at least  $2^{-2^{N_n}}$  with  $N_n = O(n \log n)$ .*

*Proof.* Let  $F_n$  be the product of all nonzero univariate polynomials  $f$  that can be computed from the variable  $X$  by an SLP over  $S$  of size  $n$ . Note that such  $f$  have degree at most  $2^n$ . Then  $R_n^S$  is the set of roots of  $F_n$ . There are at most  $\prod_{i=1}^n 3(|S| + i - 1)^2 \leq (3(|S| + n)^2)^n$  SLPs over  $S$ . Therefore,  $\deg F_n \leq (6(|S| + n)^2)^n$ , which shows the first assertion.

Before showing the second assertion we introduce a notation: let  $\|g\|_1$  denote the sum of the absolute values of the coefficients of a univariate polynomial  $g$ . It is easy to see that  $\|g \cdot h\|_1 \leq \|g\|_1 \cdot \|h\|_1$ .

Suppose now  $S = \emptyset$ . If  $f(X)$  is computed by an SLP of size  $n$  over  $\emptyset$  from the variable  $X$ , then one can show that  $\log \|f\|_1 \leq (n + 1)2^n$ ; see, e.g., [21, Lemma 4.16]. By the submultiplicativity of  $\|\cdot\|_1$  we conclude

$$\log \|F_n\|_1 \leq (3n^2)^n (n + 1)2^n \leq 2^{O(n \log n)}.$$

Rump [55] showed that the distance between any two distinct real roots in a univariate polynomial  $P$  with integer coefficients and degree  $d$  is at least  $2\sqrt{2}(d^{\frac{d}{2}+1}(\|P\|_1 + 1)^d)^{-1}$ . The second assertion follows by applying this bound to the polynomial  $F_n$ .  $\square$

LEMMA 3.6. *For any finite  $S \subset \mathbb{R}$ , the set of real numbers that are not approximable with respect to  $S$  has Lebesgue measure zero.*

*Proof.* Let  $\alpha \in \mathbb{R}$  and  $x_n$  be the binary approximation of  $\alpha$  with a precision of  $n^2$  digits, i.e.,  $|\alpha - x_n| < 2^{-n^2}$ . Clearly, there is an SLP over  $\{1/2\}$  of size  $O(n^2)$  representing  $x_n$ . Furthermore, suppose that  $\alpha$  has distance at least  $2^{-n^2}$  from  $R_n^S$  for all sufficiently large  $n$ , say for  $n \geq m$ . Then  $x_n$  is contained in the interval  $I_n^S(\alpha)$  for  $n \geq m$ . Hence, by definition,  $\alpha$  is approximable with respect to  $S$ .

These reasonings show that for all  $m \in \mathbb{N}$

$$B := \{\alpha \in \mathbb{R} \mid \alpha \text{ is not approximable w.r.t. } S\} \subseteq \bigcup_{n \geq m} U_n,$$

where  $U_n := \{x \in \mathbb{R} \mid \exists \rho \in R_n^S \mid |x - \rho| < 2^{-n^2}\}$  denotes the  $2^{-n^2}$ -neighborhood of  $R_n^S$ . Denoting by  $\lambda(A)$  the Lebesgue measure of a set  $A \subseteq \mathbb{R}$ , we get from Lemma 3.5

$$\lambda(U_n) \leq 2 |R_n^S| 2^{-n^2} \leq 2(6(n + |S|))^n 2^{-n^2} \leq 2^{-\frac{1}{2}n^2}$$

for sufficiently large  $n$ . Therefore, we conclude that for all sufficiently large  $m$

$$\lambda(B) \leq \sum_{n=m}^{\infty} 2^{-\frac{1}{2}n^2}.$$

Since the series  $\sum_n 2^{-\frac{1}{2}n^2}$  is convergent and  $m$  was arbitrary, we conclude that  $\lambda(B) = 0$ .  $\square$

*Proof of Theorem 3.2.* We consider for  $\alpha := (\alpha_1, \dots, \alpha_k) \in \mathbb{R}^k$  and  $0 \leq i \leq k$  the complexity classes  $\mathcal{C}_i(\alpha) := \mathbf{P}^{\text{PosSLP}(\{\alpha_1, \dots, \alpha_i\})} / \text{poly}$ . Clearly,  $\mathcal{C}_k(\alpha) \neq \mathcal{C}_0(\alpha)$  implies that  $\mathcal{C}_s(\alpha) \neq \mathcal{C}_{s-1}(\alpha)$  for some index  $s$ . By applying Lemma 3.4 to the set of constants  $S = \{\alpha_1, \dots, \alpha_{s-1}\}$ , we obtain that  $\{\alpha \in \mathbb{R}^k \mid \mathcal{C}_k(\alpha) \neq \mathcal{C}_0(\alpha)\}$  is a subset of

$$\subseteq \bigcup_{s=1}^k \{\alpha \in \mathbb{R}^k \mid \alpha_s \text{ is not approximable w.r.t. } \{\alpha_1, \dots, \alpha_{s-1}\}\}.$$

Lemma 3.6 says that, for fixed  $\alpha_1, \dots, \alpha_{s-1}$ , the set

$$\{\alpha_s \in \mathbb{R} \mid \alpha_s \text{ is not approximable w.r.t. } \{\alpha_1, \dots, \alpha_{s-1}\}\}$$

has Lebesgue measure zero. It follows from Fubini's theorem that the right-hand subset of  $\mathbb{R}^k$  has measure zero as well, which shows the assertion.  $\square$

We can actually prove for many specific real numbers that they are approximable. Indeed, quite surprisingly, for any elementary function  $f(X)$  there exists a sequence  $(R_n(X))$  of rational functions such that  $|R_n(x) - f(x)| < 2^{-n}$  for all  $x \in [0, 1]$ , and such that  $R_n(X)$  can be computed by a straight-line program of polylogarithmic size (using divisions) from  $X$ . The elementary functions include the algebraic functions, the natural logarithm, and the exponential function. For algebraic functions, such approximating rational functions can be constructed with Newton's method; see Kung and Traub [46]. For the natural logarithm, the construction of such approximations relies on the AGM (arithmetic-geometric mean) iteration going back to Gauss, Lagrange, and Legendre, which, in particular, gives very good approximations of  $\pi$ . The latter algorithms were discovered by Brent [18] and Salamin [56]. The book by Borwein and Borwein [15] provides a complete and in-depth exposition of this subject.

