POSITIVE EXISTENTIAL DEFINABILITY OF MULTIPLICATION FROM ADDITION AND THE RANGE OF A POLYNOMIAL

HECTOR PASTEN AND XAVIER VIDAUX

Abstract. We consider the problem of recovering multiplication in the integers from enrichments of its additive structure, in the positive existential context. We prove that if a conjecture by Caporaso-Harris-Mazur holds, then for all integer-valued polynomials F of degree at least 2, multiplication is positive existentially definable in $(\mathbb{Z}; 0, 1, +, R_F, =)$ where R_F is the unary relation $F(\mathbb{Z})$. Similar results were only known for the polynomials $F(t) = t^2$ (under the Bombieri-Lang conjecture) and $F(t) = t^n$ (under a generalization of the *abc* conjecture).

Contents

1. Introduction and results

We are interested in the general problem of determining for which extensions of the additive structure of a ring one can recover multiplication. A very relevant result in the spirit of this general problem is the following - see [18] and [32] (this theorem can be seen as a prototype of deeper results on Zariski geometries, see for instance the discussion in [17, p. 118]):

Theorem 1.1. *A subset R of $\mathbb{C}^n$ is constructible but not definable in the module structure of $\mathbb{C}^n$ if and only if multiplication is definable in $(\mathbb{C}; +, =, R)$.*

In the arithmetic setting of $\mathbb{Z}$, some relevant progress have been achieved in the context of first-order definable sets (see [2] for a general survey on the subject), although no general classification has been established. Much less is known in the positive existential situation, where the Diophantine analogue of Theorem 1.1 would be a solution to the following:

Date: October 9, 2015.

2010 *Mathematics Subject Classification.* Primary 11U05, Secondary 14G05, 39A70.

Key words and phrases. Definability, Undecidability, Hilbert's tenth problem, Caporaso-Harris-Mazur conjecture, Integer-valued polynomials, Diophantine equations, The equation $F(x) = G(y)$.

Both authors have been partially supported by the second author's Fondecyt project 1130134 (Chile). During this research, H. P. was supported by an Ontario Graduate Scholarship at Queen's University, a Benjamin Peirce Fellowship at Harvard, and by a Schmidt Fellowship and by the NSF at the Institute for Advanced Study. This material is based upon work supported by the National Science Foundation under agreement No. DMS-1128155. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

Problem 1.2. *Classify the recursively enumerable subsets $R \subseteq \mathbb{Z}^n$ for which multiplication is positive existentially definable over the structure* $(\mathbb{Z}; 0, 1, +, =, R)$.

Requiring that R is recursively enumerable is a natural condition. Indeed, after the work of M. Davis, H. Putnam, J. Robinson and Y. Matiyasevich [19], we know that recursively enumerable sets over $\mathbb{Z}$ are the same as the positive existentially definable sets in the ring $\mathbb{Z}$ (DMPR Theorem).

One cannot hope that the naive arithmetic analogue of Theorem 1.1 holds: for instance, the full theory of

$$(\mathbb{Z}; 0, 1, +, =, \{2^n : n \in \mathbb{Z}_{>0}\})$$

is decidable, hence multiplication is not definable — see [34]. Another relevant example is given by the set $\mathcal{P}$ of prime numbers. Woods [38] proved that under Dickson's conjecture the full theory of

$$(\mathbb{Z}_{\geq 0}; 0, 1, +, =, \mathcal{P})$$

is undecidable, while under the same conjecture the existential theory is decidable (see [37]).

The existence of some recursively enumerable set $R \subseteq \mathbb{Z}$ for which multiplication is positive existentially definable over $(\mathbb{Z}; 0, 1, +, =, R)$ is not obvious. As far as we know, the only unconditional result in this direction was obtained by Poonen and Shlapentokh [30], motivated by an application to extensions of Hilbert's tenth problem: they prove that multiplication is positive existentially definable in the structure

$$(\mathbb{Z}_{>0}; 1, +, =, \{2^n + n^2 : n \in \mathbb{Z}_{>0}\})$$

(see also Remark 3.17, *Ibid.*, where they mention a similar result by Matiyasevich).

No characterization of such sets R has been proposed. See below for some relevant references. Our main result addresses Problem 1 for $R \subseteq \mathbb{Z}$ being the image of an arbitrary univariate polynomial on $\mathbb{Z}$, and solves this case completely assuming the Bombieri-Lang conjecture; indeed, a consequence of it (the Caporaso-Harris-Mazur conjecture) is enough for our purposes. It turns out that the degree of the polynomial whose image is R is the only parameter involved in the classification. For the general case, we do not know what kind of invariants could be involved.

Before stating our results in a precise way, let us briefly recall the relevant Diophantine conjectures. In [5], Caporaso, Harris and Mazur have shown that the Bombieri-Lang conjecture (on rational points of varieties of general type) implies a very strong version of Faltings' Theorem. Namely, under the Bombieri-Lang conjecture, given a number field K and an integer $g \geq 2$, there exists a constant $M = M(g, K)$ such that every curve X defined over K with genus g has at most M rational points over K. Further work by Abramovich [1] and Pacelli [23] show that, under the Bombieri-Lang conjecture, the constant M should only depend on g and on the degree of K over $\mathbb{Q}$, not on the particular K. More precisely, the Bombieri-Lang conjecture implies the following (see Theorem 1.1 and Corollary 1.2 in [23]):

Conjecture 1.3 (Caporaso-Harris-Mazur; Abramovich; Pacelli)**.** *Let $g \geq 2$ and d be positive integers. There is a constant $M(g, d)$ such that for any number field K with $[K : \mathbb{Q}] \leq d$ and for any smooth projective curve X defined over K with genus g one has*

$$\#X(K) \leq M(g, d).$$

In the spirit of this conjecture, Poonen [29] has raised a number of striking questions for algebraic families of schemes over a base.

In [35], Stoll uses the Chabauty method to prove Conjecture 1.3 in the case of hyperelliptic curves under the assumption that the Mordell-Weil rank of the Jacobian of the curve is not too large (namely, at most $g - 3$). This has been recently extended to all curves satisfying the same condition on the rank of the Jacobian [12].

Let us introduce some notation. A *$\mathbb{Z}$-valued polynomial* is a polynomial in $\mathbb{Q}[t]$, say F, satisfying $F(\mathbb{Z}) \subseteq \mathbb{Z}$. The symbol R denotes a unary relation symbol. We consider the first order language $\mathcal{L} = \{0, 1, +, =, R\}$. Given a polynomial $F \in \mathbb{Q}[t]$, we denote by $\mathcal{R}_F$ the set $F(\mathbb{Z})$. In particular, when F is $\mathbb{Z}$-valued we may define the $\mathcal{L}$-structure $\mathfrak{Z}_F = (\mathbb{Z}; 0, 1, +, =, \mathcal{R}_F)$.

We will be interested in the positive existential theory of $\mathfrak{Z}_F$, and more generally in positive-existential definitions in this structure. Our main result is:

Theorem 1.4. *Assume Conjecture 1.3. Let $F \in \mathbb{Q}[t]$ be a $\mathbb{Z}$-valued polynomial of degree $n \geq 2$. Multiplication is positive-existentially $\mathcal{L}$-definable in $\mathfrak{Z}_F$. In particular, the positive existential theory of $\mathfrak{Z}_F$ is undecidable.*

We remark that the condition $n \geq 2$ cannot be dropped, because the theory of $\mathfrak{Z}_{at+b}$ is decidable for any $a, b \in \mathbb{Z}$.

The undecidability part of the statement follows from the fact that the positive existential theory of the ring $\mathbb{Z}$ is undecidable (as a consequence of DMPR Theorem). In more elementary terms, one can re-state the undecidability consequence as follows:

Corollary 1.5. *Assume Conjecture 1.3. Let $F \in \mathbb{Q}[t]$ be a $\mathbb{Z}$-valued polynomial of degree $n \geq 2$. The following problem is undecidable:*

Given a system of first degree polynomial equations with integral coefficients, decide whether or not it has a solution with some prescribed variables in $\mathcal{R}_F$.

Particular instances of the problem addressed in Theorem 1.4 have already attracted special attention. J. R. Büchi considered the case when $F(t) = t^2$ (see [15] and [21]). Even for this simple polynomial it is not known how to establish an unconditional version of Theorem 1.4. Nevertheless, Vojta [36] proved a version of Theorem 1.4 for $F(t) = t^2$ under the Bombieri-Lang conjecture for surfaces (instead of Conjecture 1.3). For the case of the polynomials $F(x) = x^n$ with $n \geq 2$, the first author [24] proves similar results, assuming a suitable version of the ABC conjecture instead. At this point let us mention that the technique in [36] is not suitable for the case of polynomials of degree ≥ 3, as it would involve the explicit computation of the special set of higher dimensional varieties of general type. Also, note that the technique in [24] fails in an essential way when F does not have repeated factors. Such restrictions do not arise in the present work.

If we consider the full theory instead of the positive existential theory, then much more is known. In [31, p. 50, Sect. 5], Putnam realized that one can easily define the squaring function from the set of squares in the natural numbers. Büchi [4] then noticed that Putnam's result can be generalized by induction, obtaining the following (here $\mathbb{N}$ stands for the set of non-negative integers): *Let $F \in \mathbb{Q}[t]$ be $\mathbb{Z}$-valued and let $\mathcal{R}'_F = F(\mathbb{N}) \cap \mathbb{N}$. If F has degree ≥ 2 and positive leading coefficient, then multiplication is $\mathcal{L}$-definable in the structure $\mathfrak{N}_F = (\mathbb{N}; 0, 1, +, =, \mathcal{R}'_F)$.* From this, undecidability of the full theory of $\mathfrak{N}_F$ follows unconditionally. The arguments of Putnam and Büchi strongly use universal quantifiers, and hence are not suitable in the positive existential context.

A main intermediate result needed for proving Theorem 1.4 is the following, which can be of independent interest.

Theorem 1.6. *Assume Conjecture 1.3. Let $F \in \mathbb{Q}[t]$ be a polynomial of degree $n \geq 2$. There is a positive integer N depending only on F such that the following holds:*

If $G \in \mathbb{Q}[t]$ has the same degree and same leading coefficient as F, and if it satisfies that $G(j) \in \mathcal{R}_F$ for each $j = 1, \dots, N$, then there is $\epsilon \in \{-1, 1\}$ and $b \in \mathbb{Z}$ such that $G(t) = F(\epsilon t + b)$.

We prove this theorem in Section 3. If in this theorem we only want to conclude that $G(t) = F(\alpha t + \beta)$ for some *complex numbers* α and β, then we need only assume that N depends on n rather than on F itself (see Theorem 3.6).

