DECIDABILITY OF EXTENSIONS OF PRESBURGER ARITHMETIC BY HARDY FIELD FUNCTIONS

HERA BROWN AND JAKUB KONIECZNY

ABSTRACT. We study the extension of Presburger arithmetic by the class of sub-polynomial Hardy field functions, and show the majority of these extensions to be undecidable. More precisely, we show that the theory $\mathrm{Th}(\mathbb{Z}; <, +, \lfloor f \rceil)$, where f is a Hardy field function and $\lfloor \cdot \rceil$ the nearest integer operator, is undecidable when f grows polynomially faster than x. Further, we show that when f grows sub-linearly quickly, but still as fast as some polynomial, the theory $\mathrm{Th}(\mathbb{Z}; <, +, \lfloor f \rceil)$ is undecidable.

1. INTRODUCTION

1.1. **Background.** Presburger arithmetic, the first-order theory $\mathrm{Th}(\mathbb{N}; +)$ of the natural numbers with addition, is known to be decidable [Pre29], whereas Peano arithmetic, the extension of Presburger arithmetic by multiplication $\mathrm{Th}(\mathbb{N}; +, \times)$, is known to be undecidable [Chu36]. The undecidability of Peano arithmetic provides a method that can be used to show that various other extensions of Presburger arithmetic are undecidable; if multiplication can be defined in such an extension, then that extension is undecidable. For instance, the extension of Presburger arithmetic with the squaring function $\mathrm{Th}(\mathbb{N}; +, x \mapsto x^2)$ is undecidable, since $a = bc$ holds *iff* $a = (b+c)^2 - b^2 - c^2$ (This observation appears to first have been made by Tarski [Tar53]).

This leads to the question of whether any extension of Presburger arithmetic by a polynomial-like function in general is undecidable. It is easy to see that, for integer-valued polynomials p of degree greater than 2, the extension of Presburger arithmetic by that polynomial $\mathrm{Th}(\mathbb{N}; +, p)$ is undecidable. This is because we can define multiplication in the extension in much the same way as we could with the squaring function. Bès [Bès01] surveys further decidable and undecidable extensions of Presburger arithmetic, some of which are shown to be undecidable by defining multiplication in Presburger arithmetic.

1.2. **New Results.** Hardy field functions (with polynomially bounded growth), discussed in detail in Section 2, are a far-reaching generalisation of polynomial sequences which is often studied in combinatorial number theory and ergodic theory, see e.g. [Bos81], [Bos94], [Fra09] and [Ric22]. They are particularly well-behaved from the point of view of analysis, which often allows one to adapt arguments originally applied to polynomials to this wider class of functions.

While we postpone proper definition of Hardy field functions, for now we point out that they contain all *logarithmico-exponential functions* — that is, the functions that can be built up from the basic arithmetical operations over the reals (addition,

1

multiplication, subtraction, division), exponentiation and the taking of logarithms. Thus, for instance

$$f(x) = x^2 + 3x + 2, \quad g(x) = \sqrt{x}\log x + \tfrac{1}{\sqrt[3]{x}}, \text{ and } \quad h(x) = 2^{x^{3/5}+\log x} - 2$$

are all Hardy field functions.

Since we are interested in extensions of the Presburger arithmetic — which concerns the integers — and since Hardy field functions generally take real values we need a way to construct integer-valued variants of Hardy field functions. For this, we recall that for $x \in \mathbb{R}$ the operator $\lfloor x \rceil$ denotes the best integer approximation of x, meaning that $\lfloor x \rceil - 1/2 \le x < \lfloor x \rceil + 1/2$. We will also occasionally use the floor and the ceiling functions, $\lfloor x \rfloor$ and $\lceil x \rceil$, respectively. For a function f we let $\lfloor f \rceil$ denote the function that rounds f to the nearest integer (i.e. $\lfloor f \rceil (x) = \lfloor f(x) \rceil = \lceil f(x) - (1/2) \rceil$). Another technical issue we need to deal with is that Hardy field functions are generally defined only on an interval $[x_0, \infty)$ rather than on all of $\mathbb{R}$. For the sake of simplicity, by convention, we extend any Hardy field function to $\mathbb{R}$ by assigning the value 0 outside of the domain of definition. We are ultimately interested in evaluating the functions under consideration on large integers, so this issue does not affect the reasoning.

We now consider a question raised in [Kon24]: Given a Hardy field function whose rate of growth is polynomial and faster than linear, is the first-order theory $\mathrm{Th}(\mathbb{Z}; <, +, \lfloor f \rceil)$ (Note that $\mathrm{Th}(\mathbb{Z}; <, +)$ is equivalent to $\mathrm{Th}(\mathbb{N}; +)$) decidable? In this paper we answer this question negatively. Formally, we prove the following theorem:

Theorem A. *Let $f : [x_0, \infty) \to \mathbb{R}$ be a Hardy field function such that*

$$(1) \qquad \lim_{x \to \infty} \frac{f(x)}{x} = \infty \quad \text{and} \quad \lim_{x \to \infty} \frac{f(x)}{x^d} = 0$$

for an integer $d \ge 2$. Then the first-order theory of $\mathrm{Th}(\mathbb{Z}; <, +, \lfloor f \rceil)$ is undecidable.

Similarly, we can also deal with Hardy field functions whose rate of growth is slower than linear but not too slow.

Theorem B. *Let $f : [x_0, \infty) \to \mathbb{R}$ be a Hardy field function such that*

$$(2) \qquad \lim_{x \to \infty} \frac{f(x)}{x^\varepsilon} = \infty \quad \text{and} \quad \lim_{x \to \infty} \frac{f(x)}{x} = 0$$

for some $\varepsilon > 0$. Then the first-order theory of $\mathrm{Th}(\mathbb{Z}; <, +, \lfloor f \rceil)$ is undecidable.

Broadly, then, the extension of Presburger arithmetic by most polynomial-like Hardy field functions yields an undecidable theory, as expected.

1.3. **Proof Outline.** We prove Theorem A in two parts; we first treat the *super-linear* case, where the Hardy field function f grows faster than a quadratic polynomial, and the *near-linear* case, where f grows faster than a linear polynomial but slower than a quadratic polynomial. Building on these results, we then prove Theorem B, or the *sub-linear* case, where f grows slower than a linear function, separately.

In the super-linear case, we define multiplication using the fact that, over specific and arbitrarily large intervals, f can be closely approximated by a Taylor polynomial. By differentiating such polynomials, we can define multiplication between arbitrarily large numbers, and so define multiplication generally.

In the near-linear case, we use the near-linear growth of f to define an interval where f looks like a linear function. We show that there are sufficiently many of these intervals to define multiplication over a restricted domain. By taking difference sets, we then extend this restricted domain to the whole of $\mathbb{Z} \times \mathbb{Z}$. This defines multiplication generally.