More precisely, we shall understand by an *elementary function* a function built up from rational constants by finitely many arithmetic operations, applications of  $\exp$ ,  $\ln$ , and the operation of taking a solution of a polynomial equation. (For a formal definition see [19].)

**THEOREM 3.7.** *Let  $\alpha$  be the value of an elementary function at a rational number. Then the following hold:*

1.  $\alpha$  is approximable. In particular,  $e = \exp(1)$  and  $\pi$  are approximable.
2. We have  $\mathbf{P}^{\text{PosSLP}(\{\alpha\})} \subseteq \mathbf{P}^{\text{PosSLP}}/1$ , where  $/1$  means one bit of advice.

*Proof.* 1. By Lemma 3.5 we know that  $\epsilon_n = 2^{-2^{N_n}}$  with  $N_n = O(n \log n)$  is a lower bound on the minimum distance between two different elements of  $R_n^\emptyset$ . Note that there is an SLP over  $\{1/2\}$  of polynomial size computing  $\epsilon_n$  (repeated squaring).

Let  $\alpha$  be as in the statement of the theorem. Without loss of generality we may assume that  $\alpha$  is transcendental. According to Borwein and Borwein [14, Table 1], for each  $n$  there is an SLP of size  $n^{O(1)}$  (using divisions) computing an approximation  $a_n$  of  $\alpha$  that satisfies  $|a_n - \alpha| < \frac{1}{2}\epsilon_n$ . By checking the proofs (cf. Borwein and Borwein [15]) one sees that these SLPs are uniform; i.e., they can be constructed in polynomial time in  $n$ .

We claim that there exist  $b_n \in \{0, 1\}$  such that  $x_n = a_n + b_n \frac{1}{2}\epsilon_n$  lies in the interval  $I_n^\emptyset(\alpha)$  and thus satisfies the requirement in Definition 3.3. Hence  $\alpha$  is approximable.

Indeed, let  $\ell_n$  and  $r_n$  denote the left and right endpoints of the interval  $I_n^\emptyset(\alpha)$ , and denote by  $m_n := \frac{1}{2}(\ell_n + r_n)$  its midpoint. Consider first the case where  $\alpha < m_n$ . If  $\alpha \leq a_n$ , then  $a_n < \alpha + \frac{1}{2}\epsilon_n < m_n + \frac{1}{2}\epsilon_n \leq r_n$ , and hence  $x_n := a_n \in I_n^\emptyset(\alpha)$ . Else if  $a_n < \alpha$ , then  $\alpha < a_n + \frac{1}{2}\epsilon_n < \alpha + \frac{1}{2}\epsilon_n \leq r_n$ , and hence  $x_n := a_n + \frac{1}{2}\epsilon_n \in I_n^\emptyset(\alpha)$  does the job. In the case where  $\alpha \geq m_n$  one argues similarly.

2. We follow the proof of Lemma 3.4. However, since the SLPs computing the approximation  $a_n$  are polynomial-time uniform, only one bit of advice (corresponding to  $b_n$ ) is in fact needed to emulate the computation with  $\alpha$ .  $\square$

We have not been able to find a specific number that is *provably* nonapproximable. It is quite possible that there are no nonapproximable numbers at all.

**4. PosSLP lies in CH.** The counting hierarchy CH was defined by Wagner [66] and was studied further by Torán [64]; see also [8, 6]. A problem lies in CH if it lies in one of the classes in the sequence PP, PP<sup>PP</sup>, etc.

THEOREM 4.1. BitSLP is in CH.

*Proof.* It was shown by Hesse, Allender, and Mix Barrington [39] that there are Dlogtime-uniform threshold circuits of polynomial size and constant depth that compute the following function:

**Input:** A number  $X$  in Chinese remainder representation. That is, a sequence of values indexed  $(p, j)$  giving the  $j$ th bit of  $X \bmod p$ , for each prime  $p < n^2$ , where  $0 \leq X \leq 2^n$  (thus we view  $n$  as an appropriate “size” measure of the input).

**Output:** The binary representation of the unique natural number  $X < \prod_{p \text{ prime}, p < n^2} p$  whose value modulo each small prime is encoded in the input.

Let this circuit family be denoted  $\{D_n\}$ .

Now, as in the proof of [6, Lemma 5], we consider the following exponentially big circuit family  $\{E_n\}$ , which computes BitSLP.

Given as input an encoding of a straight-line program representing integer  $W$ , we first build a new program computing the positive integer  $X = W + 2^{2^n}$ . Note that the bits of the binary representation of  $W$  (including the sign bit) can easily be obtained from the bits of  $X$ .

Level 1 of the circuit  $E_n$  consists of gates labeled  $(p, j)$  for each prime  $p$  such that  $p < 2^{2^n}$  and for each  $j : 1 \leq j \leq \lceil \log p \rceil$ . The output of this gate records the  $j$ th bit of  $X \bmod p$ . (Observe that there are exponentially many gates on level 1, and also note that the output of each gate  $(p, j)$  can be computed in time polynomial in the size of the binary encoding of  $p$  and the size of the given straight-line program representing  $X$ . Note also that the gates on Level 1 correspond to the gates on the input level of the circuit  $D_{2^{2^n}}$ .)