Let us briefly sketch the idea of the proof of Theorem 1.6: If $G(j) \in \mathcal{R}_F$ for $j = 1, \dots, N$, with N large, then this would produce many rational points in the plane curve X defined by $G(x) = F(y)$. If $G(t) = F(t + \nu)$ for some $\nu \in \mathbb{Q}$ then such rational points will obviously exist, and one would like that this is the only possible case where many rational points can appear. Namely, a naive hope would be that in any other case X is an irreducible curve of geometric genus $g \geq 2$ bounded in terms of n, so that (under Conjecture 1.3) N is bounded in terms of n. However, even if $G(t)$ is not of the form $F(t + \nu)$, the curve X can very well have components of geometric genus 0 or 1 due to the reducibility of X or to the presence of singularities, and one needs more work to get around these issues. One of the main strategies to make this argument work consists of an auxiliary construction that increases the genus of the irreducible components of X — see Section 2 and Proposition 3.1. It turns out that the outlined approach eventually leads to the conclusion that $G(t) = F(\alpha t + \beta)$ for some $\alpha, \beta \in \mathbb{C}$ (see Theorem 3.6), and at this point a rationality result (Proposition 3.3) of combinatorial nature leads to Theorem 1.6 — see Section 3.

For Theorem 1.4, it is crucial that the bound N does not depend on the polynomial G — see for instance the proof of Lemma 4.1. Section 4 is dedicated to proving Theorem 1.4. Basically, the idea is to construct a formula using Theorem 1.6 and difference operators — see the beginning of Section 4 for a brief outline of the argument. As a prototypical example of this approach, we refer to Büchi's idea (see [15]) in the case of $F(t) = t^2$ (see also [28, Theorem 2.4] and [26, Section 11] for the case $F(t) = t^n$). For general polynomials, some technicalities arise in the case of even degree. Except for the use of Theorem 1.6, the presentation in Section 4 is independent of the rest of the paper.

Nevertheless, if we allow N to also depend on G, then we obtain the following unconditional result through an easy adaptation of the end of the proof of Theorem 1.6 (by replacing the use of Conjecture 1.3 by Faltings' Theorem).

Corollary 1.7. *Let F and G in $\mathbb{Q}[t]$ be polynomials of the same degree and same leading coefficient. If $G(j) \in \mathcal{R}_F$ for all large enough integers j, then there is $\epsilon \in \{-1, 1\}$ and $b \in \mathbb{Z}$ such that $G(t) = F(\epsilon t+b)$.*

When we restrict to the case of $F(t) = t^n$, the result is well-known (see [33]). It should be noted, however, that Corollary 1.7 also follows from a theorem of Davenport-Lewis-Schinzel [7, Theorem 1] (with their notation, take $f(x, y)$ to be our $G(x) - F(y)$). The two proofs are of a completely different nature.

After the previous discussion, it is worth noting that the diophantine equation $F(x) = G(y)$ is a classical object of study in number theory, see for instance the article by Bilu and Tichy [3] and the references therein. However, the Bilu-Tichy theorem only gives valuable geometric information for curves of the form $f(x) = g(y)$ provided that they have infinitely many integral points. If the latter condition is not satisfied, such a curve can very well have components of genus zero without being related to the Bilu-Tichy standard pairs (see [3]). The number of integral points in these non-Bilu-Tichy curves can be arbitrarily large, even if both f and g are required to be in $\mathbb{Z}[t]$, of the same degree and monic. This is the case, for instance, for the curves defined by $x^n - ax^{n-1} = y^n - by^{n-1}$, for any given $n \geq 3$ and suitable choices of $a, b \in \mathbb{Z}$.

As we use a conjecture on uniformity to prove Theorem 1.4, it is natural to ask if it is possible (assuming a stronger conjecture if necessary) to find an $\mathcal{L}$-formula defining existentially multiplication in $\mathfrak{Z}_F$ which only depends on n but not on the particular F. Our proof of Theorem 1.4 does not give such a uniform definition, and indeed we will show the following unconditional result in Section 5.

Theorem 1.8. *Let $n \geq 2$ be an integer. There is no positive existential $\mathcal{L}$-formula $\phi(x, y, z)$ uniformly defining the relation $z = xy$ across the structures $\mathfrak{Z}_F$ as $F \in \mathbb{Q}[t]$ ranges over the set $\{at^n : a \in \mathbb{Z}_{>0}\}$. In particular, there is no uniform positive existential $\mathcal{L}$-definition of multiplication across the structures $\mathfrak{Z}_F$ as $F \in \mathbb{Q}[t]$ ranges over the set of all $\mathbb{Z}$-valued polynomials of degree n.*

We conclude this introduction with a few problems.

After the Theorem 1.8 and in view of the work by Putnam and Büchi discussed above, we propose the following problem.

Problem 1.9. *Let $n \geq 2$ be an integer. Is there a first-order $\mathcal{L}$-formula that uniformly defines multiplication across the structures $\mathfrak{Z}_F$ as $F \in \mathbb{Q}[t]$ ranges over the set of all $\mathbb{Z}$-valued polynomials of degree n?*

Let $R_1, \dots, R_m$ be unary relation symbols and consider the language $\mathcal{L}_m = \{0, 1, +, =, R_1, \dots, R_m\}$. Given $\mathbb{Z}$-valued polynomials $F_1, \dots, F_m \in \mathbb{Q}[t]$ we define the $\mathcal{L}_m$-structure $\mathfrak{Z}_{F_1,\dots,F_m} = (\mathbb{Z}; 0, 1, +, =, \mathcal{R}_{F_1}, \dots, \mathcal{R}_{F_m})$.

Problem 1.10. *Find polynomials $F_1, \dots, F_m$ such that multiplication can be positive-existentially defined in $\mathfrak{Z}_{F_1,\dots,F_m}$ without invoking any conjecture.*

In the particular case where $m = 2$, $F_1 = t^2$ and $F_2 = t^3$, this question was asked by L. Lipshitz (in oral communication with the second author). Even when the unary relations are not required to be the range of polynomials (but still are recursively enumerable sets), the only results that we are aware of are the one by Poonen and Shlapentokh [30] mentioned above, and by the first author in [25, Ch. 8], who proves that multiplication can be positive-existentially defined in the structures

$$(\mathbb{Z}; 0, 1, +, =, \mathcal{R}_{t^2}, \{p : p \text{ is prime}\}) \quad \text{and} \quad (\mathbb{Z}; 0, 1, +, =, \mathcal{R}_{t^2}, \{2^n : n \geq 0\}).$$

Finally, consider the following variation of Problem 1.2:

Problem 1.11. *Classify the recursive subsets $R \subseteq \mathbb{Z}^n$ for which the structure $(\mathbb{Z}; 0, 1, +, =, R)$ has undecidable positive existential theory.*

Any recursive R that works for Problem 1.2 yields an example for Problem 1.11, although it is not known whether the converse holds. In any case, these questions naturally arise, for instance, in the context of Hilbert's tenth problem for $\mathbb{Q}$: using an elliptic curve of rank 1 (for example) one can interpret $(\mathbb{Z}; 0, 1, +, =)$, and to show undecidability of the Diophantine theory of $\mathbb{Q}$ it would suffice to interpret (in such a model) a relation R for which the positive existential theory of $(\mathbb{Z}; 0, 1, +, =, R)$ is undecidable. The relevance of this approach is that nowadays it is widely believed that the set $\mathbb{Z}$ is not Diophantine in $\mathbb{Q}$, after a conjecture of Mazur [20, 22] and recent work of Koenigsmann [13]. On the other hand, the same conjecture of Mazur implies that no *bijective* Diophantine interpretation of $(\mathbb{Z}; 0, 1, +, \times, =)$ is possible in $\mathbb{Q}$ (cf. [6]), but this does not immediately rule out the possibility of using a relation R for which $(\mathbb{Z}; 0, 1, +, R, =)$ is undecidable.

2. Geometric preliminaries

In this section we prove some geometric results, mainly about polynomials in two variables and the plane curves that they define.

Lemma 2.1. *Let $F, G \in \mathbb{C}[t]$ be polynomials of the same degree $n \geq 1$. If $F(x) - G(y) \in \mathbb{C}[x, y]$ has a factor linear in x or y, then $G(t) = F(at + b)$ for some $a, b \in \mathbb{C}$ with $a \neq 0$.*

Proof. Assume without loss of generality that $F(x) - G(y)$ has a factor $P(x, y) = u(x)y - v(x)$ which is linear in y, with u and v coprime polynomials in the variable x. Substituting the formal variable y by the rational function $\frac{v(x)}{u(x)}$ in $F(x) - G(y)$, we obtain

$$F(x) - G\left(\frac{v(x)}{u(x)}\right) = 0.$$

Since $F = G(v/u)$ and G are polynomials of degree $n \geq 1$, we see that v/u has no pole in $\mathbb{C}$. As u and v are coprime, we deduce that u has no zero in $\mathbb{C}$, hence u is a constant. Comparing degrees, we conclude that v has degree one. Therefore, F and G are equal modulo a linear change of variable. □

Proposition 2.2. *Let $P(x, y) \in \mathbb{C}[x, y]$ be an irreducible polynomial which has degree at least 2 in y. Considering P as a polynomial in y with coefficients in $\mathbb{C}[x]$, let $\Delta(x) \in \mathbb{C}[x]$ be its discriminant. We have:*

1. *$\Delta(x)$ is not the zero polynomial, and*
2. *for any $\lambda \in \mathbb{C}$ that is not a zero of the polynomial Δ (namely, $\Delta(\lambda) \neq 0$), and for any integer $r \geq 1$, the polynomial $P(x^r + \lambda, y)$ is irreducible in $\mathbb{C}[x, y]$.*

(When P is irreducible and has degree 1 in y, the polynomial $P(x^r + \lambda, y)$ always is irreducible.)

Remark 2.3. *The following simple example can help to clarify the role of the discriminant in the proposition above. Consider $P(x, y) = xy^2 - 1$, which is irreducible and has the required degree in y. In this case $\Delta(x) = 4x$ and hence the proposition gives that $P(x^r + \lambda, y)$ is irreducible for all integers $r \geq 1$ and $\lambda \in \mathbb{C} \smallsetminus \{0\}$. Moreover, the only case when $\Delta(\lambda) = 0$ is $\lambda = 0$ for which we get $P(x^r + \lambda, y) = x^r y^2 - 1$, which is reducible for infinitely many r (indeed, all even integers r).*

We thank the anonymous referee for providing us the following proof for Proposition 2.2. It replaces a more laborious proof that we had in an earlier version of the manuscript.

Proof of Proposition 2.2. The polynomial $P(x, y)$ remains irreducible as an element of $\mathbb{C}(x)[y]$ by Gauss's lemma. As it is non-constant in y we can look at its roots in an algebraic closure of $\mathbb{C}(x)$; they are distinct because of irreducibility and because we are in characteristic zero. Therefore $\Delta(x)$ is not the zero polynomial.

Let us prove Item (2). Without loss of generality we can assume $\lambda = 0$, so that $\Delta(0) \neq 0$ (indeed, we may apply Item (2) with $\lambda = 0$ to the polynomial $\tilde{P}(x, y) = P(x + \lambda, y)$). We show that $P(x^r, y)$ is irreducible. Let us write $P(x, y) = a_d y^d + \cdots + a_0$ where $a_i \in \mathbb{C}[x]$ and $d \geq 2$ is the degree of P in

y. Let α be a root of $P(x,y)=0$ (seen as equation in y) in some fixed algebraic closure of $K:=\mathbb{C}(x)$ and let $u=x^{1/r}$ be in the same algebraic closure of K.

