UNCOMPUTABLY LARGE INTEGRAL POINTS ON ALGEBRAIC PLANE CURVES?

J. MAURICE ROJAS

Dedicated to Professor Manuel Blum on the occassion of his $60^{\underline{\text{th}}}$ *birthday.*

Abstract. We show that the decidability of an amplification of Hilbert's Tenth Problem in three variables implies the existence of uncomputably large integral points on certain algebraic curves. We obtain this as a corollary of a new positive complexity result: the Diophantine prefix $\exists\forall\exists$ is **generically** decidable. This means that we give a precise geometric classification of those polynomials $f \in \mathbb{Z}[v, x, y]$ for which the question

$$\exists v \in \mathbb{N} \text{ such that } \forall x \in \mathbb{N} \;\; \exists y \in \mathbb{N} \text{ with } f(v, x, y) = 0?$$

may be undecidable, and we show that this set of polynomials is quite small in a rigourous sense. (The decidability of $\exists\forall\exists$ was previously an open question.) We also show that if integral points on curves **can** be bounded effectively, then $\exists\exists\forall\exists$ is generically decidable as well. We thus obtain a connection between the decidability of certain Diophantine problems, height bounds for points on curves, and the geometry of certain complex surfaces and 3-folds.

1. Introduction

We derive new complexity-theoretic limits on what can be discerned about the set of integral points of a variety of low dimension. In particular, we exhibit a new family of decidable Diophantine sentences related to the remaining open cases of Hilbert's Tenth Problem. As a corollary, we obtain a Diophantine problem whose decidability implies the following surprising assertion: for a general algebraic plane curve $\{(x, y) \in \mathbb{C} \mid f(x, y) = 0\}$, it is impossible to express the size of the largest positive integral point as a Turing computable function of the degree and coefficient sizes of f.

Finding such bounds is literally one of the holy grails of number theory. Huge, but nevertheless computable, upper bounds have already been found for a number of important classes of curves, such as curves of genus one [BC70], Thue curves [Bak68], hyperelliptic curves [Bak69], superelliptic curves [Bri84], and certain rational curves [Pou93].[1] For example, it is known that for any polynomial equation of the form

$$y^2 = a + bx + cx^2 + dx^3,$$

Date: November 20, 1998.

1991 *Mathematics Subject Classification.* 03D35, 11D72, 14G99 (Primary); 11G30, 14H99, 14J26 (Secondary).

⋆ In: *Theoretical Computer Science*, special issue in honor of Professor Manuel Blum's $60^{\underline{\text{th}}}$ birthday, vol. 235, March, 2000. Also available from `http://xxx.lanl.gov/math.AG/9809009`.

Partially supported by a National Science Foundation Mathematical Sciences Postdoctoral Fellowship and a Hong Kong CERG Grant.

[1]By a **curve** (resp. **surface** or **3-fold**) we will always mean a one-dimensional (resp. two-dimensional or three-dimensional) **complex** zero set of some set of polynomial equations.

where $a, b, c, d \in \mathbb{Z}$ and $a+bx+cx^2+dx^3$ has three distinct complex roots, all **integral** solutions must satisfy

$$|x|, |y| \leq \exp((10^6 H)^{10^6}),$$

where H is any upper bound on $|a|, |b|, |c|, |d|$ [Bak75].[2]

However, finding such bounds, even ones monstrously larger than those already known, for **general** algebraic curves has been out of reach for decades. Furthermore, the analogous question for algebraic surfaces, even in $\mathbb{C}^3$, has so far been addressed only through deep conjectures of Lang and Vojta [Lan83, Voj87].

Our first main theorem relates the decidability of certain Diophantine sentences in four variables with the computability of upper bounds on the size of integral points on algebraic curves. So let us briefly recall Hilbert's Tenth Problem in n variables:

"Decide whether an arbitrary $\boldsymbol{f \in \mathbb{Z}[x_1, \ldots, x_n]}$ has an integral root or not."

We will denote this well-known Diophantine problem by $\boldsymbol{\mathcal{HTP}_{\mathbb{Z}}(n)}$. Similarly, the analogous problem where we wish to determine the existence of an integral root, with all coordinates **positive**, will be denoted by $\boldsymbol{\mathcal{HTP}_{\mathbb{N}}(n)}$. We will also need the following closely related functions.

Definition 1. *For any subset $R \subseteq \mathbb{C}$ closed under addition and multiplication, define the functions*

$$\mathbf{Big}_{R,n}, \mathbf{ExactCard}_{R,n} : \mathbb{Z}[x_1, \ldots, x_n] \longrightarrow \mathbb{N} \cup \{0, \infty\}$$

as follows: Let S_f be the hypersurface $\{(x_1, \ldots, x_n) \in \mathbb{C}^n \mid f(x_1, \ldots, x_n) = 0\}$. Then $\mathbf{Big}_{R,n}(f)$ is the supremum of $\max\{|r_1|, \ldots, |r_n|\}$ as $(r_1, \ldots, r_n)$ ranges over $\{(0, \ldots, 0)\}$ and the set of all points of S_f in R^n. Finally, $\mathbf{ExactCard}_{R,n}(f)$ is the number of points of S_f in R^n.

It is not hard to see that the decidability of $\mathcal{HTP}_{\mathbb{N}}(n)$ implies the decidability of $\mathcal{HTP}_{\mathbb{Z}}(n)$, so $\mathcal{HTP}_{\mathbb{N}}(n)$ is at least as hard as $\mathcal{HTP}_{\mathbb{Z}}(n)$. Similarly, the computability of $\mathbf{Big}_{\mathbb{N},n}$ (resp. $\mathbf{ExactCard}_{\mathbb{N},n}$) easily implies the computability of $\mathbf{Big}_{\mathbb{Z},n}$ (resp. $\mathbf{ExactCard}_{\mathbb{Z},n}$). Also, via brute-force enumeration, it is easy to see that $\mathbf{ExactCard}_{\mathbb{N},n}$ (resp. $\mathbf{ExactCard}_{\mathbb{Z},n}$) is computable iff $\mathbf{Big}_{\mathbb{N},n}$ (resp. $\mathbf{Big}_{\mathbb{Z},n}$) is computable. However, we also have the following more subtle fact.

Main Theorem 1. *At least one of the following two statements is* **false***:*

1. *The function $\mathbf{Big}_{\mathbb{N},2}$ is Turing computable.*
2. *The Diophantine sentence*

   $$\exists u \in \mathbb{N} \;\; \exists v \in \mathbb{N} \;\; \forall x \in \mathbb{N} \;\; \exists y \in \mathbb{N} \text{ with } f(u, v, x, y) = 0$$

   is decidable in the special case where the underlying 3-fold S_f contains a surface which is a bundle of curves (each with a genus zero component) fibered over a curve C in the (u, v)-plane, where C has infinitely many positive integral points.

[2]For any integral point $(x, y) \in \mathbb{Z}^2$, the quantity $\max\{|x|, |y|\}$ is usually called the **height** of (x, y). Also, the preceding height bound has since been considerably improved, e.g., [Sch92].

In particular, $\mathcal{HTP}_{\mathbb{N}}(3)$ *is a special case of the problem mentioned in statement (2).*

The geometric notions mentioned above are clarified in section 2. Alternative classes of C for which Main Theorem 1 remains true are mentioned in sections 1.1 and 5.