The higher levels of the circuit are simply the gates of  $D_{2^{2^n}}$ .

in fact PP  
✓ PH ⊆ P  
by Toda's Theorem  
PH ⊆ CH ⊆ PSPACE

Now, similar to the proof of [6, Lemma 5], we claim that for each constant  $d$  the following language is in the counting hierarchy:  $L_d = \{(F, P, b) : F \text{ is the name of a gate on level } d \text{ of } E_n \text{ and } F \text{ evaluates to } b \text{ when given straight-line program } P \text{ as input}\}$ .

We have already observed that this is true when  $d = 1$ . For the inductive step, assume that  $L_d \in \text{CH}$ . Here is an algorithm to solve  $L_{d+1}$  using oracle access to  $L_d$ . On input  $(F, P, b)$ , we need to determine whether the gate  $F$  is a gate of  $E_n$ , and if so, we need to determine whether it evaluates to  $b$  on input  $P$ .  $F$  is a gate of  $E_n$  iff it is connected to some gate  $G$  such that, for some  $b'$ ,  $(G, P, b') \in L_d$ . This can be determined in  $\text{NP}^{L_d} \subseteq \text{PP}^{L_d}$ , since  $D_n$  is Dlogtime-uniform. That is, we can guess a gate  $G$ , check that  $G$  is connected to  $F$  (this takes only linear time because of the uniformity condition), and then use our oracle for  $L_d$ . If  $F$  is a gate of  $E_n$ , we need to determine whether the majority of the gates that feed into it evaluate to 1. (Note that all of the gates in  $D_n$  are MAJORITY gates.) That is, we need to determine whether it is the case that for most bit strings  $G$  such that  $G$  is the name of a gate that is connected to  $F$ ,  $(G, P, 1)$  is in  $L_d$ . This is clearly computable in  $\text{PP}^{L_d}$ .

Thus in order to compute BitSLP, given program  $P$  and index  $i$ , compute the name  $F$  of the output bit of  $E_n$  that produces the  $i$ th bit of  $N$  (which is easy because of the uniformity of the circuits  $D_{2^{2^n}}$ ) and determine if  $(F, P, 1) \in L_d$ , where  $d$  is determined by the depth of the constant-depth family of circuits presented in [39].  $\square$

Theorem 4.1 shows that  $\text{BP}(\text{P}_{\mathbb{R}}^0)$  lies in CH. A similar argument can be applied to an analogous restriction of “digital”  $\text{NP}_{\mathbb{R}}$  (i.e., where nondeterministic machines over the reals can guess “bits” but cannot guess arbitrary real numbers). Bürgisser and Cucker [20] present some problems in PSPACE that are related to *counting* problems over  $\mathbb{R}$ . It would be interesting to know whether these problems lie in CH.

Although Theorem 4.1 shows that BitSLP and PosSLP both lie in CH, some additional effort is required in order to determine the level of CH where these problems reside. We present a more detailed analysis for PosSLP, since it is our main concern in this paper. (A similar analysis can be carried out for BitSLP, showing that it lies in  $\text{PH}^{\text{PPPPPPPP}}$  [7].)

The following result implies Theorem 1.3, since Toda's theorem [63] shows that  $\text{PP}^{\text{PH}^A} \subseteq \text{P}^{\text{PP}^A}$  for every oracle  $A$ .

THEOREM 4.2.  $\text{PosSLP} \in \text{PH}^{\text{PPPP}}$ .

*Proof.* We will use the Chinese remaindering algorithm of [39] to obtain our upper bound on PosSLP. (Related algorithms, which do not lead directly to the bound reported here, have been used on several occasions [2, 28, 33, 48, 49].) Let us introduce some notation relating to Chinese remaindering.  $M_n = \sum_{p \leq 2^{n^2}} p$

For  $n \in \mathbb{N}$  let  $M_n$  be the product of all odd primes  $p$  less than  $2^{n^2}$ . By the prime number theorem,  $2^{2^n} < M_n < 2^{2^{n^2+1}}$  for  $n$  sufficiently large. For such primes  $p$  let  $h_{p,n}$  denote the inverse of  $M_n/p \bmod p$ .  $\frac{h_m \cdot h_{p,n}}{p} \equiv 1 \bmod p$

Any integer  $0 \leq X < M_n$  can be represented uniquely as a list  $(x_p)$ , where  $p$  runs over the odd primes  $p < 2^{n^2}$  and  $x_p = X \bmod p$ . Moreover,  $X$  is congruent to  $\sum_p x_p h_{p,n} M_n/p$  modulo  $M_n$ . Hence  $X/M_n$  is the fractional part of  $\sum_p x_p h_{p,n}/p$ .

Define the family of approximation functions  $\text{app}_n(X)$  to be  $\sum_p B_p$ , where  $B_p = x_p h_{p,n} \sigma_{p,n}$  and  $\sigma_{p,n}$  is the result of truncating the binary expansion of  $1/p$  after  $2^{n^4}$  bits. Note that for  $n$  sufficiently large and  $X < M_n$ ,  $\text{app}_n(X)$  is within  $2^{-2^{n^3}}$  of  $X/M_n$ .