The discriminant of a binary form is SL_2-invariant. We apply this observation to the binary form $z^dP(x,y/z)\in K[y,z]$ using the action of $\mathrm{SL}_2(\mathbb{C})$, and we see that we can assume that α is integral above the place $v_0:=\mathrm{ord}_x$ of $\mathbb{C}(x)$ (i.e. it does not take the value ∞ above the place v_0). Such a transformation will not change the polynomial $\Delta(x)$, it will not change the fact that $P(x,y)$ is irreducible (although $P(x,y)$ might be different after such a transformation), the coefficients a_j will remain in $\mathbb{C}[x]$ and it will not change the irreducibility or reducibility of $P(x^r,y)$. Hence, we can assume that $v_0(a_d)=0$ in addition to the original setup, i.e. that α is integral above v_0.

Since $v_0(\Delta)=0$ (i.e. $\Delta(0)\neq 0$) we see that v_0 does not ramify in the extension $K(\alpha)/K$. On the other hand, v_0 is totally ramified in the extension $\mathbb{C}(u)/K$, hence, by [9, Lemma 2.5.8] we get that $K(\alpha)$ and $\mathbb{C}(u)$ are linearly disjoint over K. As P is irreducible we know $[K(\alpha):K]=d$, so by linear disjointness

$$dr=[K(\alpha):K][\mathbb{C}(u):K]=[K(\alpha,u):K]=[K(\alpha,u):\mathbb{C}(u)][\mathbb{C}(u):K]$$

hence $[K(\alpha,u):\mathbb{C}(u)]=d$. Therefore $P(x,y)$ remains irreducible in $\mathbb{C}(u)[y]$, that is, $P(u^r,y)$ is irreducible. Up to relabeling the variable u, this is exactly what we wanted. □

Corollary 2.4. *Let m,n be positive integers, with $n\geq 2$. There is a constant $c_0=c_0(m,n)$ such that the following holds:*

Let $P\in\mathbb{C}[x,y]$ be irreducible of bidegree (m,n). For any $\lambda\in\mathbb{C}$ with at most c_0 exceptions, and for any $r\geq 1$, the polynomial $P(x^r+\lambda,y)$ is irreducible.

This corollary will be combined with the following result in our applications.

Proposition 2.5. *Let m,n be positive integers, with $n\geq 2$. If $P\in\mathbb{C}[x,y]$ is an irreducible polynomial of bidegree (m,n), then there is $\lambda_0\in\mathbb{C}$ such that the following holds for every $r\geq 1$:*

For any $\lambda\in\mathbb{C}\setminus\{\lambda_0\}$ such that $Q_\lambda(x,y)=P(x^r+\lambda,y)$ is irreducible, the zero set of $Q_\lambda(x,y)$ is an irreducible plane curve of geometric genus $g\geq\frac{r}{2}+1-n$.

Proof. The basic idea is to apply the Riemann-Hurwitz formula to the map $(x,y)\mapsto x$ on the curve defined by $P(x^r+\lambda,y)=0$. We need many ramification points in order to give a lower bound for the genus, and they are obtained as follows: we find an initial one for the map $(x,y)\mapsto x$ on the curve $P(x,y)=0$ and then we make many copies of it by base-change by $x^r+\lambda$ for suitable λ. To make this work, however, one needs to work on the desingularization of projective closures. Unfortunately the previous idea produces ramification points on a curve that is not the one that we want to consider, and some care is necessary in order to conclude. See also the remark after the present proof.

Let $X\subseteq\mathbb{A}^2$ be the zero set of P; we will refer to the zero set of x in $\mathbb{A}^2$ as x-axis. Let X' be the Zariski-closure of X in $\mathbb{P}^1\times\mathbb{P}^1$. Since P is irreducible, X' is irreducible. The map $p\colon X\to\mathbb{A}^1$; $(x,y)\mapsto x$ from X to the x-axis extends to a morphism $\pi\colon X'\to\mathbb{P}^1$. Let $\nu\colon\widetilde{X'}\to X'$ be the normalization of X', so that $\widetilde{X'}$ is a smooth, irreducible, projective curve. The map $\pi\nu\colon\widetilde{X'}\to\mathbb{P}^1$ is finite of degree n as P has degree n on y. The map $\pi\nu$ has at least two branch points because $\deg(\pi\nu)=n\geq 2$. Hence, there is at least one branch point of $\pi\nu$ in the affine chart $\mathbb{A}^1$ of $\mathbb{P}^1$ given by the x-axis; let $\lambda_0\in\mathbb{A}^1$ be such a point. This λ_0 can be taken as the λ_0 of the statement. The next commutative diagram summarizes this construction.

$$\begin{tikzcd}
X \arrow[r] \arrow[d, "p"] & X' \arrow[d, "\pi"] & \widetilde{X'} \arrow[l, "\nu"'] \\
\mathbb{A}^1 \arrow[r] & \mathbb{P}^1 &
\end{tikzcd}$$

Choose any $\lambda\in\mathbb{C}\smallsetminus\{\lambda_0\}$ such that $Q_\lambda(x,y)=P(x^r+\lambda,y)$ is irreducible. Let $\rho':\mathbb{P}^1\to\mathbb{P}^1$ be the extension of the map $\rho:\mathbb{A}^1\to\mathbb{A}^1$ given by $x\mapsto x^r+\lambda$ on the x-axis. If we base-change the *square* in the previous diagram by ρ', then we obtain the following commutative diagram

$$\begin{tikzcd}
Y \arrow[rr] \arrow[dr, "h"] \arrow[dd, "q"'] & & Y' \arrow[dr, "h'"] \arrow[dd, "\varpi"' near start] & & \widetilde{Y'} \arrow[ll, "\mu"'] \arrow[dr, "\widetilde{h}"] & \\
& X \arrow[rr, dotted] \arrow[dd, dotted, "p"' near start] & & X' \arrow[dd, dotted, "\pi"] & & \widetilde{X'} \arrow[ll, dotted, "\nu"] \\
\mathbb{A}^1 \arrow[rr] \arrow[dr, "\rho"'] & & \mathbb{P}^1 \arrow[dr, "\rho'"'] & & & \\
& \mathbb{A}^1 \arrow[rr, dotted] & & \mathbb{P}^1 & &
\end{tikzcd}$$

where Y is the zero set of $Q_\lambda(x,y)$ in $\mathbb{A}^2$ (which is irreducible by assumption on λ), $q\colon Y \to \mathbb{A}^1$ is given by $(x,y) \mapsto x$, Y' is the projective closure of Y in $\mathbb{P}^1 \times \mathbb{P}^1$ (hence, irreducible), ϖ is the extension of q, the maps h and h' are induced by base change, $\mu\colon \widetilde{Y'} \to Y'$ is the normalization map, and $\widetilde{h}\colon \widetilde{Y'} \to \widetilde{X'}$ is by definition the map obtained from the universal property of normalization (of the curve X') applied to $h'\mu\colon \widetilde{Y'} \to X'$ (in general, this is *not* induced by base change by ρ'). More precisely, h is the map induced by

$$\begin{array}{ccc} \mathbb{C}[x,y]/(P) & \to & \mathbb{C}[x,y]/(Q_\lambda) \\ x & \mapsto & x^r + \lambda \\ y & \mapsto & y \end{array} .$$

The diagram commutes because the cube is obtained by base change, and $\tilde{h}$ satisfies $\nu\tilde{h} = h'\mu$ by definition.

Note that $\widetilde{Y'}$ is a smooth projective model of Y. Therefore, by definition of geometric genus we must show that the genus g of $\widetilde{Y'}$ satisfies $g \geq r/2 + 1 - n$.

Consider $\xi = \pi\nu\colon \widetilde{X'} \to \mathbb{P}^1$ and $\zeta = \varpi\mu\colon \widetilde{Y'} \to \mathbb{P}^1$ as rational functions (both of which have degree n, the degree in y of P and Q_λ), and note that by commutativity of the previous diagram we have $\tilde{h}^*\xi = \xi\tilde{h} = \rho'\zeta = \zeta^r + \lambda$. Also note that ρ' is branched exactly at λ and ∞, and it is otherwise étale. In particular, it is étale above a neighborhood U of λ_0. Let b be one of the r preimages of λ_0 by ρ', and observe that b is not 0 because $\rho'(0) = \lambda \neq \lambda_0$. Let $\mathfrak{p} \in \xi^{-1}(\lambda_0) \subseteq \widetilde{X'}$ be such that ξ ramifies at $\mathfrak{p}$; it exists because λ_0 is a branch point for ξ. Before we continue with the argument, we need the following:

Claim 2.6. *There exists $\mathfrak{q} \in \widetilde{Y'}$ such that $\tilde{h}(\mathfrak{q}) = \mathfrak{p}$ and $\zeta(\mathfrak{q}) = b$.*

Proof of the claim. Indeed, consider the open sets $U' = \rho'^{-1}U$, $W = \pi^{-1}U \subseteq X'$ and $W' = \xi^{-1}U = \nu^{-1}W \subseteq \widetilde{X'}$, and recall that $\rho'|_{U'} : U' \to U$ is étale (by choice of U). Note that $b \in U'$ and $\mathfrak{p} \in W'$. Since $\varpi : Y' \to \mathbb{P}^1$ is the base change of $\pi : X' \to \mathbb{P}^1$ by ρ', we have that the fibered product $V = U' \times_U W$ is an open set of Y', and since $\rho'|_{U'} : U' \to U$ is étale we get that $h'|_V : V \to W$ is étale. On the other hand, W' is smooth (as $\widetilde{X'}$ is smooth) and $\nu|_{W'} : W' \to W$ is birational (because ν is the normalization map), therefore by properties of étale base change we conclude that $V' := V \times_W W'$ is smooth and the projection $V' \to V$ is birational. Therefore, V' is included as a dense open subset $i : V' \to \widetilde{Y'}$ in such a way that the following diagram commutes:

$$\begin{tikzcd}
& Y' & & \widetilde{Y'} \arrow[ll, "\mu"] \arrow[dd, "\widetilde{h}"] \\
U' \arrow[d] & V \arrow[l] \arrow[u, hook] \arrow[d] & V' \arrow[l] \arrow[ur, hook, "i"'] \arrow[d] & \\
U & W \arrow[l] & W' \arrow[l] \arrow[r, hook] & \widetilde{X'}
\end{tikzcd}$$

Finally, since $b \in U'$, $\mathfrak{p} \in W'$, $\xi|_{W'}(\mathfrak{p}) = \rho'|_{U'}(b) = \lambda_0 \in U$ and $V' = V \times_W W' = U' \times_U W'$, we get that there is a point $\mathfrak{q}_0 \in V'$ mapped to b and $\mathfrak{p}$ by the projections of V', hence we can take $\mathfrak{q} = i(\mathfrak{q}_0)$. □

Fix a local parameter t at $\mathfrak{p}$ and a local parameter s at $\mathfrak{q}$. Working in the completion of the local rings at $\mathfrak{p}$ and $\mathfrak{q}$ we obtain $h^*t = u \cdot s^e$ for some unit $u \in \widehat{\mathcal{O}}^{\times}_{\widetilde{Y'},\mathfrak{q}}$ and some integer $e \geq 1$ (analyzing the proof of the previous claim one can see that $e = 1$, but we don't need this fact). Since $h^*dt = d(h^*t)$, we deduce $h^*dt = e \cdot u \cdot s^{e-1}ds$ (we remark that $\cdot$ denotes multiplication, as opposed to composition).