In the sub-linear case, we use the fact that the inverse of f can be approximated in our theory, as well as the fact that the inverse of f grows faster than x, to define a near-linear or super-linear rounded Hardy field function. We then apply Theorem A, and undecidability follows.

1.4. **Future directions.**

1.4.1. *Weakening of conditions.* In proving Theorem A, we use only a few properties that Hardy field functions have, namely that they are d-times differentiable and have well-behaved Taylor approximations. It would be interesting to see which broader classes of functions also satisfy these requirements, as well as seeing how these requirements may be weakened further (particularly with regards to the equidistribution results that are required in the proof of Theorem A).

1.4.2. *Extension to non-polynomial functions.* The proofs above also focus on the case where f grows only polynomially quickly, but it might be interesting to see what non-polynomial Hardy field functions provide undecidable extensions of Presburger arithmetic. It seems that functions that grow exponentially or faster, and their inverses, would provide decidable extensions of Presburger arithmetic by ideas similar to Semënov's [Sem80, Sem84]. But functions that grow between polynomially and exponentially fast seem more interesting.

In particular, it seems that using the function $f(x) = 2^{\sqrt{x}}$ we can define a function with polynomial growth. Taking $f^{-1}(f'(x)) - x$, we get a function that looks similar to $\sqrt{x} \log x$, and by the results of this paper rounding this function and extending Presburger arithmetic by it leads to an undecidable theory. This then raises the question of how far this idea can be generalised:

Question 1.1. Given a Hardy field function $f : [x_0, \infty) \to \mathbb{R}$ such that

$$(3) \qquad \lim_{x \to \infty} \frac{f(x)}{x^n} > \infty \quad \text{and} \quad \lim_{x \to \infty} \frac{f(x)}{m^x} = 0$$

for all integers n and $m > 1$, is the first-order theory of $\mathrm{Th}(\mathbb{Z}; <, +, \lfloor f \rfloor)$ decidable?

1.4.3. *Generalisation to other theories.* Given that the theory of Skolem arithmetic, namely $\mathrm{Th}(\mathbb{N}; \times)$, is decidable [Bès01], it would be interesting to see whether the similar theory of $\mathrm{Th}(\mathbb{N}; \times, \lfloor f \rfloor)$ is decidable as well. This relates to a question raised by Korec [Kor01] as to whether the theory $\mathrm{Th}(\mathbb{N}; \times, X)$ is decidable, where X is the image of some polynomial function. In particular, it would be interesting to see whether Hardy field functions can in general be used to define addition as well as multiplication, and so used to show undecidability of the above theory. This leads us to the following question:

Question 1.2. Let $f \colon \mathbb{R} \to \mathbb{R}$ be a Hardy field function such that

$$(4) \qquad \lim_{x \to \infty} \frac{f(x)}{x^d} = \infty \quad \text{and} \quad \lim_{x \to \infty} \frac{f(x)}{x^{d+1}} = 0$$

for an integer $d > 1$. Is the first-order theory of $\mathrm{Th}(\mathbb{Z}; \times, \lfloor f \rfloor)$ decidable?

A further question along these lines would be whether just the theory $\mathrm{Th}(\mathbb{N}; \lfloor f \rceil)$ is decidable as well.

1.5. **Notation.** We let $\mathbb{N}$ be the set of nonnegative integers $\{0, 1, 2, \dots\}$.

For $x \in \mathbb{R}$, we define the integer part $\lfloor x \rfloor$ of x to be $\max\{n \in \mathbb{Z} \mid n \leq x\}$. We then define the ceiling of x to be $\lceil x \rceil = \lfloor -x \rfloor$ and the nearest integer of x to be $\lfloor x \rceil = \lceil x - 1/2 \rceil$. When applying the nearest integer function to a function generally, we write $\lfloor f \rceil (x)$ for $\lfloor f(x) \rceil$. We also write the circle norm of x as $\|x\|_{\mathbb{R}/\mathbb{Z}} = \min\{|x - n| \mid n \in \mathbb{Z}\}$ to denote the distance of x to the nearest integer.

2. Hardy fields

We define Hardy fields as follows. Let B be a set of equivalence classes of continuous real-valued functions in one variable, where we say that two such functions f and g are equivalent when they eventually agree i.e. when there exists some x_0 such that, for all $x > x_0$, we have $f(x) = g(x)$. Such equivalence classes are also called *germs*. The set B naturally gives rise to a ring $(B, +, \times)$. We say that a Hardy field is a subfield of the ring $(B, +, \times)$ that is closed under differentiation. A Hardy field function is a function that belongs to a Hardy field, or more precisely whose germ at ∞ belongs to the union of all Hardy fields.

The union of all Hardy fields is large enough to include a variety of interesting functions. This includes, as mentioned in Section 1.2, the class of logarithmico-exponential functions built up from real polynomials, exponentiation, and the taking of logarithms. This gives us both a natural class of examples of Hardy field functions, as well as a natural class of functions to compare general Hardy field functions to.

Hardy field functions exhibit many properties that make them well suited to analytic arguments. As a first instance of this principle, because of the fact that every Hardy field function is asymptotically comparable to 0, we have the following standard fact.

Lemma 2.1. *Let $f \colon \mathbb{R} \to \mathbb{R}$ be a Hardy field function. Then f is either eventually positive, eventually negative, or eventually zero. Likewise, f is either eventually increasing, eventually decreasing, or eventually constant.*

As a consequence, it makes sense to compare rates of growth of different Hardy field functions. Given two eventually positive functions f and g belonging to the same Hardy field, we write:

- $f(x) \ll g(x)$ if $\lim_{x \to \infty} f(x)/g(x) < \infty$;
- $f(x) \prec g(x)$ if $\lim_{x \to \infty} f(x)/g(x) = 0$;
- $f(x) \sim g(x)$ if $\lim_{x \to \infty} f(x)/g(x) \in (0, \infty)$.

Note that $f(x) \ll g(x)$ holds if and only if either $f(x) \prec g(x)$ or $f(x) \sim g(x)$.

In particular, throughout we consider Hardy field functions $f \colon [x_0, \infty) \to \mathbb{R}$; by this we mean that f behaves as usual on the half-line $[x_0, \infty)$, and that $f(x) = 0$ for all $x < x_0$. We pick x_0 such that f is either strictly increasing or strictly decreasing over the interval $[x_0, \infty)$, which by Lemma 2.1 we are licenced to do. This does

not affect the correctness of our arguments when applied to Hardy field functions generally, but merely simplifies proofs.

Lemma 2.2. *Let $f, g \colon [x_0, \infty) \to \mathbb{R}$ be eventually positive functions belonging to the same Hardy field. Then either $f(x) \prec g(x)$ holds, $f(x) \sim g(x)$ holds, or $f(x) \succ g(x)$ holds. Further, exactly one of the above holds.*

One convenient feature of Hardy field functions is that their derivatives have a rate of growth that is easy to describe, as shown in the following result.