Let the input to PosSLP be a program  $P$  of size  $n$  representing the integer  $W$ ,

$$\left. \begin{array}{l} \text{PosSLP} \in \text{PH}^A \\ A \in \text{PH}^{\text{PP}^B} \\ B \in \text{PH}^{\text{PP}} \end{array} \right\} \Rightarrow A \in \text{PH}^{\text{PPPPPPPP}}$$

$$\left[ \begin{array}{l} \text{PH} \subseteq \text{P}^{\text{PP}} \text{ (Toda)} \\ \text{PH}^{\text{PP}} \subseteq \text{P}^{\text{PP}} \text{ as well (!)} \\ \text{PP}^{\text{PHPP}} \subseteq \text{PP}^{\text{PPPP}} \subseteq \text{PP}^{\text{PP}} \end{array} \right]$$

$$\begin{array}{l} \text{NP}^{\text{PP}} \subseteq \text{P}^{\text{PPPP}} \\ \uparrow \checkmark \\ \text{NP} \subseteq \text{P}^{\text{PP}} \\ \Downarrow ? \\ \text{NP}^{\text{PP}} \subseteq (\text{P}^{\text{PP}})^{\text{PP}} \\ \subseteq \text{P}^{\text{PPPPPP}} \\ \subseteq \text{P}^{\text{PP}} \end{array}$$

$$\boxed{\text{PP}^{\text{PH}^A} \subseteq \text{P}^{\text{PP}^A}} \Rightarrow \text{PH}^{\text{PP}^{\text{PH}^{\text{PP}}}} \subseteq \text{PH}^{\text{P}^{\text{PP}^{\text{PP}}}} \subseteq \text{PH}^{\text{PP}^{\text{PP}}}$$

and set  $Y_n = 2^{2^n}$ . Since  $|W| \leq Y_n$ , the number  $X := W + Y_n$  is nonnegative, and we can easily transform  $P$  into a program of size  $2n + 2$  representing  $X$ . Clearly,  $W > 0$  iff  $X > Y_n$ . Note that if  $X > Y_n$ , then  $X/M_n$  and  $Y_n/M_n$  differ by at least  $1/M_n > 2^{-2^{n^2+1}}$ , which implies that it is enough to compare the binary expansions of  $\text{app}_n(X)$  and  $\text{app}_n(Y_n)$ . (Interestingly, this seems to be somewhat easier than computing the bits of  $X$  directly.)

We can determine whether  $X > Y_n$  in  $\text{PH}$  relative to the following oracle  $A$ :  $A = \{(P, j, b, 1^n) : \text{the } j\text{th bit of the binary expansion of } \text{app}_n(X) \text{ is } b, \text{ where } X \text{ is the number represented by straight-line program } P \text{ and } j \text{ is given in binary}\}$ .

Lemma 4.3 completes the proof by showing that  $A \in \text{PH}^{\text{PP}^{\text{PP}}}$ .  $\square$

LEMMA 4.3.  $A \in \text{PH}^{\text{PP}^{\text{PP}}}$ .

*Proof.* Assume for the moment that we can show that  $B \in \text{PH}^{\text{PP}}$ , where  $B := \{(P, j, b, p, 1^n) : \text{the } j\text{th bit of the binary expansion of } B_p (= x_p h_{p,n} \sigma_{p,n}) \text{ is } b, \text{ where } p < 2^{n^2} \text{ is an odd prime, } x_p = X \bmod p, X \text{ is the number represented by the straight-line program } P, \text{ and } j \text{ is given in binary}\}$ . In order to recognize the set  $A$ , it clearly suffices to compute  $2^{n^4}$  bits of the binary representation of the sum of the numbers  $B_p$ . A uniform circuit family for the iterated sum is presented by Maciel and Thérien in [50, Corollary 3.4.2] consisting of MAJORITY gates on the bottom (input) level, with three levels of AND and OR gates above. As in the proof of Theorem 4.1, the construction of Maciel and Thérien immediately yields a  $\text{PH}^{\text{PP}^B}$  algorithm for  $A$ , by simulating the MAJORITY gates by  $\text{PP}^B$  computation, simulating the OR gates above the MAJORITY gates by  $\text{NP}^{\text{PP}^B}$  computation, etc. The claim follows, since by Toda's theorem [63],  $\text{PH}^{\text{PP}^B} \subseteq \text{PH}^{\text{PP}^{\text{PH}^{\text{PP}}}} = \text{PH}^{\text{PP}^{\text{PP}}}$ . It remains only to show that  $B \in \text{PH}^{\text{PP}}$ .  $\square$

LEMMA 4.4.  $B \in \text{PH}^{\text{PP}}$ .

*Proof.* Observe that, given  $(P, j, b, p)$ , we can determine in polynomial time whether  $p$  is prime [4], and we can compute  $x_p$ .

In  $\text{PH} \subseteq \text{P}^{\text{PP}}$  we can find the least generator  $g_p$  of the multiplicative group of the integers mod  $p$ . The set  $C = \{(q, g_p, i, p) : p \neq q \text{ are primes and } i \text{ is the least number for which } g_p^i \equiv q \bmod p\}$  is easily seen to lie in  $\text{PH}$ . We can compute the discrete log base  $g_p$  of the number  $M_n/p \bmod p$  in  $\#\text{P}^C \subseteq \text{P}^{\text{PP}}$  by the algorithm that nondeterministically guesses  $q$  and  $i$ , verifies that  $(q, g_p, i, p) \in C$ , and if so generates  $i$  accepting paths. Thus we can compute the number  $M_n/p \bmod p$  itself in  $\text{P}^{\text{PP}}$  by first computing its discrete log, and then computing  $g_p$  to that power, mod  $p$ . The inverse  $h_{p,n}$  is now easy to compute in  $\text{P}^{\text{PP}}$ , by finding the inverse of  $M_n/p \bmod p$ .

Our goal is to compute the  $j$ th bit of the binary expansion of  $x_p h_{p,n} \sigma_{p,n}$ . We have already computed  $x_p$  and  $h_{p,n}$  in  $\text{P}^{\text{PP}}$ , so it is easy to compute  $x_p h_{p,n}$ . The  $j$ th bit of  $1/p$  is 1 iff  $2^j \bmod p$  is odd, so bits of  $\sigma_{p,n}$  are easy to compute in polynomial time. (Note that  $j$  is exponentially large.)