Write $e_{\mathfrak{p}}$ for the ramification index of $\mathfrak{p}$ with respect to ξ and $e_{\mathfrak{q}}$ for the ramification of $\mathfrak{q}$ with respect to ζ. Thus, $d\xi = v \cdot t^{e_{\mathfrak{p}}-1}dt$ for some unit $v \in \widehat{\mathcal{O}}^{\times}_{\widetilde{X'},\mathfrak{q}}$, and $d\zeta = w \cdot s^{e_{\mathfrak{q}}-1}ds$ for some unit $w \in \widehat{\mathcal{O}}^{\times}_{\widetilde{Y'},\mathfrak{q}}$. On the one hand, we have

$$\begin{aligned} d(\zeta^r + \lambda) &= d(h^*\xi) = h^*d\xi = h^*(v \cdot t^{e_{\mathfrak{p}}-1}dt) \\ &= (h^*v) \cdot (h^*t)^{e_P - 1} h^*dt \\ &= (h^*v) \cdot u^{e_{\mathfrak{p}}-1} \cdot s^{e(e_{\mathfrak{p}}-1)} \cdot e \cdot u \cdot s^{e-1}ds \\ &= \alpha \cdot s^{ee_{\mathfrak{p}}-1}ds \end{aligned}$$

for some unit $\alpha \in \widehat{\mathcal{O}}^{\times}_{\widetilde{Y'},\mathfrak{q}}$. On the other hand, we have

$$d(\zeta^r + \lambda) = r\zeta^{r-1}d\zeta,$$

where $r\zeta^{r-1} \in \widehat{\mathcal{O}}^{\times}_{\widetilde{Y'},\mathfrak{q}}$ is a unit, because $\zeta(\mathfrak{q}) = b \neq 0$. Therefore, we have

$$d\zeta = \beta s^{ee_{\mathfrak{p}}-1}ds$$

for some unit $\beta \in \widehat{\mathcal{O}}^{\times}_{\widetilde{Y'},\mathfrak{q}}$, and we deduce that $e_{\mathfrak{q}} = ee_{\mathfrak{p}}$. Since $e \geq 1$ and $\mathfrak{p}$ is ramified (hence $e_{\mathfrak{p}} \geq 2$), we conclude that $\mathfrak{q}$ is ramified with respect to ζ and hence b is a branch point for ζ.

We deduce that ζ has at least r branch points (b was any of the r preimages of λ_0 by ρ'). The Riemann-Hurwitz formula applied to $\zeta : \widetilde{Y'} \to \mathbb{P}^1$ then gives $2n = 2\deg(\zeta) \geq 2 - 2g + r$ and we conclude $g \geq r/2 + 1 - n$. □

Remark 2.7. *The main complication in the previous proof is that $\widetilde{Y'} \neq Y' \times_{X'} \widetilde{X'}$ in general. Even worse, we don't have a map $Y' \times_{X'} \widetilde{X'} \to \widetilde{Y'}$ compatible with the respective morphisms to Y' and $\widetilde{X'}$ (note that in Claim 2.6 we constructed such a map, but only on a suitable open set). Indeed, one can consider for instance $P(x, y) = x^2 - y^2 - 1$, $r = 3$, $\lambda = 1$. In this case X' is smooth hence ν can be taken as the identity map, while Y' is (irreducible and) singular, hence $Y' \times_{X'} \widetilde{X'} \simeq Y'$ is singular and there is no compatible map to its normalization $\widetilde{Y'}$.*

3. The equation $G(x) = H(y)$

We first prove a proposition which can have other applications in the study of diophantine equations of the form $G(x) = H(y)$.

Proposition 3.1 (Controling the genus)**.** *Let $n \geq 2$ be an integer. There is a constant $c_1 = c_1(n)$ such that the following holds:*

Let $F, G \in \mathbb{C}[t]$ be polynomials of degree n. Suppose that $G(t)$ is not of the form $F(at + b)$ with $a, b \in \mathbb{C}$ and $a \neq 0$. For any $\lambda \in \mathbb{C}$ with at most c_1 exceptions and for any $r \geq 1$, the zero set of $G(x^r + \lambda) - F(y)$ is a plane curve whose irreducible components X_i have geometric genus g_i satisfying

$$\frac{r}{2} + 1 - n \leq g_i \leq \frac{(nr-1)(nr-2)}{2}.$$

Proof. First note that the upper bound follows from the Plücker genus formula for plane curves.

Let

$$G(x) - F(y) = \prod P_i^{s_i}(x, y)$$

be the factorization in irreducibles of $G(x) - F(y) \in \mathbb{C}[x, y]$. By Corollary 2.4, for each i, there exists a constant $c_{0,i}$ depending only on the bidegree (m_i, n_i) of P_i such that for any λ with at most $c_{0,i}$ exceptions and for any $r \geq 1$, the polynomial $P_i(x^r + \lambda, y)$ is irreducible. By Lemma 2.1, none of the P_i is linear in x or in y, hence in particular we have $n_i \geq 2$. By Proposition 2.5, the polynomial $P_i(x^r+\lambda, y)$ defines a plane irreducible curve of geometric genus

$$g_i \geq \frac{r}{2} + 1 - n_i \geq \frac{r}{2} + 1 - n \tag{1}$$

for any λ with at most $c_{0,i}+1$ exceptions. Note that since each $c_{0,i}$ is bounded from above by a function that depends only on n (because each m_i and n_i is bounded from above by n), we can choose c_1 depending only on n large enough so that $c_1 \geq \sum_i (1+c_{0,i})$, hence insuring that Equation (1) is valid for each i. □

The next proposition is an easy exercise in Galois theory.

Proposition 3.2. *Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$. Let $H \in \mathbb{Q}[x,y]$ be a polynomial of total degree D. Suppose that $P \in \overline{\mathbb{Q}}[x,y]$ is an irreducible polynomial with at least one non-zero coefficient in $\mathbb{Q}$ and such that P divides H in $\overline{\mathbb{Q}}[x,y]$. Let K be the number field generated over $\mathbb{Q}$ by the coefficients of P. We have $[K:\mathbb{Q}] \leq D$.*

Before we can prove Theorem 1.6, we need one more result:

Proposition 3.3 (Rationality)**.** *Let $F(t) \in \mathbb{Q}[t]$ be a polynomial of degree $n \geq 2$. There is a constant $N = N(F)$ with the following property:*

If a polynomial $G(t) \in \mathbb{Q}[t]$ satisfies the conditions

(i) *G has degree n and it has the same leading coefficient as F,*
(ii) *there are $\alpha, \beta \in \mathbb{C}$ such that $G(t) = F(\alpha t + \beta)$, and*
(iii) *$G(1), G(2), \dots, G(N)$ belong to $F(\mathbb{Z})$,*

then there is $\epsilon \in \{-1,1\}$ and $\nu \in \mathbb{Z}$ such that $G(t) = F(\epsilon t + \nu)$.

Example 3.4. *Choosing $F(t) = t^4 - 3t^2$ and $G(t) = F(it-2i) = t^4 - 8t^3 + 27t^2 - 44t + 28 \in \mathbb{Q}[t]$, we have $G(1) = 4 = F(2)$ and $G(2) = 0 = F(0)$, and $G(3) = 4 = F(2)$. So in this case $N(F) \geq 4$.*

Remark 3.5. *In general, we don't know whether $N(F)$ can be taken just in terms of n (uniformly on the coefficients of F). Nevertheless, the uniformity on G provided by this proposition is enough for our applications.*

Before proceeding with the proof, let us briefly outline the main steps that guide the computations. One supposes that G is given satisfying (i),(ii) and (iii) for some N, the goal then being to bound N only in terms of F. From conditions (ii) and (iii), there exist integers ℓ_k such that $F(\alpha k+\beta) = G(k) = F(\ell_k)$, for $k = 1, \dots, N$.

- The first part of the argument consists of showing that for "most" $k \in I_N := \{1,\dots,N\}$ one has that $\alpha k + \beta$ is approximately equal to $\xi_k \ell_k$ for suitable n-th roots of unity ξ_k depending on k — see the inequality (5) below.
- Then we observe that there is a root of unity α' and a complex number β' such that for "many" values of $k \in I_N$ one has that ℓ_k is approximately equal to $\alpha' k + \beta'$ — see the inequality (6) below. In fact, immediately after this point we will show that $\alpha' \in \{-1,1\}$, so that we can choose ε to be α'.
- Fixing certain j_0 and looking at the approximations for $\ell_k - \ell_{j_0}$ obtained in the previous step, one deduces that there is $\nu \in \mathbb{Z}$ such that for "several" values of $k \in I_N$ one has an exact equality $\ell_k = \epsilon k + \nu$, cf. Equation (7). Once this is done, it will be easy to conclude.

Of course, it is important to keep track of how the bounds depend on the various parameters so that at the end N only depends on F.

Proof of Proposition 3.3. We will treat N as a parameter and we will show that it can be chosen just in terms of F (we will give a concrete value of N at the end of the proof).

Assume that for certain G the three conditions (i), (ii), (iii) are satisfied. First note that because the leading term of $G(t) = F(\alpha t + \beta)$ is the same as the one of $F(t)$, we have $\alpha^n = 1$.

Let c be the leading coefficient of F, let H be the maximum of the absolute values of the coefficients of F and put $H' = \frac{nH}{|c|}$. Write $I_N = \{1, 2, \dots, N\}$. For $k \in I_N$ choose an integer ℓ_k such that $G(k) = F(\ell_k)$.