Lemma 2.3 ([Fra09, Lem. 2.1]). *Let $f \colon [x_0, \infty) \to \mathbb{R}$ be a Hardy field function that satisfies $t^{-d} \ll |f(t)| \ll t^d$ for some $d \in \mathbb{N}$. Then $|f'(t)| \ll |f(t)|/t$.*

Another convenient feature of Hardy field functions is that they can be accurately approximated by their Taylor expansions. Given a function $f \colon [x_0, \infty) \to \mathbb{R}$ that has sufficiently many derivatives, for $x \geq x_0$ and $y \geq 0$, we can always consider the length-ℓ Taylor expansion

$$f(x + y) = P_{x,\ell}(y) + R_{x,\ell}(y),$$

where $P_{x,\ell}$ is the Taylor polynomial

$$P_{x,\ell}(y) = f(x) + yf'(x) + \cdots + \frac{y^{\ell-1}}{(\ell-1)!} f^{(\ell-1)}(x),$$

and $R_{x,\ell}$ is the remainder term (which we can consider to be defined simply as $R_{x,\ell}(y) = f(x+y) - P_{x,\ell}(y)$). Since Hardy field functions do have sufficiently many derivatives, we can consider such Taylor expansions of Hardy field functions. We will use the following standard estimate (similar results can be found e.g. in [Fra09] or [KM24, Prop. 2.9]).

Proposition 2.4. *Let $f \colon [x_0, \infty) \to \mathbb{R}$ be a Hardy field function that satisfies $t^{d-1} \ll |f(t)| \prec t^d$ for some $d \in \mathbb{N}$. Then we have*

$$R_{x,d}(y) \ll y^d f(x)/x^{d+1}$$

for sufficiently large x and all $0 \leq y \leq x$. (The constant implicit in the asymptotic notation depends only on f).

Proof. Recall that for any $x \geq x_0$ and $y \geq 0$ there exists $z \in [0, y]$ such that

$$R_{x,d}(y) = \frac{y^d}{d!} f^{(d)}(x + z).$$

Iterating Lemma 2.3 d times, we see that $f^{(d)}(t) \ll f(t)/t^d \to 0$ as $t \to \infty$. Since $f^{(d)}$ is a Hardy field function and is eventually monotone, we have

$$|R_{x,d}(y)| \leq \frac{y^d}{d!} \left| f^{(d)}(x) \right| \ll y^d f(x)/x^d. \qquad \square$$

We will also need the following results on distribution of Hardy field sequences. (We point out that [Bos94] in fact provides if and only if statements, but we will only be interested in one direction).

Theorem 2.5 ([Bos94, Thm. 1.9]). *Let $f_1, f_2, \ldots, f_k$ be functions belonging to the same Hardy field.*

Suppose that for each $n_1, n_2, \ldots, n_k \in \mathbb{Z}$, not all zero, and for every polynomial $p(x) \in \mathbb{Q}[x]$, letting

$$g(x) = n_1 f_1(x) + n_2 f_2(x) + \cdots + n_k f_k(x) - p(x),$$

we have $\lim_{x \to \infty} |g(x)| = \infty$. *Then the sequence*

$$(f_1(n) \bmod 1, f_2(n) \bmod 1, \dots, f_k(n) \bmod 1)_{n=0}^{\infty}$$

is dense in $\mathbb{R}^k / \mathbb{Z}^k$.

Remark 2.6. Note that, on the stronger condition that $\lim_{x \to \infty} |g(x)| / \log x = \infty$, the sequence $(f_1(n) \bmod 1, f_2(n) \bmod 1, \dots, f_k(n) \bmod 1)_{n=0}^{\infty}$ is also uniformly distributed in $\mathbb{R}^k / \mathbb{Z}^k$ [Bos94, Thm. 1.8].

3. Proof of the super-linear case

In this section we will prove Theorem A in the case where when $f(x) \gg x^2$. Broadly speaking, we will prove that all such Hardy field functions have what will be called the P_d *property*, which expresses that a function looks like a polynomial over arbitrarily long intervals. From that, we will introduce the $P_d^{\mathbb{Z}}$ property, which expresses that f looks like an *integer-valued* polynomial over arbitrarily long intervals. We will then show that if f has the $P_d^{\mathbb{Z}}$ property, then the first-order theory $\mathrm{Th}(\mathbb{Z}; <, +, \lfloor f \rfloor)$ is undecidable. A key step of the argument is differentiating the polynomial given by the $P_d^{\mathbb{Z}}$ property.

To begin with, we conduct the proof under the additional assumption that $x^{d-1} \prec f(x) \prec x^d$ for some $d \geq 3$. In particular, we initially exclude the case where $f(x) \sim x^{d-1}$, which we cover in a separate Subsection 3.5. The proof in the latter case follows along broadly similar lines. However, failure of certain equidistribution results forces us to introduce some new ideas.

3.1. **The P_d property.** We first introduce the P_d *property*, which holds of a function when that function can be approximated arbitrarily closely, and over arbitrarily long intervals, by some polynomial of degree less than d. Formally, we will say that a function $f \colon [x_0, \infty) \to \mathbb{R}$ has property P_d for some $d \in \mathbb{N}$ if for each $M \in \mathbb{N}$ and $\varepsilon > 0$ there exists some $N \in \mathbb{N}$ and a degree-$(d-1)$ polynomial p such that for all $0 \leq m < M$ we have $|f(N+m) - p(m)| < \varepsilon$. A convenient feature of Hardy field functions with polynomial growth is that they enjoy the property P_d, as shown in the following lemma.

Lemma 3.1. *Let f be a Hardy field function such that $x^{d-1} \ll f(x) \prec x^d$ for some $d \in \mathbb{N}$. Then f has the P_d property.*

Proof. Pick any $M \in \mathbb{N}$ and $\varepsilon > 0$, and let N be a large integer, to be determined in the course of the argument. Recall that we can expand $f(N+m)$ as $P_{N,d}(m) + R_{N,d}(m)$, where $P_{N,d}(m)$ is the degree-$(d-1)$ Taylor polynomial and $R_{N,d}(m)$ is the corresponding remainder term. Assuming, as we may, that $N > M$, for $0 \leq m \leq M$ by Proposition 2.4 we have $|R_{N,d}(m)| \ll M^d f(N)/N^d$. Since $f(N)/N^d \to 0$ as $N \to \infty$, picking sufficiently large N we can ensure that $|R_{N,d}(m)| \leq \varepsilon$, as needed. $\square$