Thus our task is to obtain the  $j$ th bit of the product of  $x_p h_{p,n}$  and  $\sigma_{p,n}$ , or (equivalently) adding  $\sigma_{p,n}$  to itself  $x_p h_{p,n}$  times. The problem of adding  $\log^{O(1)} n$  many  $n$ -bit numbers lies in uniform  $\text{AC}^0$  [32]. Simulating these  $\text{AC}^0$  circuits leads to the desired  $\text{PH}^{\text{PP}}$  algorithm for  $B$ .  $\square$

**5. An observation on derandomizing ACIT.** The connections between algebraic complexity and the counting hierarchy in the preceding section were first introduced in an earlier version of this paper [5]. Recently, these connections have led to further developments. Bürgisser shows in [23] that the counting hierarchy provides



a useful tool for showing implications among several hypotheses in algebraic complexity theory that were not previously known to be related. In that same paper, he also improves a theorem of Koiran, relating the arithmetic circuit complexity of the permanent to a frequently studied question about the complexity of expressing  $n!$ . We have some new observations to present on this topic, and we start by recalling some background and definitions.

We will follow the terminology of Shub and Smale [59], and say that  $n!$  is “easy” if there is a sequence of SLPs  $C_n$  of size  $\log^{O(1)} n$ , where  $C_n$  represents the number  $n!$ . Following the same convention, we say that  $n!$  is “ultimately easy” if there is a sequence of SLPs  $C_n$  of size  $\log^{O(1)} n$ , where  $C_n$  represents a nonzero multiple of the number  $n!$ . (It does not matter which multiple is represented.) Shub and Smale conjectured that  $n!$  is not ultimately easy, and they showed that this condition implies that  $P_C \neq NP_C$ . It is also pointed out in [12] that if factoring is sufficiently hard to compute, it implies that  $n!$  is not easy. There are a number of papers that touch on the questions of whether or not  $n!$  is easy or ultimately easy. The reader is referred to [25, 23, 12] for more references. A goal of this section is to relate these questions to the complexity of ACIT.

Note that if  $n!$  is not ultimately easy, it says merely that there are *infinitely many*  $n$  for which multiples of  $n!$  require large circuits. It may be useful also to consider the hypothesis that this condition holds for *all* large  $n$ ; that is, for all  $k$  there is an  $m$  such that for all  $n > m$  there is no SLP of size  $\log^k n$  representing a nonzero multiple of  $n!$ . Let us call this condition “ $n!$  is ultimately hard.”

The following implications are known to hold:

$$\begin{aligned} n! \text{ is ultimately hard} &\Rightarrow n! \text{ is not ultimately easy} \Rightarrow n! \text{ is not easy} \\ &\Rightarrow \text{the permanent requires arithmetic circuits of superpolynomial size} \Rightarrow \text{AFIT} \\ &\quad \in \bigcap_{\epsilon > 0} \text{io-}[\text{DTIME}(2^{n^\epsilon})], \end{aligned}$$

where  $\text{io-}[\text{DTIME}(t(n))]$  denotes the class of problems  $A$  for which there is a deterministic algorithm running in time  $t(n)$  that solves  $A$  correctly for all instances of length  $n$ , for infinitely many  $n$ , and where AFIT denotes arithmetic formula identity testing: a special case of ACIT. The third implication is from [23], the fourth is from [42, Theorem 7.7]. Derandomization results such as those of [42] usually come in two flavors. If one assumes that a particular function (such as the permanent) is hard on infinitely many input lengths, then one obtains only algorithms that work correctly on infinitely many input lengths. One can also obtain an algorithm that works correctly on all input lengths if one starts with a stronger assumption, such as that the permanent requires large circuits on all input lengths.

It has not been known whether any of these hypotheses are sufficiently strong to derandomize ACIT itself, although it is known that if ACIT is in  $\bigcap_{\epsilon > 0} \text{DTIME}(2^{n^\epsilon})$  (or even in  $\bigcap_{\epsilon > 0} \text{NTIME}(2^{n^\epsilon})$ ), then either the permanent requires arithmetic circuits of superpolynomial size or  $\text{NEXP} \not\subseteq P/\text{poly}$  [42]. We observe now that the following implication holds.

**PROPOSITION 5.1.** *We have the following:*

1. *If  $n!$  is ultimately hard, then  $\text{ACIT} \in \bigcap_{\epsilon > 0} \text{DTIME}(2^{n^\epsilon})$ .*
2. *If  $n!$  is not ultimately easy, then  $\text{ACIT} \in \bigcap_{\epsilon > 0} \text{io-}[\text{DTIME}(2^{n^\epsilon})]$ .*

*Proof.* We prove only the second claim. The first is easier and follows by the same method.

First note that, by Proposition 2.2, it is sufficient to prove the implication for EquSLP instead of ACIT. Assume that  $n!$  is not ultimately easy. Then for every  $k$

there is an infinite set  $I(k)$  of numbers such that for all  $m \in I(k)$  no SLP of size at most  $\log^k m$  can produce a nonzero multiple of  $m!$ .

Given  $\epsilon > 0$ , pick any  $\gamma$  such that  $0 < \gamma < \epsilon$ . Choose  $k$  to be the least integer larger than  $1/\gamma$ . For any  $m \in I(k)$  set  $n = \lfloor \log^k m \rfloor$ .