Write $F(t)=ct^n+\sum_{i=0}^{n-1} f_it^i$ and $q_k=\max\{|\ell_k|,|\alpha k+\beta|\}$. Since $F(\ell_k)=G(k)=F(\alpha k+\beta)$ we have

$$\begin{aligned}|c|\cdot|\ell_k^n-(\alpha k+\beta)^n| &= \left|\sum_{i=0}^{n-1} f_i(\ell_k^i-(\alpha k+\beta)^i)\right| \le H\sum_{i=0}^{n-1}|\ell_k^i-(\alpha k+\beta)^i|\\ &\le 2H\sum_{i=0}^{n-1}\max\{|\ell_k|^i,|\alpha k+\beta|^i\}\le 2H\sum_{i=0}^{n-1}q_k^i\\ &\le 2Hnq_k^{n-1}\end{aligned}$$

hence

$$|\ell_k^n-(\alpha k+\beta)^n|\le 2H'\max\{|\ell_k|,|\alpha k+\beta|\}^{n-1}. \tag{2}$$

Suppose that $|\alpha k+\beta|>(4H'+2)^{1/n}|\ell_k|$, hence

$$\frac{1}{2}|\alpha k+\beta|^n>(2H'+1)|\ell_k|^n, \tag{3}$$

so that

$$|\ell_k^n-(\alpha k+\beta)^n|\ge|\alpha k+\beta|^n-|\ell_k|^n>\frac{1}{2}|\alpha k+\beta|^n+2H'|\ell_k|^n\ge\frac{1}{2}|\alpha k+\beta|^n+2H'|\ell_k|^{n-1}$$

where the strict inequality comes from Equation (3), and because $\ell_k\in\mathbb{Z}$. Combining this estimate with (2) we would get

$$|\alpha k+\beta|^n\le -4H'|\ell_k|^{n-1}+4H'\max\{|\ell_k|,|\alpha k+\beta|\}^{n-1}\le 4H'|\alpha k+\beta|^{n-1}$$

which can only happen if $|\alpha k+\beta|\le 4H'$. Since $|\alpha|=1$ we see that this can happen for at most $8H'+1$ values of $k\in I_N$; call E this exceptional set, so that $\#E\le 8H'+1$. Therefore, we have proved that for each $k\in I_N-E$ we have

$$|\alpha k+\beta|\le(4H'+2)^{1/n}|\ell_k|.$$

Note that since F has degree n, we can have $\ell_k=0$ for at most n values of $k\in I_N$. Enlarge E to a set E' in order to include these values of k, so that $\#E'\le 8H'+n+1$ and for each $k\in I_N-E'$ we have

$$|\alpha k+\beta|\le(4H'+2)^{1/n}|\ell_k|\quad\text{ and }\quad \ell_k\neq 0. \tag{4}$$

Let μ_n be the set of n-th roots of 1. For each k, choose $\xi_k\in\mu_n$ that minimizes the quantity

$$\left|\frac{\alpha k+\beta}{\ell_k}-\xi_k\right|.$$

The distance between $x=\frac{\alpha k+\beta}{\ell_k}\in\mathbb{C}$ and the closest $\xi\in\mu_n\smallsetminus\{\xi_k\}$ to ξ_k is at least a half of the distance $|\xi_k-\xi|$. Examining the n-th roots of unity we see that $n|\xi_k-\xi|\ge 2$ for $n\ge 2$, so we have $n|x-\xi|\ge 1$. In particular, for all $\xi\in\mu_n$ with $\xi\neq\xi_k$ we have

$$\left|\frac{\alpha k+\beta}{\ell_k}-\xi\right|\ge\frac{1}{n}.$$

We deduce

$$\begin{aligned}|\ell_k^n-(\alpha k+\beta)^n| &= |\ell_k|^n\left|\left(\frac{\alpha k+\beta}{\ell_k}\right)^n-1\right|\\ &= |\ell_k|^n\left|\prod_{\xi\in\mu_n}\left(\frac{\alpha k+\beta}{\ell_k}-\xi\right)\right|\\ &\ge |\ell_k|^n\left|\frac{\alpha k+\beta}{\ell_k}-\xi_k\right|\frac{1}{n^{n-1}}\\ &= \frac{|\ell_k|^{n-1}}{n^{n-1}}|\alpha k+\beta-\xi_k\ell_k|.\end{aligned}$$

We obtain

$$|\alpha k+\beta-\xi_k\ell_k|\le \frac{n^{n-1}}{|\ell_k|^{n-1}}|\ell_k^n-(\alpha k+\beta)^n|\le 2n^{n-1}H'\max\left\{1,\left|\frac{\alpha k+\beta}{\ell_k}\right|\right\}^{n-1}$$

by Equation (2). Therefore, for each $k\in I_N-E'$ we have from Equation (4)

$$|\alpha k+\beta-\xi_k\ell_k|\le 2n^{n-1}H'(4H'+2)^{(n-1)/n}=:K_F \tag{5}$$

where K_F only depends on F.

Put $\alpha_k=\alpha/\xi_k$ and $\beta_k=\beta/\xi_k$, so that for each $k\in I_N-E'$ we have

$$|\alpha_k k+\beta_k-\ell_k|\le K_F$$

since $|\xi_k|=1$. Note that ξ_k varies in μ_n. The pigeonhole principle shows that there is a set $I'\subseteq I_N$ with $\#I'\ge N/n$ and there is $\zeta\in\mu_n$ such that for all $k\in I'$ we have $\xi_k=\zeta$. Let $\alpha'=\alpha/\zeta$ and $\beta'=\beta/\zeta$, so that for all $k\in I'$ we have $\alpha_k=\alpha'$ and $\beta_k=\beta'$. Hence, for all $k\in I'-E'$ we get

$$|\alpha' k+\beta'-\ell_k|\le K_F. \tag{6}$$

Fix $j_0\in I'-E'$. For each $k\in I'-E'$ we have

$$|\alpha'(k-j_0)-(\ell_k-\ell_{j_0})|\le|\alpha' k+\beta'-\ell_k|+|\alpha' j_0+\beta'-\ell_{j_0}|<2K_F.$$

We claim that if $N\gg_F 1$, then $\alpha'\in\{-1,1\}$. By contradiction, suppose that $\alpha'\notin\{-1,1\}$ and recall that $\alpha'\in\mu_n$ (indeed, $\alpha'^n=1$). Then $|\Im(\alpha')|>1/n$ and we would have for each $k\in I'-E'$

$$2K_F\ge|\alpha'(k-j_0)-(\ell_k-\ell_{j_0})|\ge|\Im(\alpha'(k-j_0)-(\ell_k-\ell_{j_0}))|=|\Im(\alpha'(k-j_0))|\ge\frac{|k-j_0|}{n}.$$

Suppose that

$$N\ge(4nK_F+8H'+3n+1)n.$$

Since $\#(I'-E')\ge N/n-8H'-n-1$, if we choose $k_0\in I'-E'$ satisfying $|k_0-j_0|\ge\frac{1}{2}\#(I'-E')$ (which is always possible) then we would get

$$2K_F\ge\frac{|k_0-j_0|}{n}\ge\frac{N/n-8H'-n-1}{2n}\ge\frac{4nK_F+2n}{2n}=2K_F+1$$

which is a blatant contradiction. Therefore, if $N\ge(4nK_F+8H'+3n+1)n$ (which we assume from now on) then $\alpha'\in\{-1,1\}$.

Knowing that $\alpha'=\pm1$, we revisit the inequality

$$|\alpha'(k-j_0)-(\ell_k-\ell_{j_0})|<2K_F$$

which is valid for $k\in I'-E'$. Writing $\gamma_k=\alpha'(k-j_0)-(\ell_k-\ell_{j_0})$, we have $\gamma_k\in\mathbb{Z}$ because $\alpha'=\pm1$. Moreover we have $|\gamma_k|<2K_F$. Invoking the pigeonhole principle once again, we see that there is $J\subseteq I'-E'$ with

$$\#J\ge\frac{1}{4K_F+1}\#(I'-E')$$

and there is an integer $\gamma\in[-2K_F,2K_F]$ such that for each $k\in J$ we have $\gamma_k=\gamma$. Therefore, for each $k\in J$ we get

$$\alpha'(k-j_0)-(\ell_k-\ell_{j_0})=\gamma$$

which means

$$\ell_k=\alpha' k+\nu \tag{7}$$

where $\nu=\ell_{j_0}-\alpha' j_0-\gamma\in\mathbb{Z}$ and $\alpha'=\pm1$. This is the ν from the statement of the result (and $\epsilon=\alpha'$).

Finally, we need to show that $G(t)=F(\alpha' t+b)$. Since F and G have degree n, it suffices to check the equality $G(k)=F(\alpha' k+\nu)$ for at least $n+1$ values of k. We assume that

$$N\ge(2n(4K_F+1)+8H'+n+1)n.$$

Note that it is compatible with our previous assumption on N. Moreover, it implies

$$\#J\ge\frac{1}{4K_F+1}\#(I'-E')\ge 2n.$$

It turns out that for each $k \in J$ we have $\ell_k = \alpha' k + \nu$ and hence

$$F(\alpha' k + \nu) = F(\ell_k) = G(k)$$

for at least $2n$ values of k, as we needed.

This proves the result with $N = \lceil (2n(4K_F + 1) + 8H' + n + 1)n \rceil$. □

We conclude this section with a "geometric" version of Theorem 1.6 (which enjoys of some additional uniformity). This, together with Proposition 3.3, immediately implies Theorem 1.6. Note that Conjecture 1.3 has not been used so far.

Theorem 3.6. *Assume Conjecture 1.3. Let $F \in \mathbb{Q}[t]$ be a polynomial of degree $n \geq 2$ and write $\mathcal{R}_F = F(\mathbb{Z})$. There is a positive integer N depending only on n (not on the particular F) such that the following holds: If $G \in \mathbb{Q}[t]$ has the same degree and same leading coefficient as F, and if it satisfies that $G(j) \in \mathcal{R}_F$ for each $j = 1, \ldots, N$, then there are $\alpha, \beta \in \mathbb{C}$, with $\alpha \neq 0$, such that $G(t) = F(\alpha t + \beta)$.*

Proof. We prove (by contradiction) that if $G(j) \in \mathcal{R}_F$ for $j = 1, \ldots, N$, then $G = F(\alpha t + \beta)$ for some complex numbers $\alpha \neq 0$ and β. Here, N is a constant depending only on n (not on F or G) whose value will be given in the proof.

Suppose that $G(t)$ is not of the form $F(\alpha t + \beta)$, with $\alpha, \beta \in \mathbb{C}$ and $\alpha \neq 0$. Let $r = 2n + 2$. By Proposition 3.1, there exists $c_1 = c_1(n)$ such that for every $\lambda \in \mathbb{C}$ with at most c_1 exceptions, the zero set of $G(x^r + \lambda) - F(y)$ is a plane curve whose irreducible components X_i have geometric genus g_i satisfying

$$2 = \frac{r}{2} + 1 - n \leq g_i \leq \frac{(nr-1)(nr-2)}{2} < 5n^4.$$

Therefore, there exists an integer $\lambda \in \{0, 1, \ldots, c_1\}$ such that the above holds. Fix such a λ.

By Proposition 3.2, for each irreducible factor $P \in \bar{\mathbb{Q}}[x, y]$ of $G(x^r + \lambda) - F(y) \in \mathbb{Q}[x, y]$ having a non-zero coefficient in $\mathbb{Q}$, there is a number field of degree $\leq nr = n(2n + 2)$ over $\mathbb{Q}$ which contains all the coefficients of P. Let K be the field generated by all these (finitely many) number fields and note that all the irreducible components X_i are defined over K. Since there are at most nr irreducible factors of $G(x^r + \lambda) - F(y)$, the degree of K over $\mathbb{Q}$ is at most $d = (nr)^{nr}$.

Since we are assuming Conjecture 1.3, for each i there exists a constant $M_i = M(g_i, d)$ such that $\#X_i(K) \leq M_i$ (recall that $g_i \geq 2$). Since each g_i is bounded by a function of n (namely, $g_i < 5n^4$) and since $d = (nr)^{nr} = (n(2n + 2))^{n(2n+2)}$, we see that each M_i can be bounded in terms of n independently of the particular polynomials F and G. Hence there exists M' depending only on n such that $M' > \max_i M_i$.