3.2. **The $P_d^{\mathbb{Z}}$ property.** Recall that we are ultimately interested not in a Hardy field function f but rather in its integer-valued rounding $\lfloor f \rfloor$. Like in the previous section, let us suppose for a moment that on some interval $[N, N+M)$ the Hardy field function f is closely approximated by a degree-$(d-1)$ polynomial p, in the sense that for all $0 \leq m < M$ we have $|f(N+m) - p(m)| < \varepsilon$ for some small constant $\varepsilon > 0$. In this situation, it is not necessarily the case that $\lfloor f \rfloor$ is closely approximated by $\lfloor p \rfloor$. Indeed, if for some $0 \leq m < M$ we have $f(N+m) >$

$k + (1/2) > p(m)$ with $k \in \mathbb{Z}$ then $\lfloor f(N+m) \rceil = k+1 \neq k = \lfloor p(m) \rceil$. As a first step, we would like to avoid this behaviour, which is most easily accomplished by requiring that $\|f(N+m)\|_{\mathbb{R}/\mathbb{Z}}$ and $\|p(m)\|_{\mathbb{R}/\mathbb{Z}}$ are both small. Secondly, we note that (in the regime where M is much larger than d) the only way for $\|p(m)\|_{\mathbb{R}/\mathbb{Z}}$ to be small for all $0 \leq m < M$ is if p is closely approximated by an integer-valued polynomial, i.e. a polynomial q such that $q(\mathbb{Z}) \subseteq \mathbb{Z}$ (since we only use this statement as a source of intuition, we leave it admittedly vague). This motivates us to introduce a property $P_d^{\mathbb{Z}}$, which is an analogue of the property P_d discussed earlier. We will say that a function $f \colon [x_0, \infty) \to \mathbb{R}$ has property $P_d^{\mathbb{Z}}$ for some $d \in \mathbb{N}$ if for each $M \in \mathbb{N}$ and $\varepsilon > 0$ there exists $N \in \mathbb{N}$ and a degree-$(d-1)$ *integer-valued* polynomial p such that for all $0 \leq m < M$ we have $|f(N+m) - p(m)| < \varepsilon$. Above, we require that the polynomial p should have degree *exactly* $d-1$, as opposed to *at most* $d-1$; this requirement will play an important role in later considerations.

Lemma 3.2. *Let f be a Hardy field function such that $x^{d-1} \prec f(x) \prec x^d$ for some $d \in \mathbb{N}$. Then f has the $P_d^{\mathbb{Z}}$ property.*

Proof. Pick any $M \in \mathbb{N}$ and $\varepsilon > 0$. Recall from the proof of Lemma 3.1 that for sufficiently large N we can accurately approximate f on $[N, N+M)$ using the Taylor expansion $P_{N,d}$, meaning that $|f(N+m) - P_{N,d}(m)| < \varepsilon/2$ for all $0 \leq m < M$. Recall also that the coefficients of $P_{N,d}$ are given by

$$P_{N,d}(m) = \sum_{k=0}^{d-1} \frac{f^{(k)}(N)}{k!} m^k.$$

Consider the polynomial p obtained from $P_{N,d}$ by applying rounding to each coefficient:

$$p(m) = \sum_{k=0}^{d-1} \left\lfloor \frac{f^{(k)}(N)}{k!} \right\rceil m^k.$$

Since p has integer coefficients, it is clearly integer-valued. Our plan is to show that, for a judicious choice of N, the circle norms of coefficients of $P_{N,d}$ are small and consequently f is closely approximated by p.

We will apply Theorem 2.5 to the functions $f, f', \ldots, f^{(d-1)}/(d-1)$. For each $0 \leq k \leq d$ we have $f^{(k)}(x) \sim f(x)/x^k$. As a consequence, for any non-trivial linear combination $h(x) = c_0 f(x) + c_1 f'(x) + \cdots + c_{d-1} f^{(d-1)}(x)/(d-1)!$ with $c_0, c_1, \ldots, c_{d-1} \in \mathbb{Z}$ we have $h(x) \sim f(x)/x^k$, where ℓ is the first index with $c_\ell \neq 0$. Thus, for any polynomial p with degree e we have $|h(x) - p(x)| \sim f(x)/x^\ell$ if $d - \ell > e$ or $|h(x) - p(x)| \sim x^e$ otherwise (that is, if $d - \ell \leq e$). In either case, we have $|h(x) - p(x)| \succ 1$, as needed. We conclude that the sequence $\left(f(N), f'(N), \ldots, f^{(d-1)}(N)/(d-1)! \right)_{N=0}^{\infty}$ is dense modulo 1, and in particular it includes points with arbitrarily small circle norms. Hence, we can find N such that for all $0 \leq k < d$ we have:

$$\left\| \frac{f^{(k)}(N)}{k!} \right\|_{\mathbb{R}/\mathbb{Z}} \leq \frac{\varepsilon}{2dM^k}.$$

Therefore, we have the estimate

$$|P_{N,d}(m) - p(m)| \leq \sum_{k=0}^{d-1} \left\| \frac{f^{(k)}(N)}{k!} \right\|_{\mathbb{R}/\mathbb{Z}} M^k \leq \varepsilon/2.$$

Combining this with the previously mentioned estimate on $|f(N+m) - P_{N,d}(m)|$ we conclude that $|f(N+m) - p(m)| < \varepsilon$, as needed. Finally, increasing N if necessary, we may assume that the leading coefficient of p, i.e. $\lfloor f^{(d-1)}(N)/(d-1)! \rfloor$, is non-zero. $\qquad\square$

3.3. **Discrete derivatives.** Using Lemma 3.2, for a Hardy field function f satisfying the assumptions of Theorem A, we can find arbitrarily long intervals $[N, N+M)$ where $\lfloor f \rceil$ agrees some integer-valued polynomial p. The goal of the next two subsections is to prove the following lemma, asserting that this property implies that the theory $\mathrm{Th}(\mathbb{Z}; <, +, \lfloor f \rceil)$ is undecidable.

Lemma 3.3. *Let* $f \colon [x_0, \infty) \to \mathbb{R}$ *be a function that satisfies the* $P_d^{\mathbb{Z}}$ *property for some* $d \geq 3$. *Then the theory* $\mathrm{Th}(\mathbb{Z}; <, +, \lfloor f \rceil)$ *is undecidable.*

A key ingredient of the proof of Lemma 3.3 is the notion of differentiation for sequences indexed by integers, which will ultimately help us define multiplication. To this end, we introduce the *discrete derivative* and the *symmetric discrete derivative* of a function:

Definition 3.4. Given a function $f \colon \mathbb{Z} \to \mathbb{R}$ and an integer m, the *discrete derivative* $\Delta_m f \colon \mathbb{Z} \to \mathbb{R}$ is given by

$$\Delta_m f(n) = f(n+m) - f(n)$$

and the *symmetric discrete derivative* $\boldsymbol{\Delta}_m f \colon \mathbb{Z} \to \mathbb{R}$ is given by

$$\boldsymbol{\Delta}_m f(n) = \Delta_m \Delta_n f(0) = f(n+m) - f(n) - f(m) + f(0).$$