Suppose we are given as input an SLP  $C$  of size  $n$ . Note that the binary encoding of  $m$  has length at most  $n^{1/k}$ —but we do not know what  $m$  is. Thus we try all numbers  $z$  having binary encoding of length at most  $n^{1/k}$  (one of which will be  $m$ ). We then compute the binary representation of  $z!$  with the obvious algorithm, which takes time at most  $z^2 \log^{O(1)} z$ , which is less than  $2^{n^\gamma}$  for sufficiently large  $n$ . Then we evaluate the SLP  $C$  modulo  $z!$ ; we accept iff the result is zero for all of the numbers  $z$ . This algorithm works correctly, since by our assumption, the SLP  $C$  cannot produce a nonzero multiple of  $m!$ . The running time is  $2^{O(n^\gamma)} 2^{O(n^\gamma)}$ , which is less than  $2^{n^\epsilon}$  for all large  $n$ .  $\square$

We remark that this proof makes use of no special properties of the factorial function. As one of the referees has pointed out to us, the same upper bound follows if there is any sequence of numbers  $(a(n))$  such that the binary representation of  $a(n)$  can be computed from  $n$  in time polynomial in  $m$ , the length of the binary representation of  $a(n)$ , such that no multiple of  $a(n)$  can be represented by an arithmetic circuit of size  $\log^{O(1)} m$ . If we drop the requirement that  $a(n)$  be computable in time polynomial in  $m$ , then a simple counting argument (or Kolmogorov complexity argument) shows that *most* numbers  $a(n)$  have this property.

**6. Closing remarks.** NP-hardness is firmly established as a useful tool for providing evidence of intractibility. We believe that **PosSLP can become a useful tool for providing evidence of intractibility for problems that do not appear to be NP-hard** and for providing evidence that certain problems do not lie in NP or reduce to NP. Indeed, results of this flavor have already started to appear: **Etessami and Yannakakis have recently shown that PosSLP reduces to the problem of finding mixed strategy profiles close to exact Nash equilibria in three-person games** [35]; i.e., they show that this fundamental but very challenging numerical problem of computational game theory is PosSLP-hard. We may regard this PosSLP-hardness result as evidence that the problem is not NP-easy. In contrast, the related, weaker, and much less elusive notion of computing a strategy profile approximately satisfying the equilibrium conditions is trivially NP-easy. It would be most interesting to establish similar PosSLP-hardness results for other natural numerical problems in the computational sciences (e.g., computational physics) for which no efficient and “fool-proof” methods, even nondeterministic ones, are known but which also do not appear to be NP-hard.

There are several directions for further research suggested by the results that we have presented. We would very much like to see a resolution of our Conjecture 1, and we think that it is likely that PosSLP lies at a lower level of the counting hierarchy than is proved in Theorem 1.3. Perhaps better upper bounds can be presented at least for the sum-of-square-roots problem. Can better evidence be presented for the intractibility of PosSLP? **Can some important problems in  $\text{NP}_{\mathbb{R}}$  (such as the existential theory of the reals) be shown to lie in the counting hierarchy?**

**Acknowledgments.** We acknowledge helpful conversations with Kousha Etessami, Sambuddha Roy, Felipe Cucker, Lenore Blum, Richard Lipton, Parikshit Gopalan, Mark Braverman, Madhu Sudan, Klaus Meer, Pascal Koiran, Qi Cheng, James Demmel, Salil Vadhan, Fengming Wang, Valentine Kabanets, Neeraj Kayal, and Kristoffer Arnsfelt Hansen.