We note that Alan Baker has conjectured [Jon81, Section 5] that $\mathcal{HTP}_{\mathbb{Z}}(2)$ is decidable. Thus the truth of statement (1) above would imply an algorithm for deciding $\mathcal{HTP}_{\mathbb{N}}(2)$, and thus a positive answer to Baker's conjecture as well. We also point out that the computability of $\mathbf{ExactCard}_{\mathbb{Z},2}$ (and $\mathbf{ExactCard}_{\mathbb{N},2}$) is **still** an open question, in spite of the fact that explicit (albeit huge) upper bounds on $\mathbf{ExactCard}_{\mathbb{Z},2}$ are known in many cases [Bom90, Pou93].

On the other hand, Z. W. Sun has proved that $\mathcal{HTP}_{\mathbb{Z}}(11)$ is undecidable [Sun92a]. Also, Y. V. Matiyasevich has shown (the proof appearing in a paper of J. P. Jones [Jon82]) that $\mathcal{HTP}_{\mathbb{N}}(9)$ is undecidable. However, although the decidability of $\mathcal{HTP}_{\mathbb{N}}(1)$ and $\mathcal{HTP}_{\mathbb{Z}}(1)$ is a simple algebraic exercise, the remaining cases of $\mathcal{HTP}_{\mathbb{N}}(n)$ and $\mathcal{HTP}_{\mathbb{Z}}(n)$, as of mid-1998, are still completely open.

Our result above thus tells us something new about the next harder (and open) cases of $\mathcal{HTP}_{\mathbb{N}}(n)$.

Remark 1. *The computability of* $\mathbf{Big}_{\mathbb{Z},n}$ *(resp.* $\mathbf{ExactCard}_{\mathbb{Z},n}$*) does* **not** *trivially imply the computability of* $\mathbf{Big}_{\mathbb{N},n}$ *(resp.* $\mathbf{ExactCard}_{\mathbb{N},n}$*): It is possible for* $\mathbf{Big}_{\mathbb{Z},n}(f)$ *(resp.* $\mathbf{ExactCard}_{\mathbb{Z},n}$*) to be infinite and thus give us no decisive information about the value of* $\mathbf{Big}_{\mathbb{N},n}(f)$ *(resp.* $\mathbf{ExactCard}_{\mathbb{N},n}$*).*

This connection between height bounds and Hilbert's Tenth Problem points to an unusual possibility: The search for general effective height bounds for integral points on algebraic curves may be futile. Indeed, it would have perhaps been more interesting to prove the statement "$\mathcal{HTP}_{\mathbb{N}}(3)$ is decidable $\Longrightarrow$ $\mathbf{Big}_{\mathbb{N},2}$ is uncomputable," or better still, "$\mathcal{HTP}_{\mathbb{Z}}(3)$ is decidable $\Longrightarrow$ $\mathbf{Big}_{\mathbb{Z},2}$ is uncomputable." However, Main Theorem 1 is at least a first step in this direction. We will comment further on strengthening Main Theorem 1 in the conclusion of this paper.

While our first main result is negative in the sense that it implies undecidability for certain Diophantine sentences, its proof follows easily from our derivation of two positive results on Diophantine sentences. To describe these results, let us introduce the following notation: We say that "the **Diophantine prefix** $\exists v \forall x \exists y$ is decidable" iff there is a Turing machine algorithm which decides the sentence

$$\exists v \forall x \exists y \text{ with } f(v,x,y)=0$$

for arbitrary input $f \in \mathbb{Z}[v,x,y]$, and where the quantification is over the **positive** integers. This notation extends in an obvious way to other combinations of quantifiers and variables such as $\exists v \exists y$, $\exists u \exists v \exists y$, etc. Finally, by **generic** decidability, we will mean that a prefix is decidable when the input is restricted to an a priori fixed "large" set. This is made more precise below and in section 2.

We will prove the following result.

Main Theorem 2. *The prefix $\exists v \forall x \exists y$ is* **generically** *decidable. More precisely, it is decidable on the collection of those f for which the underlying complex surface S_f does* **not** *have an irreducible component which is a bundle of curves (each with a genus zero component) fibered over the v-axis.*

By simply considering those polynomials in $\mathbb{Z}[v,y]$, note that the prefix $\exists v \exists y$ (or, equivalently, $\mathcal{HTP}_{\mathbb{N}}(2)$) is a special case of the prefix $\exists v \forall x \exists y$. It is also easy to see (cf. section 2) that the set of "hard" f **omitted** by our result above happens to include $\mathbb{Z}[v,y]$. Furthermore, via theorem 4 at the end of this section, we can algorithmically determine whether f satisfies the above hypothesis.

It should of course be pointed out that the decidability of $\exists\forall\exists$ was a completely open problem. In fact, J. P. Jones [Jon81] has conjectured that the prefixes $\exists\forall\exists$ and $\exists\exists$ are equivalent. Put another way, this is the conjecture that $\exists\forall\exists$ is decidable $\Longleftrightarrow \mathcal{HTP}_{\mathbb{N}}(2)$ is decidable. So while we still haven't resolved the decidability of $\exists\forall\exists$, we now at least know a geometric characterization of where any potential obstruction to decidability may lie. In particular, it follows from a fundamental result of algebraic geometry that our hypothesis rules out certain **ruled** surfaces, i.e., surfaces which are traced out by an infinite family of lines. The latter statement is also clarified in section 2.

Our final main theorem is a seemingly paradoxical extension of the preceding result.

Main Theorem 3. *The prefix $\exists u \exists v \forall x \exists y$ is decidable on the collection of f for which the underlying 3-fold S_f contains* **no** *surface which is a bundle of curves (each with a genus zero component) fibered over a curve in the (u,v)-plane.*

We can algorithmically determine whether f satisfies the preceding hypothesis as well, via theorem 4 at the end of this section. Also, if $\mathbf{Big}_{\mathbb{N},2}$ turns out to be computable, then we can further strengthen Main Theorem 3 by obtaining **generic** decidability for $\exists\exists\forall\exists$. This conditional result will follow easily from our geometric arguments later (cf. remark 6).

The "near paradox" arises from the following result of Y. V. Matiyasevich and Julia Robinson.[3]

The MR Theorem. [MR74] *The quantifier prefix $\exists\exists\forall\exists$ is* **un***decidable, i.e., there is no Turing machine which decides for an* **arbitrary** *input $f \in \mathbb{Z}[u,v,x,y]$ whether there is a $(u,v)\in\mathbb{N}^2$ such that $\forall x\ \exists y$ with $f(u,v,x,y)=0$.* ■

In any event, Main Theorem 3 gives us a necessary geometric condition classifying those f for which the above Diophantine sentence is undecidable. It is easy to see (cf. section 2) that this set of "hard" f includes the prefix $\exists u \exists v \exists y$ (i.e., the problem $\mathcal{HTP}_{\mathbb{N}}(3)$). However, this does **not** necessarily imply that the prefix $\exists u \exists v \exists y$ is undecidable — the undecidability of $\exists u \exists v \forall x \exists y$ may be due to **other** polynomials

[3]The paper [Jon81] contains many important results related to the MR Theorem, and for non-Russian readers may be a better reference than the original reference [MR74].

in our exceptional locus. We also emphasize that the set of exceptional f in Main Theorem 3 is strictly larger than the set of f considered in Main Theorem 1.