Of course, the discrete derivative of an integer-valued function is again integer-valued. We also point out that the discrete derivative operators commute: $\Delta_m \Delta_n = \Delta_n \Delta_m$. The symmetric derivative, as the name suggests, is a symmetric function of the arguments: $\boldsymbol{\Delta}_m f(n) = \boldsymbol{\Delta}_n f(m)$. For reasons of symmetry, given an integer $r \geq 1$ and integers $n_0, n_1, \ldots, n_r$ we write

$$\boldsymbol{\Delta}^r f(n_0, n_1, \ldots, n_r) \quad \text{for} \quad \boldsymbol{\Delta}_{n_r} \boldsymbol{\Delta}_{n_{r-1}} \ldots \boldsymbol{\Delta}_{n_1} f(n_0).$$

A particularly useful feature of the discrete derivative (symmetric or otherwise) is that its application to a polynomial yields a polynomial of degree one less. As a consequence, its repeated application only leaves the leading term of the function to be considered. We make this observation concrete in the following result.

Lemma 3.5. *Let* m *be an integer and let* p *be a polynomial of degree* r *with leading coefficient* a_r.

(i) If $r \geq 1$ *then* $\Delta_m p$ *is a polynomial with degree* $r-1$ *and leading coefficient* $r a_r m$. *If* $r = 0$ *then* $\Delta_m p = 0$.

(ii) If $r \geq 2$ *then* $\boldsymbol{\Delta}_m p$ *is a polynomial with degree* $r-1$ *and leading coefficient* $r a_r m$. *If* $r = 0$ *or* $r = 1$ *then* $\boldsymbol{\Delta}_m p = 0$.

Proof. It is straightforward to verify by an explicit computation that item (i) holds for $r = 0$ and item (ii) holds for $r = 0, 1$. For $r \geq 2$, $\Delta_m p$ and $\boldsymbol{\Delta}_m p$ differ only by a constant (equal to $p(m) - p(0)$) so it suffices to prove item (i).

We proceed by induction on r, the case $r = 0$ already having been considered. Thus, we may assume that $r \geq 1$ and the claim has already been proved for all $r' < r$.

We may write $p(x) = a_r x^r + \tilde{p}(x)$ where $\deg \tilde{p} < r$. By the inductive assumption, $\Delta_m \tilde{p}$ is a polynomial of degree strictly less than $r - 1$ (or identically zero if $r = 1$), so it suffices to deal with the leading term. We can explicitly compute that

$$a_r(x + m)^r - a_r x^r = \sum_{k=1}^{r} \binom{r}{k} a_r m^k x^{r-k},$$

where the right side is a degree-$(r - 1)$ polynomial with leading coefficient $r a_r m$, as needed.

$\square$

For brevity, we write $\boldsymbol{\Delta}^r f(a, b)$ for $\boldsymbol{\Delta}^r f(a, b, 1, 1, \dots, 1)$ whenever $r \geq 1$. As an application of Lemma 3.5 we almost immediately get the following formula.

Lemma 3.6. *Let p be a polynomial with degree r and leading coefficient a_r. Then $\boldsymbol{\Delta}^{r-1} p(n, m) = r! a_r n m$.*

Proof. Iterating Lemma 3.5 we see that $\boldsymbol{\Delta}^{r-1} p(n, m)$ is a polynomial function of n with degree 1 and leading coefficient $r! a_r m$. To see that all the remaining coefficients are zero, it is enough to recall that $\boldsymbol{\Delta}^{r-1} p(n, m)$ is a symmetric function of n and m, and that $\boldsymbol{\Delta}^{r-1} p(0, 0) = 0$. $\square$

In the direction opposite to Lemma 3.5, we have the following characterisation of polynomials in terms of discrete derivatives. It is a standard observation for instance following from discussion in [GKP90, Section 2.6]; we include proof for completeness.

Lemma 3.7. *Let $r \geq 0$ and let $f \colon [N, N + M) \to \mathbb{R}$ be a sequence such that $\Delta_1^{r+1} f(n) = 0$ for $N \leq n < N + M - r - 1$. Then f coincides with a polynomial of degree at most r.*

Proof. For any polynomial p of degree at most r we have $\Delta^{r+1} p = 0$, so we may freely replace f with $f - p$. Applying Lagrange interpolation, we may thus assume that $f(N) = f(N + 1) = \cdots = f(N + r) = 0$. Since $\Delta_1^{r+1} f(n) = 0$ for all n where it is defined, we see that if we have $f(n) = f(n + 1) = \cdots = f(n + r) = 0$ for some $N \leq n < N + M - r - 1$ then also $f(n + r + 1) = 0$. Reasoning by induction with respect to n we thus conclude that $f(m) = 0$ for all $N \leq m < N + M$. In particular, f is a polynomial of degree at most r $\square$

3.4. **Emulating multiplication.** Using the results obtained in Section 3.3, we next show how to use property $P_d^{\mathbb{Z}}$ to emulate multiplication. Recall that $P_d^{\mathbb{Z}}$ implies that we can find arbitrarily long intervals $[N, N + M)$ where $\lfloor f \rfloor$ agrees with an integer-valued polynomial p (in the sense that $\lfloor f \rfloor (N + m) = p(m)$). What is more, we can use Lemma 3.7 to detect intervals with the property mentioned above. Given such an interval, for $1 \leq a, b, c \leq M$ we can use Lemma 3.6 to express the property that $ab = c$ as $\boldsymbol{\Delta}^{d-2} p(a, b) = \boldsymbol{\Delta}^{d-2} p(c, 1)$. We now put this plan into practice.

Lemma 3.8. *Let $d \geq 2$ and let $\pi_d(N, M)$ be the sentence given by*

$$\exists c \neq 0 \ \forall 0 \leq m < M - d \ \Delta_1^{d-1} \lfloor f \rfloor (N + m) = c.$$

Then $\pi_d(N, M)$ holds if and only if there exists a polynomial p with degree exactly $d - 1$ such that $\lfloor f \rfloor (N + m) = p(m)$ for all $0 \leq m < M$.

Proof. Suppose that $\pi(N, M)$ holds. Applying Δ_1 once more, we conclude from Lemma 3.7 that $\lfloor f \rceil$ agrees with a polynomial p of degree at most $d-1$ on $[N, N+m)$. If p had degree strictly less than $d-1$ then, by repeated application of Lemma 3.5, we would have $\Delta_1^{d-1} \lfloor f \rceil (N + m) = 0 \neq c$, contradicting $\pi_d(N, M)$. Thus, p has degree exactly $d - 1$, as needed.