## REFERENCES

- [1] L. ADLEMAN, *Two theorems on random polynomial time*, in Proceedings of the 19th Annual IEEE Symposium on Foundations of Computer Science, IEEE Press, Piscataway, NJ, 1978, pp. 75–83.
- [2] M. AGRAWAL, E. ALLENDER, AND S. DATTA, *On  $TC^0$ ,  $AC^0$ , and arithmetic circuits*, J. Comput. System Sci., 60 (2000), pp. 395–421.
- [3] M. AGRAWAL AND S. BISWAS, *Primality and identity testing via chinese remaindering*, J. ACM, 50 (2003), pp. 429–443.
- [4] M. AGRAWAL, N. KAYAL, AND N. SAXENA, *PRIMES is in P*, Ann. of Math., 160 (2004), pp. 781–793.
- [5] E. ALLENDER, P. BÜRGISSEER, J. KJELDGAARD-PEDERSEN, AND P. B. MILTERSEN, *On the complexity of numerical analysis*, in Proceedings of the 21st Annual IEEE Conference on Computational Complexity (CCC '06), IEEE Press, Piscataway, NJ, 2006, pp. 331–339.
- [6] E. ALLENDER, M. KOUCKÝ, D. RONNEBURGER, S. ROY, AND V. VINAY, *Time-space tradeoffs in the counting hierarchy*, in Proceedings of the 16th Annual IEEE Conference on Computational Complexity (CCC '01), IEEE Press, Piscataway, NJ, 2001, pp. 295–302.
- [7] E. ALLENDER AND H. SCHNORR, *The Complexity of the BitSLP Problem*, manuscript, Department of Computer Science, Rutgers University, 2005.
- [8] E. ALLENDER AND K. W. WAGNER, *Counting hierarchies: Polynomial time and constant depth circuits*, in Current Trends in Theoretical Computer Science, G. Rozenberg and A. Salomaa, eds., World Scientific, River Edge, NJ, 1993, pp. 469–483.
- [9] S. BERKOWITZ, *On computing the determinant in small parallel time using a small number of processors*, Inform. Process. Lett., 18 (1984), pp. 147–150.
- [10] A. BERTONI, G. MAURI, AND N. SABADINI, *Simulations among classes of random access machines and equivalence among numbers succinctly represented*, Ann. Discrete Math., 25 (1985), pp. 65–90.
- [11] L. BLUM, F. CUCKER, M. SHUB, AND S. SMALE, *Algebraic settings for the problem “ $P \neq NP$ ?”*, in The Mathematics of Numerical Analysis, Lectures in Appl. Math. 32, AMS, Providence, RI, 1996, pp. 125–144.
- [12] L. BLUM, F. CUCKER, M. SHUB, AND S. SMALE, *Complexity and Real Computation*, Springer, New York, 1998.
- [13] L. BLUM, *Computing over the reals: Where Turing meets Newton*, Notices Amer. Math. Soc., 51 (2004), pp. 1024–1034.
- [14] J. M. BORWEIN AND P. B. BORWEIN, *On the complexity of familiar functions and numbers*, SIAM Rev., 30 (1988), pp. 589–601.
- [15] J. M. BORWEIN AND P. B. BORWEIN, *Pi and the AGM, A study in analytic number theory and computational complexity*, Canadian Mathematical Society Series of Monographs and Advanced Texts, John Wiley & Sons Inc., New York, 1987.
- [16] M. BRAVERMAN AND S. COOK, *Computing over the reals: Foundations for scientific computing*, Notices Amer. Math. Soc., 55 (2006), pp. 318–329.
- [17] M. BRAVERMAN, *On the complexity of real functions*, in Proceedings of the 46th Annual IEEE Symposium on Foundations of Computer Science, IEEE Press, Piscataway, NJ, 2005, pp. 155–164.
- [18] R. P. BRENT, *Fast multiple-precision evaluation of elementary functions*, J. ACM, 23 (1976), pp. 242–251.
- [19] M. BRONSTEIN, *Symbolic integration. I, Transcendental functions*, Algorithms Comput. Math. 1, Springer-Verlag, Berlin, 1997.
- [20] P. BÜRGISSEER AND F. CUCKER, *Counting complexity classes for numeric computations II: Algebraic and semialgebraic sets*, J. Complexity, 22 (2006), pp. 147–191.
- [21] P. BÜRGISSEER, *Completeness and Reduction in Algebraic Complexity Theory*, Algorithms Comput. Math. 7, Springer-Verlag, Berlin, 2000.
- [22] P. BÜRGISSEER, *The complexity of factors of multivariate polynomials*, Found. Comput. Math., 4 (2004), pp. 369–396.
- [23] P. BÜRGISSEER, *On defining integers in the counting hierarchy and proving lower bounds in algebraic complexity*, in Proceedings of the 24th Annual Symposium on Theoretical Aspects of Computer Science (STACS'07), W. Thomas and P. Weil, eds., Lecture Notes in Comput. Sci. 44394, Springer, New York, 2007, pp. 133–144.
- [24] O. CHAPUIS AND P. KOIRAN, *Saturation and stability in the theory of computation over the reals*, Ann. Pure Appl. Logic, 99 (1999), pp. 1–49.
- [25] Q. CHENG, *On the ultimate complexity of factorials*, Theoret. Comput. Sci., 326 (2004), pp. 419–429.

- [26] D. COX, J. LITTLE, AND D. O'SHEA, *Ideals, Varieties, and Algorithms*, Springer, New York, 1991.
- [27] F. CUCKER AND D. GRIGORIEV, *On the power of real Turing machines over binary inputs*, SIAM J. Comput., 26 (1997), pp. 243–254.
- [28] G. I. DAVIDA AND B. LITOW, *Fast parallel arithmetic via modular representation*, SIAM J. Comput., 20 (1991), pp. 756–765.
- [29] R. DEMILLO AND R. LIPTON, *A probabilistic remark on algebraic program testing*, Inform. Process. Lett., 7 (1978), pp. 193–195.
- [30] J. DEMMEL AND P. KOEV, *Accurate and efficient algorithms for floating point computation*, in Applied Mathematics Entering the 21st Century: Invited Talks from the ICIAM 2003 Congress, J. M. Hill and R. Moore, eds., Proc. Appl. Math. 116, SIAM, Philadelphia, 2004, pp. 73–90.
- [31] J. DEMMEL, *The complexity of accurate floating point computation*, in Proceedings of the 2002 International Congress of Mathematicians, 2002, vol. 3, pp. 697–706.
- [32] L. DENENBERG, Y. GUREVICH, AND S. SHELAH, *Definability by constant-depth polynomial-size circuits*, Inform. and Control, 70 (1986), pp. 216–240.
- [33] P. F. DIETZ, I. I. MACARIE, AND J. I. SEIFERAS, *Bits and relative order from residues, space efficiently*, Inform. Process. Lett., 50 (1994), pp. 123–127.
- [34] K. ETESSAMI AND M. YANNAKAKIS, *Recursive Markov chains, stochastic grammars, and monotone systems of nonlinear equations*, in Proceedings of the 22nd Annual Symposium on Theoretical Aspects of Computer Science (STACS'05), V. Diekert and B. Durand, eds., Lecture Notes in Comput. Sci. 3404, Springer, New York, 2005, pp. 340–352.
- [35] K. ETESSAMI AND M. YANNAKAKIS, *On the complexity of Nash equilibria and other fixed points*, in Proceedings of the 48th Annual IEEE Symposium on Foundations of Computer Science, IEEE Press, Piscataway, NJ, 2007, pp. 113–123.
- [36] M. GAREY, R. L. GRAHAM, AND D. S. JOHNSON, *Some NP-complete geometric problems*, in Proceedings of the ACM Symposium on Theory Computations, ACM, New York, 1976, pp. 10–22.
- [37] J. HARTMANIS AND J. SIMON, *On the power of multiplication in random-access machines*, in Proceedings of the 15th Annual IEEE Symposium on Switching Automata Theory, IEEE Press, Piscataway, NJ, 1974, pp. 13–23.
- [38] J. HEINTZ AND C. P. SCHNORR, *Testing polynomials which are hard to compute*, in Logic and Algorithmic: An International Symposium Held in Honor of Ernst Specker, Monogr. No. 30 de l'Enseign. Math., University of Geneva, Geneva, Switzerland, 1982, pp. 237–254.
- [39] W. HESSE, E. ALLENDER, AND D. A. MIX BARRINGTON, *Uniform constant-depth threshold circuits for division and iterated multiplication*, J. Comput. System Sci., 65 (2002), pp. 695–716.
- [40] M. HIRVENSALO AND J. KARHUMÄKI, *Computing partial information out of intractable one—The first digit of  $2^n$  at base 3 as an example*, in Proceedings of the 27th International Symposium on Mathematical Foundations of Computer Science (MFCS), Lecture Notes in Comput. Sci. 2420, Springer, New York, 2002, pp. 319–327.
- [41] O. H. IBARRA AND S. MORAN, *Equivalence of straight-line programs*, J. ACM, 30 (1983), pp. 217–228.
- [42] V. KABANETS AND R. IMPAGLIAZZO, *Derandomizing polynomial identity tests means proving circuit lower bounds*, Comput. Complexity, 13 (2004), pp. 1–46.
- [43] P. KOIRAN AND S. PERIFEL, *The complexity of two problems on arithmetic circuits*, Theoret. Comput. Sci., 389 (2007), pp. 172–181.
- [44] P. KOIRAN, *Computing over the reals with addition and order*, Theoret. Comput. Sci., 133 (1994), pp. 35–47.
- [45] P. KOIRAN, *Elimination of constants from machines over algebraically closed fields*, J. Complexity, 13 (1997), pp. 65–82.
- [46] H. T. KUNG AND J. F. TRAUB, *All algebraic functions can be computed fast*, J. ACM, 25 (1978), pp. 245–260.
- [47] R. LIPTON AND N. VISHNOI, *Deterministic identity testing for multivariate polynomials*, in Proceedings of the Fourteenth ACM-SIAM Symposium on Discrete Algorithms (SODA), Baltimore, MD, 2003, SIAM, Philadelphia, 2003, pp. 756–760.
- [48] B. LITOW, *On iterated integer product*, Inform. Process. Lett., 42 (1992), pp. 269–272.
- [49] I. I. MACARIE, *Space-efficient deterministic simulation of probabilistic automata*, SIAM J. Comput., 27 (1998), pp. 448–465.
- [50] A. MACIEL AND D. THÉRIEN, *Threshold circuits of small majority-depth*, Inform. and Comput., 146 (1998), pp. 55–83.