The proofs of Main Theorems 2 and 3 are not difficult conceptually, but rely upon results of C. Runge [Run87, Aya91], C. L. Siegel [Sie29], and A. Schinzel [Sch82] on the distribution of integral points on curves. The necessary results are stated in section 1.1. The application of these results then relies on combining a geometric construction with a new, more effective characterization of genus zero for algebraic curves. The following definition makes this more precise.

Definition 2. *Following the notation of definition 1, suppose $g \in \mathbb{C}[a_1, \ldots, a_m, x_1, \ldots, x_n]$ and let $a := (a_1, \ldots, a_m)$. If we choose constants in $\mathbb{C}$ for all the a_i, we denote the corresponding specialization of g to a polynomial in $\mathbb{C}[x_1, \ldots, x_n]$ by g_a. For any $g \in \mathbb{C}[a_1, \ldots, a_m, x_1, x_2]$, we then define the* **genus zero locus of** *g, $\mathcal{G}_g$, to be the set of all $a \in \mathbb{C}^m$ such that S_{g_a} has an irreducible component with geometric genus zero.*[4]

By a celebrated theorem of Siegel (cf. section 1.1), detecting genus zero for a given curve (in many cases) is equivalent to detecting the existence of infinitely many integral points. So the following theorem, proved in section 3, may be of independent interest.

Theorem 4. *For any $g \in \overline{\mathbb{Q}}[a_1, \ldots, a_m, x, y]$, the locus $\mathcal{G}_g$ is a quasi-affine variety, and the equations (and inequations) defining $\mathcal{G}_g$ can be constructed effectively, e.g., by a Turing machine.*

For example, a special case which is easy to derive from the basic theory of elliptic curves [Sil95] is the following: If $g := a_1 y^2 + a_2 + a_3 x + a_4 x^3$, then the zero set of g in $\mathbb{C}^2$ has an irreducible component of genus zero iff

$$a_1 a_4 (4a_3^3 + 27a_2^2 a_4) = 0.$$

Oddly, while there are certainly algorithms for computing the genus of the zero set of a given irreducible $f \in \overline{\mathbb{Q}}[x, y]$ (e.g., [Hoe94]), the effective geometric characterization of genus zero above appears to be new. So we present a proof of theorem 4 in section 3.

In closing this first half of our introduction, we point out that our main theorems suggest that there is a deep connection between complex geometry and Diophantine complexity which has yet to be explored. In particular, we clearly need more refined geometric invariants to explicitly classify those curves (and surfaces) where we can hope to effectively study integral points.

Main Theorems 2 and 3 are proved in section 4, and Main Theorem 1 is then proved in section 5. Some interesting open questions are briefly discussed in section 6. We now describe our necessary results on integral points more precisely.

---

[4] For convenience, we will sometimes use x and y in place of x_1 and x_2 in the bivariate case.

1.1. **Curves with Many Integral Points.**

In this subsection, we will let f denote a polynomial in $\mathbb{Z}[x,y]$. Let us quote Siegel's classification of curves having infinitely many integral points.

Siegel's Theorem. [Sie29, Lan83, Aya91, Sil00] *Let C be a curve defined over $\mathbb{Z}$ and irreducible over $\mathbb{C}$. Then C has infinitely many integral points $\Longrightarrow$ C has genus zero and one or two points (necessarily nonsingular) in $\mathbb{P}^2_{\bar{\mathbb{Q}}}\setminus\mathbb{C}^2$. Furthermore, we have the following partial converse: Any C satisfying the latter condition will have infinitely many integral points in a sufficiently large finite algebraic extension of $\mathbb{Z}$.* ■

Remark 2. *By the genus of a variety V we will always mean the geometric genus of a smooth projective model for V. (Since geometric genus is a birational invariant, it will be independent of the chosen model.) The genus of a curve is described very nicely in* [Mir95]*, and the genera of higher dimensional varieties is defined in* [Har77, Kho78].

Remark 3. *For $C=S_f$, our definition of C having a "point at infinity" is simply that the compactified zero set of C intersect $\mathbb{P}^2_{\bar{\mathbb{Q}}}\setminus\mathbb{C}^2$. So the "points at infinity" condition in Siegel's Theorem can actually be checked algorithmically, simply by considering the zero set of the homogeneous polynomial $t^{\deg f} f(x/t,y/t)|_{t=0}$ in $\overline{\mathbb{Q}}^2\setminus(0,0)$.*

Note that an immediate corollary of Siegel's Theorem, and our preceding remarks, is that the condition on C in Main Theorem 1 can be replaced by the following:

"...C has a component of genus zero with at most two points (counting multiplicities) at infinity."

This version can be checked algorithmically, but gives a slightly larger exceptional case of $\exists\exists\forall\exists$ than the original condition.

The final result on integral points we quote (and paraphrase slightly) will allow us to efficiently decide a small, but highly non-trivial quantifier prefix.

The JST Theorem. [Jon81, Sch82, Tun87] *The quantifier prefix $\forall\exists$ is decidable in singly-exponential (deterministic sequential) time. More explicitly, given $P\in\mathbb{Z}[x,y]$, we have that $\forall x\ \exists y\ P(x,y)=0$ iff all of the following conditions hold:*

1. *The polynomial P factors into the form $P_0(x,y)\prod_{i=1}^k(y-P_i(x))$ where $P_0(x,y)\in\mathbb{Q}[x,y]$ has* **no** *zeroes in the ring $\mathbb{Q}[x]$, and for all i, $P_i\in\mathbb{Q}[x]$ and the leading coefficient of P_i is positive.*
2. *$\forall x\in\{1,\ldots,x_0\}\ \exists y\in\mathbb{N}$ such that $P(x,y)=0$, where $x_0=\max\{s_1,\ldots,s_k\}$, and for all i, s_i is the sum of the squares of the coefficients of P_i.*
3. *Let d be the least positive integer such that $dP_1,\ldots,dP_k\in\mathbb{Z}[x]$ and set $Q_i:=dP_i$ for all i. Then the* **union** *of the solutions of the following k congruences*

$$\begin{aligned} Q_1(x) &\equiv 0 \mod d \\ &\vdots \\ Q_k(x) &\equiv 0 \mod d \end{aligned}$$

is **all** *of $\mathbb{Z}/d\mathbb{Z}$.*

In particular, the above conditions can be checked within a number of bit-operations polynomial in the degree of P, and singly-exponential in the bit-sizes of the coefficients of P, via fast factorization of polynomials in ≤ 2 variables over $\mathbb{Q}$ and $\mathbb{Z}/d\mathbb{Z}$ [Coh93]. ■

Remark 4. *The JST Theorem can be strengthened slightly in the following way: one can replace d in condition (3) with* **any** *positive integer d' such that $d'P_1, \ldots, d'P_k \in \mathbb{Z}[x]$.*

2. Geometric Background

We first point out that a complete account of computability, decidability, and Turing machines can be found in [GJ79, Mat93, BCSS98]. Also, our notion of "input" will be fairly standard: either the sparse encoding of polynomials (over $\mathbb{Z}$ or $\mathbb{Q}$) or the bit-wise encoding of algebraic numbers, for BSS machines over $\mathbb{Z}/2\mathbb{Z}$ [BCSS98]. Finally, for most of the basic facts we will use from algebraic geometry, we refer the reader to [Har77, Mum95, Bea96]. However, for the convenience of the reader, we will restate a few of the most central notions.