Choose $N = (nM')^r + c_1$ (which depends only on n). The hypothesis that for each $j = 1, \ldots, N$ the value $G(j)$ is in the range of F implies that $G(x) - F(y)$ has at least N rational points over $\mathbb{Q}$. Since $1 + \lambda$, $2^r + \lambda$, ..., $(nM')^r + \lambda$ are x-coordinates of $\mathbb{Q}$-rational points of $G(x) - F(y)$ we see that 1, 2, ..., nM' are x-coordinates of $\mathbb{Q}$-rational points of $G(x^r + \lambda) - F(y)$. On the other hand, since y appears in every factor of $G(x^r + \lambda) - F(y)$, and because the latter has degree n in y, there are at most n curves X_i. By the pigeon-hole principle, there is a curve X_i with at least M' points with coordinates in $\mathbb{Q}$, hence in K. This contradicts the definition of M'.

Therefore, under Conjecture 1.3, for $N = (nM')^r + c_1$ (which only depends on n), we have: for every $F, G \in \mathbb{Q}[t]$ of degree n such that $G(j) \in \mathcal{R}_F$ for $j = 1, \ldots, N$, there exist $\alpha, \beta \in \mathbb{C}$ with $\alpha \neq 0$ such that $G(t) = F(\alpha t + \beta)$. □

4. Consequences in Logic

The objective of this section is to prove Theorem 1.4. The basic idea can be summarized in the following steps:

(A) Multiplication can be positive-existentially defined from addition and the squaring function $n \mapsto n^2$, thanks to the elementary observation that $z = xy$ if and only if $(x + y)^2 = x^2 + 2z + y^2$. It turns out that the squaring function can be positive-existentially defined from *any* polynomial function $n \mapsto G(n)$ with G a polynomial of degree ≥ 2, by a linear algebra argument.

(B) Our language can express the image of a polynomial F, but *a priori* not the polynomial function. Nevertheless, from Theorem 1.6 and using difference operators (whose definition will be recalled below) we will see that (under Conjecture 1.3) one can "almost" define for some fixed N the N-ary relation: $u_1, \dots, u_N$ are consecutive values of F, meaning that there is $\nu \in \mathbb{Z}$ with $u_j = F(j + \nu)$ for $1 \le j \le N$.

(C) Using difference operators once again, one can recover ν from a sequence of values $u_1, \dots, u_N$ as in the previous item. Thus, we see that the relation $\{(x, y) : \exists \nu \in \mathbb{Z}, x = \nu+1 \text{ and } y = F(1+\nu)\}$ can be defined, and this is precisely the graph of the polynomial function F.

In practice, however, the previous steps will be used in a different order, but the underlying idea is the same as the one just outlined. We will first deal with the case where F has odd degree (which turns out to be much simpler) as it gives a general idea on how the previous strategy works. In the case of even degree we will need some preliminary work on difference operators, because step (B) does not work exactly as expected (there is a sign indeterminacy) leading to some complications in step (C). For the convenience of the reader, let us recall here the basic setup of difference operators. A more refined analysis will be given in Section 4.2. We will mainly focus on interpolation aspects of these operators.

Given a sequence $\sigma = (u_1, \dots, u_n)$ of integers (or more generally, of elements of some abelian group), the first (forward) difference of σ is the sequence

$$\Delta^1(\sigma) = (u_2 - u_1, \dots, u_n - u_{n-1}).$$

For $p < n$, the p-th difference of σ is inductively defined by

$$\Delta^p(\sigma) = \Delta^1(\Delta^{p-1}(\sigma)).$$

We will refer to Δ^p as to *the p-forward difference operator*. For instance, the second difference of σ is the sequence

$$(u_3 - 2u_2 + u_1, \dots, u_n - 2u_{n-1} + u_{n-2}).$$

Note that for a sequence $\sigma = (G(1), \dots, G(n))$, where G is a polynomial of degree d and leading coefficient a, we have $\Delta(\sigma) = (H(1), \dots, H(n-1))$, where H is a polynomial of degree $d-1$ and leading coefficient da. A key elementary fact about difference operators is that the converse holds: for instance, if σ has p-th difference equal to a constant sequence, say $(b, \dots, b)$, then there exists a polynomial G of degree p and leading coefficient $b/p!$ such that $\sigma = (G(1), \dots, G(n))$.

4.1. Case of odd degree.

Let F be a $\mathbb{Z}$-valued polynomial of odd degree $n \ge 2$, with leading coefficient a. Since the family of polynomials $\{F(t), \dots, F(t+n)\}$ forms a $\mathbb{Q}$-basis of the vector space of polynomials in $\mathbb{Q}[t]$ of degree at most n, there exist rational numbers $\alpha_0, \dots, \alpha_n$, and $\gamma_0, \dots, \gamma_n$ (depending only on F) such that

$$t = \sum_{j=0}^{n} \gamma_j F(t+j) \qquad \text{and} \qquad t^2 = \sum_{j=0}^{n} \alpha_j F(t+j).$$

Let $N \ge n$ be the integer that comes from Theorem 1.6. Let $\psi(x, y)$ be the $\mathcal{L}$-formula

$$\exists u_1, \dots, u_N \left(\bigwedge_{i=1}^{N} R u_i \wedge \Delta^{(n)}\left((u_i)_1^N\right) = (a \cdot n!)_i \wedge x = \sum_{j=0}^{n} \gamma_j u_j \wedge y = \sum_{j=0}^{n} \alpha_j u_j \right).$$

For simplicity, in writing this $\mathcal{L}$-formula, we have made some slight abuses of notation (which are standard) and that we now clarify:

- Fixed natural numbers can appear in the formula, as they could be replaced by a sum of ones (this allows us to write the natural number $a \cdot n!$).
- We can multiply a variable u_j by a fixed natural number, as it stands for a fixed sum of the variables.
- In each of the items above, one can replace 'natural number' by 'integer': we can gather on each side of an equation the positive terms.
- The fact that the γ_j and α_j are rational numbers is not an issue, as we can multiply the equations where they appear by a common multiple of their denominators.

- The condition on the n-th difference is also not an issue, as it can be rewritten as a conjunction of linear equations in the variables u_i.

Similar remarks apply to most formulas in this section.

The following lemma says that the graph of the squaring function is positive-existentially definable over the language $\mathcal{L}$.

Lemma 4.1. *The formula $\psi(x, y)$ is satisfied in $\mathbb{Z}$ if and only if $y = x^2$.*

Proof. First recall that the subformula Ru_i of ψ is interpreted by '$u_i \in \mathcal{R}_F$' in the $\mathcal{L}$-structure $\mathfrak{Z}_F$.

If $y = x^2$, then $\psi(x, y)$ is satisfied in $\mathbb{Z}$ by choosing $u_i = F(i + x)$ for each i.

Suppose that the formula is satisfied in $\mathbb{Z}$. Since the n-th difference of the sequence $(u_i)_i$ is constant and equal to $a \cdot n!$, there exists a polynomial G of degree n and leading coefficient a such that $G(i) = u_i$ for each $i = 1, \dots, N$. Since $G(i) = u_i \in \mathcal{R}(F)$ for each i, we deduce from Theorem 1.6 that there exists $\epsilon \in \{-1, 1\}$ and $\nu \in \mathbb{Z}$ such that $G(t) = F(\epsilon t + \nu)$. Observe that because F has odd degree, we have $\epsilon = 1$. We have then

$$x = \sum_{j=0}^{n} \gamma_j G(j) = \sum_{j=0}^{n} \gamma_j F(\nu + j) = \nu \tag{8}$$

and

$$x^2 = \nu^2 = \sum_{j=0}^{n} \alpha_j F(\nu + j) = \sum_{j=0}^{n} \alpha_j G(j) = y. \tag{9}$$

□

Theorem 1.4 for polynomials of odd degree follows with a standard argument: because for any x and y we have $(x + y)^2 - x^2 - y^2 = 2xy$, multiplication is easily seen to be positive-existentially definable over the language $\mathcal{L}$, using the fact that the squaring function is.

We conclude this subsection with a relevant remark. An important point in the argument of this subsection is the fact that $\epsilon = 1$ in the proof of Lemma 4.1, since the degree of F is odd. For even degree, the sign indeterminacy imposes an additional complication (although the idea for constructing a formula that defines multiplication is similar). The complication is addressed by a more careful use of difference operators from which we will deduce Corollary 4.6. This corollary will serve as a substitute for the identities (8) and (9) used in the proof of Lemma 4.1.

4.2. **Some lemmas using difference operators.** Let $\mathcal{P}_d$ be the $\mathbb{Q}$-vector space of polynomials of degree at most d (with $\mathcal{P}_d = \{0\}$ if $d < 0$). Given integers m and p, we define the *m-shifted p-difference operator* $\Delta_m^p \colon \mathbb{Q}[t] \to \mathbb{Q}[t]$ by

$$\Delta_m^p(H) = \sum_{j=0}^{p} (-1)^{p-j} \binom{p}{j} H(t + j - m).$$

In other words, this is applying the p-forward difference operator to a polynomial $H(t)$, and then evaluating the resulting polynomial at $t - m$ instead of t. Therefore, we have:

Lemma 4.2. *The operator Δ_m^p is $\mathbb{Q}$-linear and its kernel is $\mathcal{P}_{p-1}$. Moreover, if Q is a polynomial of degree $d \geq p$, then $\Delta_m^p(Q)$ is a polynomial of (exact) degree $d - p$.*

The proof of this lemma is an easy exercise in linear algebra. We also have:

Lemma 4.3. *Let $a, r \in \mathbb{Q}$, with $a \neq 0$, and let $k \geq 2$. Let $H = at^{2k} + rt^{2k-2} + h(t) \in \mathbb{Q}[t]$, where $h \in \mathbb{Q}[t]$ has degree at most $2k - 3$. There are rational numbers α_1, β_1, α_2, β_2, and γ_2, depending only on k, a and r (but not on h) such that the operators*

$$L_1 = \alpha_1 \Delta_k^{2k-1} + \beta_1 \Delta_k^{2k}$$

and

$$L_2 = \alpha_2 \Delta_k^{2k-2} + \beta_2 \Delta_k^{2k-1} + \gamma_2 \Delta_k^{2k}$$

satisfy $L_1(H) = t$ and $L_2(H) = t^2$. Moreover, we have $L_1(f) = 0$ for any f of degree $\leq 2k - 2$, and $L_2(f) = 0$ for any f of degree $\leq 2k - 3$.

Proof. The statements about f are immediate consequences of Lemma 4.2. Since $\Delta_k^{2k-1}(H)$ has degree one, there exist rational numbers α_1 and u such that $\alpha_1\Delta_k^{2k-1}(H) = t+u$. Also, since $\Delta_k^{2k}(H)$ has degree zero, there exists $\beta_1 \in \mathbb{Q}$ such that $\beta_1\Delta_k^{2k}(H) = -u$. Hence, $L_1(H) = t$.