- [51] G. MALAJOVICH, *An Effective Version of Kronecker's Theorem on Simultaneous Diophantine Approximation*, Technical report, Department of Mathematics, City University of Hong Kong, Hong Kong, 1996.
- [52] J. O'ROURKE, *Advanced problem* 6369, Amer. Math. Monthly, 88 (1981), p. 769.
- [53] J. O'ROURKE, The Open Problems Project, webpage at <http://maven.smith.edu/~orourke/TOPP>.
- [54] M. RAMANA, *An exact duality theory for semidefinite programming and its complexity implications*, Math. Program., 77 (1997), pp. 129–162.
- [55] S. M. RUMP, *Polynomial minimum root separation*, Math. Comp., 33 (1979), pp. 327–336.
- [56] E. SALAMIN, *Computation of  $\pi$  using arithmetic-geometric mean*, Math. Comp., 30 (1976), pp. 565–570.
- [57] A. SCHÖNHAGE, *On the power of random access machines*, in Automata, Languages and Programming ICALP'79, H.A. Maurer, ed., Lecture Notes in Comput. Sci. 71, Springer, New York, 1979, pp. 520–529.
- [58] J. T. SCHWARTZ, *Fast probabilistic algorithms for verification of polynomial identities*, J. ACM, 27 (1980), pp. 701–717.
- [59] M. SHUB AND S. SMALE, *On the intractability of Hilbert's Nullstellensatz and an algebraic version of "P=NP"*, Duke Math. J., 81 (1996), pp. 47–54.
- [60] V. STRASSEN, *Polynomials with rational coefficients which are hard to compute*, SIAM J. Comput., 3 (1974), pp. 128–149.
- [61] S. P. TARASOV AND M. N. VYALYI, *Semidefinite programming and arithmetic circuit evaluation*, Discrete Appl. Math., 156 (2008), pp. 2070–2078.
- [62] P. TIWARI, *A problem that is easier to solve on the unit-cost algebraic RAM*, J. Complexity, 8 (1992), pp. 393–397.
- [63] S. TODA, *PP is as hard as the polynomial-time hierarchy*, SIAM J. Comput., 20 (1991), pp. 865–877.
- [64] J. TORÁN, *Complexity classes defined by counting quantifiers*, J. ACM, 38 (1991), pp. 753–774.
- [65] L. G. VALIANT, *Reducibility by Algebraic Projections*, in Logic and Algorithmic: An International Symposium Held in Honor of Ernst Specker, Monogr. No. 30 de l'Enseign. Math., University of Geneva, Geneva, Switzerland, 1982, pp. 365–380.
- [66] K. W. WAGNER, *The complexity of combinatorial problems with succinct input representation*, Acta Inform., 23 (1986), pp. 325–356.
- [67] K. WEIHRAUCH, *Computable Analysis*, Springer-Verlag, Berlin, 2000.
- [68] H. WOZNIAKOWSKI, *Why does information-based complexity use the real number model?*, Theoret. Comput. Sci., 219 (1999), pp. 451–465.
- [69] R. E. B. ZIPPEL, *Simplification of Radicals with Applications to Solving Polynomial Equations*, Master's thesis, Electrical Engineering and Computer Science Department, M.I.T., Cambridge, MA, 1977.

$\text{Eqv SLP} \in \text{CoRP}$ ,  
via computation  
modulo large primes.

introduction of CH