Remark 5. *Throughout most of this paper, "effectively computable" and "algorithmic" will be taken to mean Turing computable.*

Returning to the concept of sparse encoding, the following notation will be useful: For any $e \in \mathbb{Z}^n$, we let x^e denote the monomial term $x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}$. For any polynomial $f(x) = \sum_{e \in \mathbb{Z}^n} c_e(a) x^e \in \mathbb{C}[a_1, \ldots, a_m, x_1, \ldots, x_n]$, we then let the **support** of f, $\mathrm{Supp}(f) \subset \mathbb{Z}^n$, be the set of exponents $\{e \in \mathbb{Z}^n \mid c_e(a) \not\equiv 0\}$. (We are implicitly considering the x_i as variables to be solved for, and the a_j as parameters we are free to choose.) Also, we will let the **Newton polytope** of f, $\mathrm{Newt}(f) \subset \mathbb{R}^n$, be the convex hull of (i.e., the smallest convex set containing) $\mathrm{Supp}(f)$.

An **affine variety** is simply the complex zero set of a system of polynomial equations. (So our varieties will not necessarily be **reduced** or **irreducible** [Har77, Mum95].) More generally, a **quasi-affine** variety is the set of complex points satisfying any finite Boolean combination of polynomial equations and inequations. (Note that we mean $\neq$, not $<$ or $\leq$, when we say inequation.) In particular, when we say a set of indeterminates $\{a_1, \ldots, a_m\}$ is chosen **generically**, we will mean that $(a_1, \ldots, a_m) \in \mathbb{C}^m \setminus W$ for some **a priori fixed** quasi-affine algebraic subvariety W (depending only on the property in question) with $\mathrm{codim} W \geq 1$. For most purposes, assuming a property holds generically also implies that the property occurs with probability 1. (A classification of a broad class of probability measures on $\mathbb{C}^m$ for which this is true is not hard to derive.) We will also use the term **variety** collectively for affine and quasi-affine varieties.

As for the geometric language of our main theorems, let us recall the following definitions: A **morphism** is simply a well-defined map from one variety to another, given by rational functions. When we relax the "well-defined" stipulation and allow our map to be undefined on a subvariety of codimension ≥ 1, we then obtain a **rational** map. Also, a **birational** map is a rational map with an inverse which is again a rational map.

The inverse image of a point, for any given morphism, is usually called a **fiber**. For any curve C, we then say that a variety V is a **bundle of curves fibered over** C iff there is a morphism $\varphi : V \longrightarrow C$ such that every fiber of φ is a (not necessarily irreducible) curve.

Definition 3. [Bea96] *Assume temporarily that all varieties are irreducible, nonsingular, and compact. Let C be a curve. We then call a surface S* **ruled over** *C iff there is a morphism $\varphi : S \longrightarrow C$ with every fiber isomorphic to $\mathbb{P}^1_{\mathbb{C}}$. Similarly, we will call a surface S* **ruled** *iff there is a curve C for which S is ruled over C. Finally, an arbitrary algebraic surface S (not necessarily irreducible, nonsingular, or compact) is said to be* **rational** *iff S is birationally equivalent to $\mathbb{P}^2_{\mathbb{C}}$.*

The following two related facts will prove useful.

Theorem 5. [Kho78][5] *Suppose $f \in \mathbb{C}[a_1, \ldots, a_m, x_1, \ldots, x_n]$. Then, for generic a, the genus of $S_{f_a} \subseteq \mathbb{C}^n$ is exactly the number of lattice points in the interior of* Newt(f). ■

Theorem 6. *If S is a ruled surface, then its genus is zero. Also, if S is a bundle of curves (each with a genus zero component) fibered over another curve, then S has a component which is birationally equivalent to a ruled surface.* ■

Theorem 6 follows easily from the development of [Bea96] and, in particular, the classical Noether-Enriques theorem on algebraic surfaces [Bea96].

Two interesting examples of theorem 6 are the following:

Example 1. ($\exists v \exists y \subset \exists v \forall x \exists y$) *For any $f \in \mathbb{Z}[v, y] \setminus \{0\}$, reconsider its zero set as a polynomial in $\mathbb{Z}[v, x, y]$. Abusing notation slightly, let us denote this subvariety of $\mathbb{C}^3$ by S_f. Then there is a natural projection φ from S_f onto the v-axis, and any fiber $\varphi^{-1}(v_0)$ is clearly of the form $\{v_0\} \times C$ where C is a finite union of lines. So the hypothesis of theorem 6 is satisfied in this example. Better still, the conclusion of theorem 6 is easily verified: S_f is clearly birational to a ruled surface, since S_f is clearly a Cartesian product of a curve with a line.*

Example 2. ($\exists u \exists v \exists y \subset \exists u \exists v \forall x \exists y$) *For any $f \in \mathbb{Z}[u, v, y] \setminus \{0\}$, reconsider its zero set as a polynomial in $\mathbb{Z}[u, v, x, y]$. Abusing notation once more, let us denote this subvariety of $\mathbb{C}^4$ by S_f. Then there is a natural projection φ from S_f onto the (u, v)-plane, and any fiber $\varphi^{-1}(u_0, v_0)$ is clearly of the form $\{(u_0, v_0)\} \times C$ where C is a finite union of lines. More to the point, consider the inverse image of φ over a line L in the (u, v)-plane with positive rational slope. Clearly then, $\varphi^{-1}(L) \subset S_f$ is a surface*

[5]The version of theorem 5 stated in [Kho78] is actually a bit different, but easily implies our version here via an application of theorem 7 below.

S' fibered over L. In particular, every fiber $\varphi^{-1}(c) \cap S'$, for $c \in L$, is clearly a curve with a genus zero component. So S_f contains a surface (S') of the type specified in Main Theorems 1 and 3, and by theorem 6, this surface has a ruled component.

To prove theorem 4 we will make some use of elimination theory, but in a geometric form.

Theorem 7. *Suppose V is a quasi-affine subvariety of $\mathbb{C}^m \times \mathbb{C}^n$ defined over $\overline{\mathbb{Q}}$, and we respectively use coordinates $a := (a_1, \ldots, a_m)$ and $x := (x_1, \ldots, x_n)$ for the first and second factors. Then the following assertions hold:*

1. [Har77, Mum95] *The set of $a \in \mathbb{C}^m$ for which there is an $x \in \mathbb{C}^n$ with $(a, x) \in V$ is another quasi-affine variety $W \subseteq \mathbb{C}^m$ defined over $\overline{\mathbb{Q}}$. Furthermore, if we are given the sparse encodings of the polynomials defining V, then we can algorithmically determine the analogous data for W.*
2. [Roj99a, Roj99b] *Given the sparse encodings of the polynomials defining a* **zero**-*dimensional variety $U \subset \overline{\mathbb{Q}}^n$, the sets $U \cap \mathbb{Z}^n$ and $U \cap \mathbb{N}^n$ can be effectively computed.*
3. [GMT89, Koi97] *The decomposition of V into irreducible components, and their dimensions, can be effectively computed.* ■

A more general and explicit version of part (1) was derived by Tarski in his work on quantifier elimination (over $\mathbb{R}$) in the 1950's. Considerable improvements have since been made by other authors, giving singly-exponential complexity bounds for the problem described in part (1). However, since our main concern is decidability, we will not dwell on these important extensions.

Finally, we will need Hurwitz' Theorem [Mir95, Sil95] relating the genera of the domain and image of a morphism between curves.