Similarly, since $\Delta_k^{2k-2}(H)$ has degree 2, there are rational numbers α_2, u and v such that

$$\alpha_2\Delta_k^{2k-2}(H) = t^2 + ut + v.$$

Also, since $\Delta_k^{2k-1}(H)$ has degree 1, there exist $\beta_2, w \in \mathbb{Q}$ such that $\beta_2\Delta_k^{2k-1}(H) = -ut + w$. Finally, since $\Delta_k^{2k}(H)$ has degree 0, there exists γ_2 such that $\gamma_2\Delta_k^{2k}(H) = -v-w$. Hence, $L_2(H) = t^2$. □

For later reference, we state here the following linear algebra fact (which was already used in Subsection 4.2):

Lemma 4.4. *Let $P(t)$ be a polynomial over $\mathbb{Q}$ of degree d. The polynomials $P(t)$, $P(t+1)$,..., $P(t+d)$ are linearly independent over $\mathbb{Q}$.*

Lemma 4.5. *Let k and H be as in Lemma 4.3. There are rational numbers a_j and b_j, for $j = -k, \ldots, k$, such that*

(1) $t = \sum_{j=-k}^{k} a_j H(t+j)$,
(2) $a_{-j} = -a_j$ *for each* j,
(3) $t^2 = \sum_{j=-k}^{k} b_j H(t+j)$, *and*
(4) $b_{-j} = b_j$ *for each* j.

Proof. Let L_1 and L_2 be the operators coming from Lemma 4.3. Note that given a polynomial $P \in \mathbb{Q}[t]$ of degree $2k$, we have

$$L_1(P) = \sum_{j=0}^{2k} a'_j P(t+j-k) = \sum_{j=-k}^{k} a_j P(t+j)$$

for some coefficients a'_j and a_j in $\mathbb{Q}$ that depend only on L_1 (not on the particular P). Similarly, there are coefficients b_j in $\mathbb{Q}$ such that $L_2(P) = \sum_{j=-k}^{k} b_j P(t+j)$. Items (1) and (3) are therefore immediate.

We prove Item (2). We have

$$t = \sum_{j=-k}^{k} a_j H(t+j) = L_1(H) = L_1\left(a(t+j)^{2k}\right) = \sum_{j=-k}^{k} a_j a(t+j)^{2k}. \tag{10}$$

Therefore, we have

$$t = \sum_{j=-k}^{k} a_j a(t+j)^{2k} = \sum_{j=-k}^{k} a_j a(-t-j)^{2k} = \sum_{j=-k}^{k} a_{-j} a(-t+j)^{2k}. \tag{11}$$

From Equations (10) and (11) we obtain

$$-\sum_{j=-k}^{k} a_j a(t+j)^{2k} = -t = \sum_{j=-k}^{k} a_{-j} a(t+j)^{2k}.$$

We deduce from Lemma 4.4 that $a_{-j} = -a_j$ for each j.

We now prove Item (4). We have

$$\begin{aligned} t^2 &= \sum_{j=-k}^{k} b_j H(t+j) = L_2(H) \\ &= L_2\left(a(t+j)^{2k} + r(t+j)^{2k-2}\right) = \sum_{j=-k}^{k} b_j \left(a(t+j)^{2k} + r(t+j)^{2k-2}\right). \end{aligned} \tag{12}$$

Therefore, we have

$$\begin{aligned} t^2 &= \sum_{j=-k}^{k} b_j \left(a(t+j)^{2k} + r(t+j)^{2k-2}\right) \\ &= \sum_{j=-k}^{k} b_j \left(a(-t-j)^{2k} + r(-t-j)^{2k-2}\right) \qquad (13) \\ &= \sum_{j=-k}^{k} b_{-j} \left(a(-t+j)^{2k} + r(-t+j)^{2k-2}\right). \end{aligned}$$

From Equations (12) and (13) we obtain

$$\sum_{j=-k}^{k} b_j \left(a(t+j)^{2k} + r(t+j)^{2k-2}\right) = (-t)^2 = \sum_{j=-k}^{k} b_{-j} \left(a(t+j)^{2k} + r(t+j)^{2k-2}\right).$$

We deduce from Lemma 4.4 that $b_{-j} = b_j$ for each j. □

Corollary 4.6. *Let $F(t) = at^n + bt^{n-1} + \dots \in \mathbb{Q}[t]$ be a polynomial of even degree $n = 2k \geq 2$. There exist rational numbers a'_j and b'_j, $j = -k, \dots, k$, such that*

1. *$nat + b = \sum_{j=-k}^{k} a'_j F(t+j)$,*
2. *$a'_{-j} = -a'_j$ for each j,*
3. *$(nat+b)^2 = \sum_{j=-k}^{k} b'_j F(t+j)$, and*
4. *$b'_{-j} = b'_j$ for each j.*

Proof. Letting

$$H(t) = F\left(t - \frac{b}{na}\right),$$

we have $H(t) = at^n + rt^{n-2} + h(t) \in \mathbb{Q}[t]$, for some $r \in \mathbb{Q}$ and $h \in \mathbb{Q}[t]$ of degree $\leq n-3$. By Lemma 4.5, there exist rational numbers a_j and b_j, for $j = -k, \dots, k$, such that for each j, $a_{-j} = -a_j$ and $b_{-j} = b_j$, and such that

$$\sum_{j=-k}^{k} a_j H(t+j) = t \quad \text{and} \quad \sum_{j=-k}^{k} b_j H(t+j) = t^2,$$

By substituting in these equations t by $t + \frac{b}{na}$, we obtain

$$\sum_{j=-k}^{k} a_j F(t+j) = t + \frac{b}{na} \quad \text{and} \quad \sum_{j=-k}^{k} b_j F(t+j) = \left(t + \frac{b}{na}\right)^2,$$

hence, writing $a'_j = a_j na$ and $b'_j = b_j (na)^2$, we finally obtain

$$\sum_{j=-k}^{k} a'_j F(t+j) = nat + b \quad \text{and} \quad \sum_{j=-k}^{k} b'_j F(t+j) = (nat+b)^2$$

and clearly $a'_{-j} = -a'_j$ and $b'_{-j} = b'_j$ for each j. □

4.3. **Case of even degree.** In this subsection, we fix a $\mathbb{Z}$-valued polynomial

$$F(t) = at^n + bt^{n-1} + \dots$$

of even degree $n = 2k \geq 2$. We let a'_j and b'_j, $j = -k, \dots, k$, be the rational numbers associated to F by Corollary 4.6, and $N \geq n$ be the integer that comes from Theorem 1.6. Let A be a positive integer such that both Aa and Ab are integers (note that in particular Ana is an integer and that A depends only on F).

Let $\psi_0(x, y, z, u_{-N}, \dots, u_N)$ be the $\mathcal{L}$-formula

$$\bigwedge_{i=-N}^{N} Ru_i \wedge \Delta^{(n)}\left((u_i)_{-N}^{N}\right) = (a \cdot n!)_i \wedge x = \sum_{j=-k}^{k} Aa'_j u_j \wedge y = \sum_{j=-k}^{k} A^2 b'_j u_j \wedge x = Anaz + Ab.$$

Lemma 4.7. *The formula $\psi(x, y)$ given by*

$$\exists z, u_{-N}, \dots, u_N\, \psi_0(x, y, z, u_{-N}, \dots, u_N)$$

is satisfied in $\mathbb{Z}$ if and only if $y = x^2$ and $x = Anaz + Ab$ for some integer z.

Proof. If $y = x^2$ and $x = Anaz + Ab$ for some integer z, then $\psi(x, y)$ is satisfied in $\mathbb{Z}$ by choosing $u_i = F(i + z)$ for each i, by Corollary 4.6.

Suppose that the formula is satisfied in $\mathbb{Z}$. Let $z \in \mathbb{Z}$ be such that $x = Anaz + Ab$ (such a z exists thanks to the last part of the formula). Since $\mathbb{Z}$ satisfies $\bigwedge_{i=-N}^{N} Ru_i \wedge \Delta^{(n)}\left((u_i)_{-N}^{N}\right) = (a \cdot n!)_i$, there exists a polynomial G of degree n and leading coefficient a such that $G(i) = u_i \in \mathcal{R}(F)$ for each $i = 1, \dots, N$. By Theorem 1.6, there exists $\nu \in \mathbb{Z}$ such that $G(t) = F(\varepsilon t + \nu)$, with $\varepsilon = \pm 1$.

If $\varepsilon = 1$, then we have

$$x/A = \sum_{j=-k}^{k} a'_j G(j) = \sum_{j=-k}^{k} a'_j F(\nu + j) = na\nu + b$$

(so in particular $\nu = z$), and

$$x^2/A^2 = (naz + b)^2 = (na\nu + b)^2 = \sum_{j=-k}^{k} b'_j F(\nu + j) = \sum_{j=-k}^{k} b'_j G(j) = y/A^2.$$

If $\varepsilon = -1$, then we have

$$x/A = \sum_{j=-k}^{k} a'_j G(j) = \sum_{j=-k}^{k} a'_j F(\nu - j) = \sum_{j=-k}^{k} a'_{-j} F(\nu + j) = -\sum_{j=-k}^{k} a'_j F(\nu + j) = -(na\nu + b)$$

(so in particular $\nu = \frac{-b}{ka} - z$, where we recall that $k = n/2$) and

$$x^2/A^2 = (naz + b)^2 = \left(na\left(-\nu - \frac{b}{ka}\right) + b\right)^2 = (-na\nu - b)^2 = \sum_{j=-k}^{k} b'_j F(\nu + j)$$
$$= \sum_{j=-k}^{k} b'_{-j} F(\nu - j) = \sum_{j=-k}^{k} b'_j F(\nu - j) = \sum_{j=-k}^{k} b'_j G(j) = y/A^2.$$

In either case, we conclude $y = x^2$, with $x = Anaz + Ab$. □

Let $L = \{\ell_1, \dots, \ell_{Ana}\} \subseteq \mathbb{Z}$ be such that every integer x can be written as $m + \ell$, with m of the form $Anaz + Ab$, $z \in \mathbb{Z}$, and $\ell \in L$. This is possible because Ana and Ab are integers, with $Ana \neq 0$, so that the numbers of the form $Anaz + Ab$ with $z \in \mathbb{Z}$ form an arithmetic progression in $\mathbb{Z}$ (with difference Ana). Given $1 \leq j \leq Ana$, we let $\theta_j(x, y, v, w)$ be the $\mathcal{L}$-formula

$$x = v + \ell_j \wedge \psi(v, w) \wedge y = w + 2\ell_j v + \ell_j^2.$$

Note that it is indeed a formula over $\mathcal{L}$ since each ℓ_j depends only on n, A, a and b (or simply on F, which is fixed).

Lemma 4.8. *We have $y = x^2$ if and only if the formula $\varphi(x, y)$*

$$\exists v \exists w \bigvee_{j=1}^{Ana} \theta_j(x, y, v, w)$$

is satisfied in $\mathbb{Z}$.

Proof. Assume $y = x^2$. Let v and ℓ_i be such that $x = v + \ell_i$, with $v = Anaz + Ab$ for some integer z. Let $w = v^2$, so that $\psi(v, w)$ is satisfied. We have

$$y = x^2 = (v + \ell_i)^2 = v^2 + 2\ell_i v + \ell_i^2 = w + 2\ell_i v + \ell_i^2,$$

hence the formula $\theta_i(x, y, v, w)$ is satisfied.