Suppose now that there exists a polynomial p with degree exactly $d - 1$ such that $\lfloor f \rceil (N + m) = p(m)$ for all $0 \leq m < M$. Then, by repeated application of Lemma 3.5, we have $\Delta_1^{d-1} \lfloor f \rceil (N + m) = (d - 1)! a_{d-1}$, where a_{d-1} is the leading coefficient of p. Thus, setting $c = (d - 1)! a_{d-1}$ we see that $\pi_d(N, M)$ holds. $\square$

Lemma 3.9. *Let $d \geq 3$ and let $\mu_d(n, m, q)$ be the sentence given by*

$$\exists M > \max(n, m, q) \ \exists N \ \pi_d(N, M) \wedge \Delta_1^{d-3} \Delta_n \Delta_m \lfloor f \rceil (N) = \Delta_1^{d-2} \Delta_q \lfloor f \rceil (N).$$

Assume that f enjoys property $P_d^{\mathbb{Z}}$ and $n, m, q \geq 1$. Then, for $n, m, q \in \mathbb{N}$ we have that $\mu_d(n, m, q)$ holds if and only if $q = nm$.

Proof. Suppose that $\mu(n, m, q)$ holds. Pick admissible M and N. Since, in particular, $\pi_d(N, M)$ holds, we know from Lemma 3.8 that there exists a polynomial p of degree $d - 1$ such that $\lfloor f \rceil (N + m) = p(m)$ for $0 \leq m < M$. The equality between the discrete derivatives in the definition of $\mu(n, m, q)$ can now more simply be expressed as $\boldsymbol{\Delta}^{d-2} p(n, m) = \boldsymbol{\Delta}^{d-2} p(q, 1)$. By Lemma 3.6, this implies that $nm = q$, as needed.

Next, suppose that $q = nm$. Pick $M = q + 1$. By $P_d^{\mathbb{Z}}$, we can find N and a polynomial p of degree exactly $d - 1$ such that $f(N + m) = p(m)$ for $0 \leq m < M$. By Lemma 3.8, $\pi_d(M, N)$ holds. By Lemma 3.5, we have $\boldsymbol{\Delta}^{d-2} p(n, m) = (d - 1)! a_{d-1} nm = (d - 1)! a_{d-1} q = \boldsymbol{\Delta}^{d-2} p(q, 1)$. Hence $\mu(n, m, q)$ holds, as needed. $\square$

Proof of Lemma 3.3. It follows from Lemma 3.9 that multiplication on $\mathbb{N}$ is definable in $\mathrm{Th}(\mathbb{Z}; <, +, \lfloor f \rceil)$, and extending it to $\mathbb{Z}$ is immediate. Since $\mathrm{Th}(\mathbb{Z}; <, +, \times)$ is undecidable, so is $\mathrm{Th}(\mathbb{Z}; <, +, \lfloor f \rceil)$. $\square$

Combining Lemmas 3.2 and 3.3, we conclude that for each $d \geq 3$ and each Hardy field function f with $x^{d-1} \prec f(x) \prec x^d$, the theory $\mathrm{Th}(\mathbb{Z}; <, +, \lfloor f \rceil)$ is undecidable. This completes the proof of the first case of Theorem A.

3.5. **Generalisation to exactly polynomial growth.** Finally, we show how the argument in the earlier sections to sequences with exactly polynomial growth. Recall that previously we considered Hardy a field function f with $x^{d-1} \prec f(x) \prec x^d$ for some $d \geq 3$. Presently, we will instead assume that $f(x) \sim x^{d-1}$ (note that we make this choice instead of the more natural $f(x) \sim x^d$ for the sake of consistency with earlier considerations).

Significant part of the previously presented argument goes through without any change. Indeed, it remains the case that f enjoys the P_d property and can be accurately approximated by the Taylor polynomial $P_{N,d}$. Unfortunately, we are not able to establish the $P_d^{\mathbb{Z}}$ property. When we try to repeat the previous argument, the d-tuple formed by the coefficients of $P_{N,d}$, namely

$$(f(N), f'(N), f''(N)/2, \ldots, f^{(d-1)}(N)/(d - 1)!),$$

is not equidistributed modulo 1. Indeed, the top coefficient $f^{(d-1)}(N)/(d - 1)!$ can easily be shown to converge to a constant, and the behaviour of the remaining coefficients is potentially more complicated.

Because of the aforementioned limitation, we adapt the remainder of the argument to use property P_d instead of $P_d^{\mathbb{Z}}$. This introduces some complications since we are forced to apply discrete derivatives to functions of the form $\lfloor p \rceil$, where p is a polynomial, rather than to polynomials. Fortunately, the following lemma allows us to control errors arising from the rounding operation; we will apply it to $h(n) = p(n) - \lfloor p(n) \rceil$.

Lemma 3.10. *Let $h \colon \mathbb{Z} \to \mathbb{R}$ be a sequence with $|h(n)| \leq \varepsilon$ for all $n \in \mathbb{Z}$. Then*

$$|\Delta_{m_1} \Delta_{m_2} \ldots \Delta_{m_r} h(n)| \leq 2^r \varepsilon$$

for all integers $r \geq 1$ and all $n, m_1, m_2, \ldots, m_r \in \mathbb{Z}$.

Proof. For $r = 1$, the result follows from a straightforward computation. For $r > 1$, we use a standard inductive argument. $\square$

Using Lemma 3.10, we define a coarser variant of multiplication, which we then bootstrap to a definition of multiplication. This finishes the proof of the relevant case of Theorem A. We now put the strategy discussed above into practice. Formally, we establish the following result.

Proposition 3.11. *Let $f \colon [x_0, \infty) \to \mathbb{R}$ be a Hardy field function where $f(x) \sim x^{d-1}$ for some $d \geq 3$. Then the theory $\mathrm{Th}(\mathbb{Z}; <, +, \lfloor f \rceil)$ is undecidable.*

Proof. Fix an integer M and let N be sufficiently large such that the Hardy field function f is closely approximated by the degree-$(d-1)$ polynomial $P_{N,d}$, in the sense that we have $|f(N+m) - P_{N,d}(m)| < 1/10$ for all $0 \leq m < M$. Recall that the leading coefficient of $P_{N,d}$ is $f^{(d-1)}(N)/(d-1)!$, which converges to some non-zero constant α as $N \to \infty$. Let p be the polynomial obtained from $P_{N,d}$ by replacing the leading coefficient with α. Picking larger N if necessary, we may freely assume that $|f(N+m) - p(m)| < 1/10$ for all $0 \leq m < M$.