Theorem 8. *Suppose $\varphi : C \longrightarrow C'$ is a nonconstant morphism of nonsingular compact curves over $\mathbb{C}$. Let g and g' respectively be the genera of C and C'. Then the following relation holds:*

$$2g - 2 = (\deg \varphi)(2g' - 2) + \sum (e_\varphi(p) - 1)$$

where the sum is over all points $p \in C$ such that φ is ramified at p, and $e_\varphi(p)$ denotes the ramification index. ■

3. The Proof of Theorem 4

We will first need the following definitions.

Definition 4. *Let* $\mathrm{MultiSub}(\mathbb{Z}^n)$ *denote the set of all finite multisets of finite subsets of $\mathbb{Z}^n$. Let us also endow the following partial ordering on* $\mathrm{MultiSub}(\mathbb{Z}^n)$*: Declare $\{S_1, \ldots, S_k\} \leq \{T_1, \ldots, T_l\}$ iff there are polynomials $f_1, \ldots, f_k, g_1, \ldots, g_l \in \mathbb{C}[x_1, \ldots, x_n]$ such that $k \leq l$,* $\mathrm{Supp}(f_i) = S_i$ *for all i,* $\mathrm{Supp}(g_j) = T_j$ *for all j, and*

$\mathrm{Supp}(\prod_i f_i) = \mathrm{Supp}(\prod_j g_j)$. *Concluding this connection to factoring, let us also define the* **factor type**, $\mathcal{T}_f \in \mathrm{MultiSub}(\mathbb{Z}^n)$, *of a polynomial* $f \in \mathbb{C}[x_1, \ldots, x_n]$, *to be the multiset of supports of its irreducible factors over* $\mathbb{C}[x_1, \ldots, x_n]$.

It is not hard to see that for a given polynomial with parametric coefficients, possessing a particular factor type determines a condition defining a quasi-affine variety.

Lemma 1. *Suppose* $f \in \overline{\mathbb{Q}}[a_1, \ldots, a_m, x_1, \ldots, x_n]$. *Then, for any* $\mathcal{T} \in \mathrm{MultiSub}(\mathbb{Z}^n)$, *the set of all* $(a_1, \ldots, a_m) \in \mathbb{C}^m$ *for which* f_a *has factor type* $\mathcal{T}$ *is a quasi-affine variety defined over* $\overline{\mathbb{Q}}$. *Furthermore, the polynomials defining this variety are effectively computable.*

Proof: First note that f_a has factor type $\geq \{S_1, \ldots, S_k\}$ iff a set of equations involving $a_1, \ldots, a_m$ has a solution. This assertion is immediate, but for clarity we give the following example with $k=2$: $a_1 + a_2x^2 + a_3y^2 = (\alpha_1 + \beta_1 x + \gamma_1 y)(\alpha_2 + \beta_2 x + \gamma_2 y) \Longleftrightarrow$ the following system of equations has a solution $(\alpha_1, \beta_1, \gamma_1, \alpha_2, \beta_2, \gamma_2) \in \overline{\mathbb{Q}}^6$:

$$\begin{aligned} \alpha_1\alpha_2 - a_1 &= 0 \\ \beta_1\beta_2 - a_2 &= 0 \\ \gamma_1\gamma_2 - a_3 &= 0 \\ \alpha_1\beta_2 + \alpha_2\beta_1 &= 0 \\ &\text{etc...} \end{aligned}$$

So by theorem 7, possessing a factor type above or equal to $\{S_1, \ldots, S_k\}$ defines a quasi-affine subvariety of values of a. Now note that the poset of possible factor types for any fixed f is finite, and recall that quasi-affine varieties are closed under any finite sequence of Boolean operations. So by another application of theorem 7, the set of a for which f_a has factor type **exactly** $\{S_1, \ldots, S_k\}$ is also a quasi-affine variety. So we are done. ■

We can now at last prove theorem 4.

Proof of Theorem 4: Recall once again that quasi-affine varieties (even those defined over $\overline{\mathbb{Q}}$) are closed under any finite sequence of Boolean operations. So it suffices to prove that some collection of **algebraic functions** of the a in question form a (Turing computable) quasi-affine variety. So by lemma 1, it thus suffices to assume that g is an irreducible polynomial in $\mathbb{C}[a_1, \ldots, a_m, x, y]$, and $a \in \overline{\mathbb{Q}}^m$ is such that g_a is irreducible.

Let C be the complex zero set of g_a. Then C is an irreducible curve, possibly with singularities. The singularities of C are precisely the zero set (in the (x, y)-plane $\overline{\mathbb{Q}}^2$) of an effectively constructible system of polynomials in $\overline{\mathbb{Q}}[a_1, \ldots, a_m, x, y]$ [Har77, Mum95]. So the coordinates of every singular point are algebraic functions of $a_1, \ldots, a_m$ defined over $\overline{\mathbb{Q}}$.

Since the number of such singularities is finite, a finite sequence of blow-ups will give us a new curve $\tilde{C}$ birationally equivalent to C. Furthermore, by our preceding observations, and the structure of the blow-up map [Har77, Mum95], the coefficients of $\tilde{C}$ are algebraic functions of $a_1, \ldots, a_m$, defined over $\overline{\mathbb{Q}}$, as well.

To conclude, note that $\tilde{C}$ is a curve in $\mathbb{P}^N_{\mathbb{C}}$, where N is 2 plus the sum of the orders of the singularities of C. Furthermore, we can consider the ambient projective plane in which C lies as a coordinate subspace of $\mathbb{P}^N_{\mathbb{C}}$. So let φ be the natural projection mapping $\mathbb{P}^N_{\mathbb{C}}$ onto the x-axis of this copy of $\mathbb{P}^2_{\mathbb{C}}$.

Now let us apply theorem 8 to the preceding morphism $\varphi : \tilde{C} \longrightarrow \mathbb{P}^1_{\mathbb{C}}$. We then obtain that g_a has genus zero iff

$$2 \deg \varphi = 2 + \sum (e_\varphi(p) - 1).$$

By theorem 7 and our preceding observations (as well as the classical notion of discriminant), we can write the preceding sum of ramification indices as the order of vanishing of some (effectively constructible) polynomial in $\overline{\mathbb{Q}}[a_1, \ldots, a_m]$ at a point. Furthermore, this order of vanishing is equal to some fixed constant iff a lies in a quasi-affine variety (defined over $\overline{\mathbb{Q}}$) depending on the constant. Similarly, the degree of φ is some fixed constant iff a lies in a quasi-affine variety depending on the constant. We thus at last obtain that $\mathcal{G}_g$ is a Turing constructible quasi-affine variety. ■

4. Deciding Prefixes Ending in ∀∃

To prove Main Theorems 2 and 3, we will first describe a construction which is common to both proofs. So let us temporarily consider polynomials in $\mathbb{Z}[u, v, x, y]$. More precisely, it will be helpful to consider f as a polynomial in x and y with coefficients in $\mathbb{Z}[u, v]$. For emphasis, we will now respectively write $f_{(u,v)}$ and $f_{(u,v)}(x, y)$ in place of f and $f(u, v, x, y)$.

Definition 5. *For any $f \in \mathbb{Z}[u, v, x, y]$, let Ξ_f be the set of all pairs $(u, v) \in \mathbb{N}^2$ such that*

$$\forall x \ \exists y \text{ with } f_{(u,v)}(x, y) = 0.$$

Our main trick for proving Main Theorems 2 and 3 is the following: create an explicit quasi-affine variety $\Omega_f \subset \mathbb{C}^2$ defined over $\overline{\mathbb{Q}}$, whose positive integral points contain (and very nearly equal) Ξ_f. The following definition and lemma will clarify our complex geometric approximation.