Assume $\varphi(x, y)$ is satisfied. Let i, v and w be such that the formula $\theta_i(x, y, v, w)$ is satisfied. In particular, we have $w = v^2$, hence

$$y = w + 2\ell_i v + \ell_i^2 = (v + \ell_i)^2 = x^2.$$

□

5. Non-uniformity

In this last brief section, we prove Theorem 1.8. For the sake of contradiction, assume that there is a uniform positive existential definition of multiplication across the collection of structures $\mathfrak{Z}_F$, as F ranges over the polynomials of the form at^n with $a \in \mathbb{Z}_{>0}$. Under this assumption, one deduces from general principles that the following problem would be undecidable (see [27, Section 3, Property ($\star$)], or see [10, Corollary 2.2] for an exposition more directly applicable to our case):

Problem 5.1. *Given a system of equations of the form*

$$(S): \qquad a_{1j}x_1 + \cdots + a_{rj}x_r + b_{1j}y_1 + \cdots + b_{sj}y_s = c_j, \quad 1 \le j \le t$$

with $a_{ij}, b_{ij}, c_j \in \mathbb{Z}$, decide whether or not for each $a \in \mathbb{Z}_{>0}$ there is an integral solution with all x_i of the form ak^n, $k \in \mathbb{Z}$.

However, this problem turns out to be decidable. Here is the algorithm. Set all the a_{ij} to be 0 in (S) to obtain the system of linear equations

$$(S'): b_{1j}y_1 + \cdots + b_{sj}y_s = c_j, \quad 1 \le j \le t.$$

One can check the existence of integral solutions for (S'). Then we conclude by:

Lemma 5.2. *The system (S') has an integral solution if and only if for each $a \in \mathbb{Z}_{>0}$ there is an integral solution of (S) with all x_i of the form ak^n, $k \in \mathbb{Z}$.*

Proof. If (S') has integral solutions, then we get solutions for (S) of the desired form because $0 = a \cdot 0^n$. Conversely, if for every $a \in \mathbb{Z}_{>0}$ the system (S) has solutions as required, then reducing modulo a we see that the system (S') has solutions modulo a for every $a \in \mathbb{Z}_{>0}$. It is an elementary fact that for systems of linear equations the existence of solutions modulo a for every a implies the existence of solutions in $\mathbb{Z}$ (see Section 2.2, Chapter 1 [16]), and therefore we conclude that (S') has an integral solution. □

Since Problem 5.1 is decidable we get a contradiction. Hence, multiplication cannot be defined uniformly and Theorem 1.8 is proved.

6. Acknowledgments

We thank Mike Roth for his feedback on some of the proofs, and Erick Knight for the example in Remark 2.7. We are also grateful to Leonard Lipshitz and Thanases Pheidas for their comments on this work.

We heartily thank the anonymous referee for giving a careful reading to the manuscript and for a number of suggestions that improved the presentation.

Both authors have been partially supported by the second author's Fondecyt project 1130134 (Chile).

During this research, H. P. was supported by an Ontario Graduate Scholarship at Queen's University, a Benjamin Peirce Fellowship at Harvard, and by a Schmidt Fellowship and by the NSF at the Institute for Advanced Study. This material is based upon work supported by the National Science Foundation under agreement No. DMS-1128155. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

References

[1] D. Abramovich, *Uniformité des points rationnels des courbes algébriques sur les extensions quadratiques et cubiques.* (French) [Uniformity of rational points of algebraic curves over quadratic and cubic extensions] C. R. Acad. Sci. Paris Sér. I Math. 321 (1995), no. 6, 755–758.

[2] A. Bès, *A survey of arithmetical definability. A tribute to Maurice Boffa.* Bull. Belg. Math. Soc. Simon Stevin suppl. (2001) 1–54.

[3] Y. Bilu, R. Tichy. *The Diophantine equation f(x)=g(y).* Acta Arith 95.3 (2000): 261-288.

[4] J. R. Büchi, *Weak Second-Order Arithmetic and Finite Automata.* Mathematical Logic Quarterly 6 (1960), Issue 1-6, 66–92.

[5] L. Caporaso, J. Harris, B. Mazur, *Uniformity of rational points.* J. Amer. Math. Soc. 10 (1997), no. 1, 1–35.

[6] G. Cornelissen, K. Zahidi, *Topology of Diophantine sets: remarks on Mazur's conjectures.* In Hilbert's tenth problem: relations with arithmetic and algebraic geometry (Ghent, 1999), Amer. Math. Soc., Providence, RI, 2000, Contemp. Math. 270, 253–260.

[7] H. Davenport, D. J. Lewis, A. Schinzel, *Polynomials of certain special types.* Acta Arith. 9 (1964), 107–116.

[8] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. (German) [Finiteness theorems for abelian varieties over number fields].* Invent. Math. 73 (1983), no. 3, 349–366; Erratum, Invent. Math. 75 (1984), no. 2, 381.

[9] M. D. Fried and M. Jarden, *Field arithmetic. Second edition.* Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], **11**. Springer-Verlag, Berlin, 2005. xxiv+780 pp. ISBN: 3-540-22811-X

[10] N. Garcia-Fritz and H. Pasten, *Uniform positive existential interpretation of the integers in rings of entire functions of positive characteristic.* J. Number Theory **156** (2015), 368—393

[11] R. Hartshorne, *Algebraic Geometry.* Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977. xvi+496 pp. ISBN: 0-387-90244-9.

[12] E. Katz, J. Rabinoff and D. Zureick-Brown *Uniform bounds for the number of rational points on curves of small Mordell-Weil rank.* Preprint. arXiv:1504.00694 (2015).

[13] J. Koenigsmann *Defining $\mathbb{Z}$ in $\mathbb{Q}$.* Preprint. arXiv:1011.3424v2 (2013).

[14] S. Lang, *Algebra.* Revised third edition. Graduate Texts in Mathematics, 211. Springer-Verlag, New York, 2002. xvi+914 pp. ISBN: 0-387-95385-X.

[15] L. Lipshitz, *Quadratic forms, the five square problem, and diophantine equations*, The collected works of J. Richard Büchi (S. MacLane and Dirk Siefkes, eds.) Springer (1990), 677–680.

[16] Y. I. Manin, A. A. Panchishkin. *Number Theory I.* In Encyclopedia of Math. Sciences, 49, edited by A. N. Parshin and I. R. Shafarevich. Berlin: Springer-Verlag (1995).

[17] David Marker, *Zariski geometries.* Model theory and algebraic geometry, 107—128, Lecture Notes in Math. **1696**, Springer, Berlin, 1998.

[18] D. Marker, A. Pillay. *Reducts of* $(\mathbb{C}, +, \cdot)$ *which contain* $+$. The Journal of Symbolic Logic 55 (1990), No. 3.

[19] Y. Matiyasevich, *Enumerable sets are diophantine.* Dokladii Akademii Nauk SSSR, **191** (1970), 279-282; English translation. Soviet Mathematics Doklady 11 (1970), 354–358.

[20] B. Mazur, *The topology of rational points.* Experiment. Math. 1 (1992), no. 1, 35–45.

[21] B. Mazur, *Questions of decidability and undecidability in number theory.* J. Symbolic Logic 59 (1994), no. 2, 353–371.

[22] B. Mazur, *Speculations about the topology of rational points: an update.* In: Columbia University Number Theory Seminar (New York, 1992), Asterisque 228 (1995), 165–182.

[23] P. Pacelli, *Uniform boundedness for rational points.* Duke Math. J. 88 (1997), no. 1, 77–102.

[24] H. Pasten, *Powerful values of polynomials and a conjecture of Vojta.* J. Number Theory 133 (2013), no. 9, 2964–2998

[25] H. Pasten, *Arithmetic problems around the ABC conjecture and connections with logic.*, Ph. D. Thesis (2014). https://qspace.library.queensu.ca/bitstream/1974/12123/1/Pasten_Hector_H_201404_PhD.pdf

[26] H. Pasten, T. Pheidas and X. Vidaux, *A survey on Büchi's problem: new presentations and open problems*, Zapiski Nauchn. Sem. POMI 377 (2010), 111–140.

[27] H. Pasten, T. Pheidas and X. Vidaux, *Uniform existential interpretation of arithmetic in rings of functions of positive characteristic.* Inventiones Mathematicae 196 (2014), 453–484, DOI 10.1007/s00222-013-0472-1.

[28] T. Pheidas and X. Vidaux, *Extensions of Büchi's problem: Questions of decidability for addition and k-th powers.* Fundamenta Mathematicae 185 (2005), 171–194.

[29] B. Poonen, *Uniform boundedness of rational points and preperiodic points.* Preprint.

[30] B. Poonen and A. Shlapentokh, *Diophantine definability of infinite discrete nonarchimedean sets and Diophantine models over large subrings of number fields.* J. Reine Angew. Math. 588 (2005), 27–47.

[31] H. Putnam, *Decidability and Essential Undecidability.* The Journal of Symbolic Logic 22 (1957), no. 1, 39–54.

[32] E. D. Rabinovich, *Definability of a field in sufficiently rich incidence systems. With an introduction by Wilfrid Hodges.* QMW Maths Notes, **14**, Queen Mary and Westfield College, School of Mathematical Sciences, London, 1993. xvi+97 pp. ISBN: 0-902480-13-8.

[33] P. Ribenboim, *Polynomials whose values are powers.* Collection of articles dedicated to Helmut Hasse on his seventy-fifth birthday, II J. Reine Angew. Math., 268/269 (1974), 34–40.

[34] A. L. Semenov, *Logical theories of one-place functions on the set of natural numbers.* Izvestiya Akademii Nauk SSSR Seriya Mathematicheskaya, Vol. 47 (1983), 623–658; English translation, Mathematics of the USSR-Izvestiya, Vol. 22 (1984), 587–618.

[35] M. Stoll, *Uniform bounds for the number of rational points on hyperelliptic curves of small Mordell-Weil rank.* Preprint. arXiv:1307.1773v5 (2015).

[36] P. Vojta, *Diagonal quadratic forms and Hilbert's Tenth Problem.* Contemporary Mathematics 270 (2000), 261–274.

[37] A. R. Woods, *Some problems in logic and number theory, and their connections.* Ph.D. Thesis, University of Manchester, Manchester (1981).

[38] A. R. Woods, *Decidability and Undecidability of Theories with a Predicate for the Primes.* J. Symbolic Logic 58, No. 2 (1993), 672–687.

Department of Mathematics, Harvard University
1 Oxford Street
Cambridge, MA USA, 02138
Current address: School of Mathematics, Institute for Advanced Study
1 Einstein Drive
Princeton, NJ 08540, USA.
E-mail address: hpasten@math.harvard.edu

Departamento de Matemáticas, Universidad de Concepción
Avenida Esteban Iturra s/n - Barrio Universitario
Casilla 160 C - Concepción, Chile
E-mail address: xvidaux@udec.cl