Note that, since p is a polynomial of degree $d-1$, we can apply Lemma 3.6 to it and get that $\Delta^{d-2} p(n, m) = (d-1)! \alpha n m$. Bearing in mind that we aim to adapt Lemma 3.9, we use Lemma 3.10 to approximate

$$\left| \Delta_1^{d-3} \Delta_n \Delta_m \lfloor f \rceil (N) - (d-1)! \alpha n m \right| \leq 2^{d-1},$$

provided that $0 \leq n, m < M$. This motivates us to consider, for $0 \leq a, b, c < M$, the quantity $F_N(a, b, c)$ defined as follows:

$$F_N(a, b, c) = \Delta_1^{d-3} \Delta_a \Delta_b \lfloor f \rceil (N) - \Delta_1^{d-2} \Delta_c \lfloor f \rceil (N).$$

The estimate obtained above implies that we have

$$|F_N(a, b, c) - (d-1!) \alpha (ab - c)| \leq 2^d.$$

Fix an integer $D \geq 100 \cdot 2^d / \min(1, (d-1)! \alpha)$. The estimate above allows us to prove the following lemma:

Lemma 3.12. *Let $0 \leq a, b, c < M$. Then $|F_N(Da, b, Dc)| \leq 2^d$ if and only if $ab = c$.*

Proof. For the rightwards direction of proof, first suppose that $ab \neq c$. Since $ab - c$ is a non-zero integer, it follows that $|Dab - Dc| \geq D$. Hence $|F_N(Da, b, Dc)| \geq (d-1)! \alpha D - 2^d > 2^d$, as needed.

For the leftwards direction of proof, suppose that $ab = c$. Then $Dab - Dc = 0$ as well. It follows that $|F_N(Da, b, Dc)| \leq 2^d$ as required. $\square$

Note that $|F_N(Da, b, Dc)|$ is definable in $\mathrm{Th}(\mathbb{Z}; <, +, \lfloor f \rceil)$. Thus, Lemma 3.12 allows us to define multiplication in $\mathrm{Th}(\mathbb{Z}; <, +, \lfloor f \rceil)$. More formally, let $\mu'(n, m, q)$ denote the formula

$$\forall N_0 \; \exists N \geq N_0 \;\; |F_N(Da, b, Dc)| \leq 2^d.$$

It follows from the preceding discussion (in particular Lemma 3.12) that $\mu'(n, m, q)$ holds if and only if $ab = c$. Recalling that $\mathrm{Th}(\mathbb{Z}; <, +, \times)$ is undecidable and that multiplication is definable in $\mathrm{Th}(\mathbb{Z}; <, +, \lfloor f \rceil)$, we conclude that $\mathrm{Th}(\mathbb{Z}; <, +, \lfloor f \rceil)$ is undecidable. □

Remark 3.13. One could use the techniques used here in order to establish Theorem A also in the case where $x^{d-1} \prec f(x) \prec x^d$. We take the route discussed earlier because we consider it to be more elegant, and because it has the added advantage of allowing us to identify the property $P_d^{\mathbb{Z}}$.

Remark 3.14. We note that previously, we were able to establish undecidability of $\mathrm{Th}(\mathbb{Z}; <, +, \lfloor f \rceil)$ as the consequence purely of the property $P_d^{\mathbb{Z}}$. This is in contrast with the argument discussed presently, which uses a property strictly stronger than P_d, namely that f is closely approximable by a polynomial on the interval $[N, N + M)$ for *all* N that are sufficiently large (as a function of M). It would be interesting to determine if the property P_d by itself is sufficient to establish undecidability. The key difficulty to this approach is finding a suitable analogue of Lemma 3.8.

4. Proof of the near-linear case

In this section, we prove the second case of Theorem A where f grows superlinearly but sub-quadratically i.e. when $x \prec f(x)$ and $f(x) \prec x^2$. To this end, we first define multiplication over a limited domain, using the fact that over certain intervals f can be closely approximated by a linear function. We then use difference sets to extend this definition of multiplication to the whole of $\mathbb{Z} \times \mathbb{Z}$ and thus show $\mathrm{Th}(\mathbb{Z}; <, +, \lfloor f \rceil)$ undecidable.

4.1. **Multiplicative intervals.** We first define a property $\lambda(N, M, n)$ which, informally, states that over the interval $[N, N+M)$ the function $\lfloor f \rceil$ defines an arithmetic progression with step n. Formally, we define λ by

$$\lambda(N, M, n) \overset{\text{def}}{=} (\forall \; 0 \leq m < M) \;\; \lfloor f \rceil (N + m + 1) = \lfloor f \rceil (N + m) + n.$$

It is routine to show that $\lambda(N, M, n)$ holds if and only if for all $0 \leq m < M$ we have $\lfloor f \rceil (N + m) - \lfloor f \rceil (N) = mn$. Our next step is to establish sufficient conditions for $\lambda(N, M, n)$ to hold.

Lemma 4.1. *Let $f \colon [x_0, \infty) \to \mathbb{R}$ be a Hardy field function with $x \prec f(x) \prec x^2$. Then there exists $x_1 \geq x_0$ such that $\lambda(N, M, n)$ holds for all $N, M, n \in \mathbb{N}$ satisfying the following conditions: (1) $N \geq x_1$; (2) $\|f(N)\|_{\mathbb{R}/\mathbb{Z}} < 1/4$; (3) $|f'(N) - n| < 1/(8M)$; (4) $f''(N) < 1/(8M^2)$.*

Proof. Informally speaking, we first approximate $f(N+m)$ by $f(N) + f'(N)m$, then approximate $f'(N)$ by n, and finally apply rounding to conclude that $\lfloor f \rceil (N+m) = \lfloor f \rceil (N) + mn$.

Formally, our first goal is to show that

$$(5) \qquad\qquad |f(N + m) - f(N) - f'(N)m| < \frac{1}{16}.$$

Towards this end, we consider the Taylor expansion of f at N. We have

$$f(N+m) = f(N) + f'(N)m + \frac{1}{2}f''(N+t)m^2$$

for some $t \in [0, m]$. Thus, the expression on the right side of (5) is

$$|f(N+m) - f(N) - f'(N)m| = \left|\frac{1}{2}f''(N+t)m^2\right| \le \frac{M^2}{2}|f''(N+t)|.$$

Since $f(x) \prec x^2$, we know that $f''(x) \prec 1$, meaning that $f''(x) \to 0$ as $x \to \infty$. As a consequence, f'' is eventually decreasing, and picking x_1 sufficiently large we may assume that f'' is decreasing on $[N, \infty)$. Thus, condition (1) allows us to simplify our estimate to

$$|f(N+m) - f(N) - f'(N)m| \le \frac{M^2}{2}|f''(N)| \le \frac{1}{16},$$

where the last inequality follows from condition (4). This completes the proof of (5).