Definition 6. *Following the notation of definition 2, for any $f \in \mathbb{C}[u, v, x, y]$ let $\Omega_f := \mathcal{G}_f$, where we consider f as a polynomial in x and y with coefficients in $\mathbb{C}[u, v]$. So $\Omega_f \subset \mathbb{C}^2$ and the polynomials defining Ω_f lie in $\mathbb{C}[u, v]$.*

Lemma 2. *The set Ξ_f is contained in $\Omega_f \cap \mathbb{N}^2$. In particular, $\dim \Omega_f \geq 1$ iff f lies in the exceptional locus defined in Main Theorem 3.*

Furthermore, if we restrict to $f \in \mathbb{C}[v, x, y]$ (and thus consider $\Xi_f \subseteq \mathbb{N}$ and $\Omega_f \subseteq \mathbb{C}$), we have that $\Xi_f \subseteq \Omega_f \cap \mathbb{N}$. In particular, under this restriction, $\dim \Omega_f \geq 1$ iff f lies in the exceptional locus defined in Main Theorem 2.

Proof of Lemma 2: By Siegel's Theorem, $(u,v)\in\Xi_f \Longrightarrow S_{f_{(u,v)}}$ contains an irreducible curve of genus zero. So the inclusion $\Xi_f\subseteq\Omega_f\cap\mathbb{N}^2$ is clear. The condition for $\dim\Omega_f\geq 1$ is then just a reformulation of the condition that enough specializations of (u,v) make $S_{f_{(u,v)}}$ have genus zero. The refined statements for when $f\in\mathbb{Z}[v,x,y]$ follow similarly. ■

The description of Ξ_f as a subset of the positive integral points on a quasi-affine variety allows an intuitive complex geometric approach to constructing algorithms for a large family of special cases of Diophantine prefixes such as $\exists\forall\exists$ and $\exists\exists\forall\exists$. In particular, theorem 4 tells us that our quasi-affine variety Ω_f is effectively computable, and a judicious use of computational algebra can make this implementable. This is pursued further in [Roj99b].

Remark 6. *We now briefly clarify the statement of "genericity" in Main Theorems 2 and 3: Fix the Newton polytope $P\subset\mathbb{R}^3$ of f. Then, by theorems 5 and 6, and the classical Bertini's theorem* [Har77, Mum95]*, S_f will be an irreducible* **non***-ruled surface, provided the coefficients are chosen generically and P has at least one lattice point in its interior. Thus (except for a meager family of supports) Main Theorem 2 implies that for any fixed support we can decide $\exists\forall\exists$ for a Zariski-dense set of f. The analogous statement for Main Theorem 3 can be derived in essentially the same way, assuming the computability of* $\mathbf{Big}_{\mathbb{N},2}$.

Proof of Main Theorem 2: To construct our necessary algorithm, note that as observed in earlier situations, the variable u no longer occurs in f. So, since the prefixes $\exists u\exists v\forall x\exists y$ and $\exists v\forall x\exists y$ are identical for such f, we may now consider Ω_f as a subvariety of $\mathbb{C}$. (And the polynomials defining Ω_f lie in $\overline{\mathbb{Q}}[v]$.) Let us also assume f is not identically zero. (For when f is identically zero, the prefix in question is trivially true.)

Clearly then, if $\dim\Omega_f\leq 0$, deciding whether $\exists v\ \forall x\ \exists y$ such that $f(v,x,y)=0$ reduces to simply checking a finite[6] number of instances of the prefix $\forall\exists$. (Recall also that we can effectively detect $\dim\Omega_f\leq 0$ by theorems 4 and 7.) By the JST Theorem and theorem 7, we thus need only show that the hypothesis of Main Theorem 2 implies that $\dim\Omega_f\leq 0$. But this follows immediately from lemma 2. ■

The proof of Main Theorem 3 is almost exactly the same, save for the fact that the polynomials defining Ω_f lie in $\overline{\mathbb{Q}}[u,v]$. So we will omit the proof of Main Theorem 3 and go directly to the proof of our first main theorem.

5. The Proof of Main Theorem 1

Let us temporarily assume that $\mathbf{Big}_{\mathbb{N},2}$ is computable. Let us also temporarily assume that the stated special case of $\exists\exists\forall\exists$ is decidable. To derive a contradiction,

[6]The number of instances is bounded above by the degree of Ω_f, which can in turn be bounded above by an explicit polynomial in the degree of f [Roj99b, Main Theorem 4].

we will construct an explicit algorithm to decide the prefix $\exists\exists\forall\exists$ in general. To do this, we will again use our algebraic geometric trick from the last section.

Accordingly, our algorithm will have three cases, dictated by the topology of Ω_f in $\mathbb{C}^2$. Also note that $\exists u \exists v \forall x \exists y$ is trivially true when f is identically zero, so we may assume that f is not indentically zero.

By theorem 4, the JST Theorem, and theorem 7 once again, we know that the prefix $\forall\exists$ is sufficiently well-behaved so that we can make a simplification: we may assume that Ω_f is irreducible. Also, using part (3) of theorem 7, it is clear that Cases I, II, and III below can be distinguished effectively. So let us now solve these cases individually.

Case I: $\boldsymbol{\Omega_f = \emptyset}$

By our preceding observations, we immediately obtain that

$$\exists u \; \exists v \; \forall x \; \exists y \; f(u,v,x,y) = 0$$

is false. ■

Case II: $\boldsymbol{\dim \Omega_f = 0}$

Here, we need only check one instance of $\forall\exists$. By the JST Theorem, we can do this within singly exponential time, so we are done. ■

Case III: $\boldsymbol{\dim \Omega_f \geq 1}$

By assumption we can solve the case where $\dim \Omega_f = 2$. (Indeed, when $\dim \Omega_f = 2$, we can certainly find a curve in Ω_f satisfying the properties required in statement (2) of Main Theorem 1.) So let us assume $\dim \Omega_f = 1$ and, to simplify notation slightly, let $C := \Omega_f$. We are left with just two subcases to consider and, by assumption, we can compute $\mathbf{Big}_{\mathbb{N},2}$ to effectively distinguish them.

Case III(a): *C* has finitely many positive integral points

Since we can compute $\mathbf{Big}_{\mathbb{N},2}$, we can simply enumerate all possible positive integral points and use the JST Theorem a finite (but most likely huge) number of times to decide $\exists\exists\forall\exists$. ■

Case III(b): *C* has infinitely many positive integral points

By our initial assumption, this case of $\exists\exists\forall\exists$ is tractable as well. ■

Having thus obtained an algorithm contradicting the MR Theorem, we are done. ■

6. Conclusion

We have seen a geometric construction which implies a weak version of the statement "$\mathcal{HTP}_{\mathbb{N}}(3)$ is decidable $\Longrightarrow$ $\mathbf{Big}_{\mathbb{N},2}$ is uncomputable." The decidability of Hilbert's Tenth Problem in three variables is still open, as is the existence of computable general upper bounds on the size of integral points on algebraic curves. So knowing the decidability of $\mathcal{HTP}_{\mathbb{N}}(3)$ or the computability of $\mathbf{Big}_{\mathbb{N},2}$ would have profound implications in algorithmic number theory, not to mention arithmetic geometry.

We emphasize, however, that the uncomputability of $\mathbf{Big}_{\mathbb{Z},2}$ would by no means contradict the effective upper bounds (for heights of integral points) which have already been found [Bak68, Bak69, BC70, Bri84, Pou93] for certain special classes of curves. More precisely, should $\mathbf{Big}_{\mathbb{Z},2}$ eventually prove uncomputable, we obtain from our development that at least one of the following statements must be **true**:

(A) Effective upper bounds on integral points must cease to exist for some infinite class of non-superelliptic curves of genus at least two.[7]

(B) Detecting infinitudes of integral points on a curve of genus zero is undecidable.

Furthermore, assuming the decidability of detecting infinitudes of rational points on curves of genus ≤ 1 (and the falsity of statement (B)), the uncomputability of $\mathbf{Big}_{\mathbb{Z},2}$ would also immediately imply the uncomputability of $\mathbf{Big}_{\mathbb{Q},2}$.

It is also clearly the case that the uncomputability of $\mathbf{Big}_{\mathbb{Z},2}$ would not contradict the decidability of $\mathcal{HTP}_{\mathbb{Z}}(2)$, should the latter statement prove true. Indeed, the uncomputability of $\mathbf{Big}_{\mathbb{Z},2}$ would only rule out a stronger version of the decidability of $\mathcal{HTP}_{\mathbb{Z}}(2)$ — the determination of **all** integral points when there are only finitely many. More to the point, the existence of effective general upper bounds on the height of the **smallest** integral point is still an open question. For example, Steve Smale has conjectured that such upper bounds, for curves of positive genus, exist and will be singly-exponential in the size of the dense encoding [Sma98]. So the truth of Smale's conjecture would immediately imply a brute force algorithm for the positive genus case of $\mathcal{HTP}_{\mathbb{Z}}(2)$.

We also point out that the exceptional locus in Main Theorem 3 can be pared down somewhat: Via a suggestion of Smale, one can sometimes assume additionally that the forbidden f have a zero set which is either (a) reducible or (b) irreducible and singular. This refinement is based on examining the critical values of (the restriction to S_f of) the natural projection mapping $\mathbb{C}^4$ to the (u,v)-plane. Other refinements based on a closer examination of the real part of S_f are possible and will be mentioned in future work.

We will close by stating a few conjectures and open problems related to our development. First note that if the statement "$\mathbf{Big}_{\mathbb{N},2}$ is computable $\Longleftrightarrow$ $\mathbf{Big}_{\mathbb{Z},2}$ is computable" were true, then we could strengthen Main Theorem 1. (In particular, we could replace $\mathbf{Big}_{\mathbb{N},2}$ by $\mathbf{Big}_{\mathbb{Z},2}$.) Toward this end, we make the following conjecture on a type of equidistribution for integral points on the real part of a genus zero curve.

Conjecture 1. *Suppose $C \subset \mathbb{C}^2$ is a curve defined over $\mathbb{Z}$ and irreducible over $\mathbb{C}$. Suppose further that some irreducible component $C_{\mathbb{R}}$ of $C \cap \mathbb{R}^2$ has noncompact intersection with the first quadrant. Then $C_{\mathbb{R}}$ has infinitely many integral points $\Longrightarrow$ $C_{\mathbb{R}}$ has infinitely many positive integral points.*

The truth of this conjecture, combined with a little quantifier elimination over $\mathbb{R}$, would immediately imply the aforementioned equivalence of the computability of $\mathbf{Big}_{\mathbb{N},2}$ and $\mathbf{Big}_{\mathbb{Z},2}$.

[7]Recalling that every curve over $\mathbb{C}$ of genus two is hyperelliptic [Mir95], the results of [Gra94, Poo96] give evidence that this lower bound might need to be increased to three.

However, a potentially harder problem is to refine our proof of Main Theorem 1 to yield the truth of the following conjecture we have been alluding to.

Conjecture 2. *$\mathcal{HTP}_{\mathbb{N}}(3)$ is decidable $\Longrightarrow$ $\mathbf{Big}_{\mathbb{N},2}$ is uncomputable.*

In particular, a refinement of our geometric approach seems possible, but quite subtle. For example, the proof of a 1970 theorem which essentially computes $\mathbf{Big}_{\mathbb{Z},2}$ in the special case of genus one curves [BC70] involves constructing a very special birational map. The map Baker and Coates construct takes an arbitrary genus one curve to a curve in Weierstrass normal form, preserves rational points, and almost preserves integral points. The structure of their map was sufficiently good so that they could use the previously known bounds for curves in Weierstrass normal form to derive height bounds for the original (possibly more general) genus one curve.

An analogous construction could be attempted for reducing the exceptional locus of Main Theorems 1 and 3 to the prefix $\exists\exists\exists$. For instance, when $\dim \Omega_f = 2$ (which is arguably the hardest case), S_f is a ruled 3-fold of a very restricted type. One could then try to find a birational map (with well-bounded degree and coefficients heights) sending f to a polynomial in $R[v, x, y]$, for some (well-bounded) finite extension R of $\mathbb{Z}$. Such a construction, if done properly, could be used to prove the undecidability of $\exists\exists\exists$ or the equivalence of the decidabilities of $\exists\forall\exists$ and $\exists\exists$. Unfortunately, as of 1998, not enough is known about integral points on 3-folds, or even rational surfaces, to make this approach easy. Nevertheless, we hope to address this point in the future.

We also propose the following conjecture motivated by our results.

Conjecture 3. *The prefixes $\exists\forall\exists$ and $\exists\exists$ are decidable. However, $\mathbf{Big}_{\mathbb{N},2}$ is uncomputable and $\mathcal{HTP}_{\mathbb{N}}(3)$ is undecidable.*

The author is also willing to offer \$1000 (US) for the first correct published proof of the decidability of $\mathcal{HTP}_{\mathbb{N}}(3)$. This will hopefully prove a safe wager.

Finally, we remark that for the sake of simplicity, we have not given the best possible complexity bounds. It is therefore quite likely that Main Theorem 2 can be improved to give an algorithm which runs in doubly-exponential time. In fact, we are willing to conjecture more.

Conjecture 4. *The Diophantine prefix $\exists\forall\exists$ is generically decidable within singly-exponential time.*

7. Acknowledgements

The author would like to express his deep gratitude to Professors Lenore Blum, Manuel Blum, and Steve Smale for patiently listening to earlier versions of this work. The author also thanks James P. Jones, Barry Mazur, Zhi-Wei Sun, Shih-Ping Tung, and Paul Vojta for useful e-mail discussions. Thanks also go to an anonymous referee who made many useful suggestions. Special thanks go to Joseph H. Silverman for a very encouraging e-mail (see below).

Finally, the author would like to thank Professor Manuel Blum for his extraordinary generosity, and dedicate this paper to him. Happy 60 Manuel!

NOTE ADDED IN PROOF

Joseph H. Silverman has just proved [Sil00] my Conjecture 1 above, so we now have the equivalence of the computabilities of $\mathbf{Big}_{\mathbb{N},2}$ and $\mathbf{Big}_{\mathbb{Z},2}$! We can thus now strengthen Main Theorem 1 (and sharpen Conjectures 2 and 3) by replacing $\mathbf{Big}_{\mathbb{N},2}$ with $\mathbf{Big}_{\mathbb{Z},2}$ throughout.

Also, the author has recently proved the following strengthening of Conjecture 4: $\exists\forall\exists$ is generically decidable within the complexity class **PSPACE** [Roj99b].

References

[Aya91] Ayad, M., *"On Runge's Theorem,"* Acta. Arith. **58** (1991), no. 2, pp. 203–209.

[Bak75] Baker, Alan, *Transcendental Number Theory,* Cambridge University Press, 1975.

[Bak68] __________, *"Contributions to the Theory of Diophantine Equations I: On the Representation of Integers by Binary Forms,"* Philos. Trans. Roy. Soc. London Ser. A, 263 (1968), 173–208.

[Bak69] __________, *"Bounds for the Solutions of the Hyperelliptic Equation,"* Proc. Camb. Philos. Soc. 65 (1969), 439–444.

[BC70] Baker, Alan and Coates, John, *"Integer Points on Curves of Genus 1,"* Proc. Camb. Philos. Soc. 67 (1970), 595–602.

[Bea96] Beauville, Arnaud, *Complex Algebraic Surfaces,* second edition, London Mathematical Society Student Texts, 34, Cambridge University Press, 1996.

[BCSS98] Blum, L., Cucker, F., Shub, M., and Smale, S., *Complexity and Real Computation,* Springer-Verlag (1998).

[Bom90] Bombieri, Enrico, *"The Mordell Conjecture Revisited,"* Ann. Sculoa Norm. Sup. Pisa Cl. Sci. (4) **17** (1990), no. 4, pp. 615–640.

[Bri84] Brindza, B., *"On S-Integral Solutions of the Equation $y^m = f(x)$,"* Acta. Math. Hungar. **44** (1984), no. 1–2, pp. 133–139.

[Coh93] Cohen, Henri, *A Course in Computational Number Theory,* Graduate Texts in Mathematics, 138, Springer-Verlag, Berlin, 1993.

[GJ79] Garey, Michael R. and Johnson, David S. *Computers and Intractability: A Guide to the Theory of NP-Completeness,* A Series of Books in the Mathematical Sciences, W. H. Freeman and Co., San Francisco, Calif., 1979.

[GMT89] Gianni, P., Miller, V., and Trager, B., *"Decomposition of Algebras,"* Symbolic and Algebraic Computation (Rome, 1988), pp. 300–308, Lecture Notes in Comput. Sci., 358, Springer, Berlin, 1989.

[Gra94] Grant, David, *"Integer Points on Curves of Genus Two and Their Jacobians,"* Trans. Amer. Math. Soc. **344** (1994), no. 1, pp. 79–100.

[Har77] Hartshorne, Robin, *Algebraic Geometry,"* Graduate Texts in Mathematics, No. 52, Springer-Verlag.

[Hoe94] van Hoeij, Mark, *"An Algorithm for Computing an Integral Basis in an Algebraic Function Field,"* J. Symbolic Comput. **18** (1994), no. 4, pp. 353–363.

[Jon81] Jones, James P., *"Classification of Quantifier Prefixes Over Diophantine Equations,"* Zeitschr. f. math. Logik und Grundlagen d. Math., Bd. 27, pp. 403–410 (1981).

[Jon82] ______________, *"Universal Diophantine Equation,"* Journal of Symbolic Logic, 47 (3), pp. 549–571 (1982).

[Kho78] Khovanskii, A. G., *"Newton Polyhedra and the Genus of Complete Intersections,"* Functional Analysis (translated from Russian), Vol. 12, No. 1, January–March (1978), pp. 51–61.

[Koi97] Koiran, Pascal, *"Randomized and Deterministic Algorithms for the Dimension of Algebraic Varieties,"* Proceedings of the 38th Annual IEEE Computer Society Conference on Foundations of Computer Science (FOCS), Oct. 20–22, 1997, ACM Press.

[Lan83] Lang, Serge, *Fundamentals of Diophantine Geometry,* Springer-Verlag (1983).

[Mat93] Matiyasevich, Yuri V., *Hilbert's Tenth Problem,* MIT Press (1993).

[MR74] Matiyasevich, Yuri V. and Robinson, Julia, *"Two Universal 3-Quantifier Representations of Recursively Enumerable Sets,"* Teoriya Algorifmov i Matematicheskaya Logika (Volume dedicated to A. A. Markov), pp. 112-123, Vychislitel'nyĭ Tsentr, Akademiya Nauk SSSR, Moscow.

[Mir95] Miranda, Rick, *Algebraic Curves and Riemann Surfaces,* Graduate Studies in Mathematics, Vol. 5, American Mathematical Society.

[Mum95] Mumford, David, *Algebraic Geometry I: Complex Projective Varieties,* Reprint of the 1976 edition, Classics in Mathematics, Springer-Verlag, Berlin, 1995.

[Poo96] Poonen, Bjorn, *"Computational Aspects of Curves of Genus at Least* 2,*"* Algorithmic Number Theory (Talence, 1996), pp. 283–306, Lecture Notes in Comput. Sci., 1122, Springer, Berlin, 1996.

[Pou93] Poulakis, Dimitrios, *"Integer Points on Curves of Genus 0,"* Colloq. Math. **66** (1993), no. 1, pp. 1–7.

[Roj99a] Rojas, J. Maurice, *"Solving Sparse Degenerate Polynomial Systems Faster,"* Journal of Symbolic Computation, vol. 28, no. 1/2, July and August (special issue on elimination theory) 1999, pp. 155–186.

[Roj99b] ________________, *"On the Complexity of Diophantine Geometry in Low Dimensions,"* Proceedings of the 31st Annual ACM Symposium on Theory of Computing (STOC '99, May 1–4, 1999, Atlanta, Georgia), pp. 527–536, ACM Press, 1999.

[Run87] Runge, C., *"Über ganzzahlige Lösungen von Gleichungen zwischen zwei Veränderlichen,"* J. Reine Angew. Math. 100 (1887), pp. 425–435.

[Sch82] Schinzel, Andrzej, *Selected Topics on Polynomials,* Univ. of Michigan Press, Ann Arbor, 1982.

[Sch92] Schmidt, Wolfgang M., *"Integer Points on Curves of Genus 1,"* Compositio Mathematica **81**: 33–59, 1992.

[Sie29] Siegel, Carl Ludwig, *"Über einige Anwendungen Diophantischer Approximationen,"* Abh. Preuss. Akad. Wiss. Phys. Math. Kl. (1929), Nr. 1.

[Sil95] Silverman, Joseph H., *The Arithmetic of Elliptic Curves,* corrected reprint of the 1986 original, Graduate Texts in Mathematics 106, Springer-Verlag (1995).

[Sil00] ____________________, *"On the Distribution of Integer Points on Curves of Genus Zero,"* Theoretical Computer Science, this issue.

[Sma98] Smale, Steve, *"Mathematical Problems for the Next Century,"* Mathematical Intelligencer, to appear (1998).

[Sun92a] Sun, Zhi Wei, *"Further Results on Hilbert's Tenth Problem,"* Ph.D. Thesis, Nanjing Univ., Nanjing, 1992.

[Tun87] Tung, Shih-Ping, *"Computational Complexities of Diophantine Equations with Parameters,"* Journal of Algorithms **8**, pp. 324–336 (1987).

[Voj87] Vojta, Paul, *Diophantine Approximations and Value Distribution Theory,* Lecture Notes in Mathematics, 1239, Springer-Verlag (1987).

Department of Mathematics, City University of Hong Kong, 83 Tat Chee Avenue, Kowloon, HONG KONG

E-mail address: mamrojas@math.cityu.edu.hk *Web-page:* http://www.cityu.edu.hk/ma/staff/rojas