In order to approximate $f'(N)$ by n we simply use condition (3), which immediately yields

$$|f'(N)m - nm| < \frac{1}{8}.$$

Combining this with (5), we get

(6) $$|f(N+m) - f(N) - nm| < \frac{1}{16} + \frac{1}{8} < \frac{1}{4}.$$

It remains to deal with rounding. We have

$$a(N+m) - a(N) - nm = \lfloor f(N+m)\rceil - \lfloor f(N)\rceil - nm \lfloor f(N+m) - \lfloor f(N)\rceil - nm\rceil.$$

Bearing in mind that $\lfloor x \rceil = 0$ for all x with $|x| < 1/2$, in order to show that $\lfloor f \rceil(N+m) = \lfloor f \rceil(N) + nm$, it suffices to estimate that

$$|f(N+m) - \lfloor f(N)\rceil - nm| \le \frac{1}{4} + |f(N) + nm - \lfloor f(N)\rceil - nm|$$

$$= \frac{1}{4} + \|f(N)\|_{\mathbb{R}/\mathbb{Z}} < \frac{1}{2}$$

Note that the first inequality follows from (6), and the last one from condition (2). □

In the following lemma, we show how the conditions of Lemma 4.1 hold sufficiently often.

Lemma 4.2. *Let $f\colon [x_0, \infty) \to \mathbb{R}$ be a Hardy field function with $x \prec f(x) \prec x^2$. Then for any real $x_1 \ge x_0$ and $\varepsilon_0, \varepsilon_1, \varepsilon_2 > 0$ there exists integer n_0 such that for each $n \ge n_0$ there exists integer N satisfying the following conditions: (1) $N \ge x_1$; (2) $\|f(N)\|_{\mathbb{R}/\mathbb{Z}} < \varepsilon_0$; (3) $|f'(N) - n| < \varepsilon_1$; (4) $f''(N) < \varepsilon_2$.*

Proof. Decreasing $\varepsilon_0, \varepsilon_1, \varepsilon_2$ if necessary (in this order), we may freely assume that $\varepsilon_0, \varepsilon_1, \varepsilon_2 < 1/10$ and we have the inequalities:

$$\varepsilon_1 < \frac{10}{3}\varepsilon_0, \qquad\qquad \frac{\varepsilon_1}{\varepsilon_2} > \frac{25}{\varepsilon_1} + 5 > 50.$$

(The motivation behind these inequalities will become apparent in the course of the argument). Picking a sufficiently large value of n_0 we may freely assume that

there exists $X_0 \geq x_1$ such that $f'(X_0) = n$, $f''(X_0) < \varepsilon_2$, and f, f', f'' are strictly monotone on $[X_0, \infty)$. Let X_1, X_2, X_3 be specified by

$$f'(X_1) = n + \frac{1}{5}\varepsilon_1, \qquad f'(X_2) = n + \frac{2}{5}\varepsilon_1, \qquad f'(X_3) = n + \frac{3}{5}\varepsilon_1.$$

Let also $N_1 = \lceil X_1 \rceil < X_1 + 1$ and $N_3 = \lfloor X_3 \rfloor > X_3 - 1$. Note that $f'(X_1) - f'(X_0) = \varepsilon_1/5$ and $f''(x) \leq f''(X_0) \leq \varepsilon_2$ for $x \in [X_0, X_1]$, so the mean value theorem implies that

$$X_1 - X_0 \geq \frac{\varepsilon_1}{5\varepsilon_2} \geq 10.$$

By the same token, we have $X_2 - X_1, X_3 - X_2 \geq 10$, which in particular implies that $N_3 - N_1 \geq 10$ (which is not strictly speaking necessary, but ensures that all the points under consideration appear in the order we expect). For all integers N with $N_1 \leq N \leq N_3$ we have:

$$N \geq x_1, \qquad n + \frac{1}{5}\varepsilon_1 \leq f'(N) \leq n + \frac{3}{5}\varepsilon_1, \qquad 0 < f''(N) \leq \varepsilon_2,$$

which implies that N satisfies three out of the four desired conditions.

It remains to show that there exists N with $N_1 \leq N \leq N_3$ such that $\|f(N)\|_{\mathbb{R}/\mathbb{Z}} < \varepsilon_0$. We will in fact show that for each arc $A \subseteq \mathbb{R}/\mathbb{Z}$ with length $2\varepsilon_0$ there exists N with $N_1 \leq N \leq N_3$ such that $f(N) \bmod 1 \in A$. Consider the function $\tilde{f}(N) = f(N) - nN$. Since $\tilde{f}(N) \equiv f(N) \bmod 1$, in the previous condition we may equally well require that $\tilde{f}(N) \bmod 1 \in A$. By the mean value theorem, for $N_1 \leq N < N_3$, the value of the expression

$$\tilde{f}(N+1) - \tilde{f}(N) = f(N+1) - f(N) - n$$

belongs to the interval $\left[\frac{1}{5}\varepsilon_1, \frac{3}{5}\varepsilon_1\right]$. Since $3\varepsilon_1/5 < 2\varepsilon_0$, it follows that, for each interval I of length $2\varepsilon_0$ contained in the interval $[f(N_1), f(N_3)]$, there exists some N with $N_1 \leq N \leq N_3$ with $\tilde{f}(N)$ intersecting I. By the mean value theorem, we have

$$N_3 - N_1 \geq X_3 - X_1 - 2 \geq \frac{f'(X_3) - f'(X_1)}{\max_{X_1 \leq x \leq X_3} f''(x)} - 2$$
$$= \frac{f'(X_3) - f'(X_1)}{f''(X_1)} - 2 \geq \frac{2\varepsilon_1}{5\varepsilon_2} - 2 \geq \frac{10}{\varepsilon_1}.$$

As a consequence, using the mean value theorem yet again, we get

$$f(N_3) - f(N_1) \geq (N_3 - N_1) \min_{N_1 \leq x \leq N_3} f'(x)$$
$$= (N_3 - N_1)f'(N_1) \geq \frac{10}{\varepsilon_1} \cdot \frac{\varepsilon_1}{5} = 2.$$

Thus, we can find an interval $\tilde{A} \subseteq [f(N_1), f(N_3)]$ such that $\tilde{A} \bmod 1 = A$, and we can find N with $N_1 \leq N \leq N_3$ with $\tilde{f}(N) \in \tilde{A}$. This completes the argument. $\square$

Combining Lemmas 4.1 and 4.2, we immediately obtain the following consequence.

Corollary 4.3. *For each M there exists n_0 such that for all $n \geq n_0$ there exists N such that $\lambda(N, M, n)$ holds.*

4.2. **Restricted multiplication.** In the previous subsection, we established sufficient conditions for $\lambda(N, M, n)$ to hold. We now show how we can use λ to define a restricted form of multiplication. Towards this end, we consider the condition $\mu_0(n, m, p)$ given by

$$\exists N \ \exists (0 \leq m < M) \ \lambda(N, M, n) \wedge (a(N + m) = a(N) + p).$$

Recalling that $\lambda(N, M, n)$ implies that $\lfloor f \rfloor (N + m) = \lfloor f \rfloor (N) + nm$, we immediately see that if $\mu_0(n, m, p)$ holds then $p = nm$. Thus, μ_0 defines multiplication on the (definable) set $D_0 \subseteq \mathbb{Z} \times \mathbb{Z}$ consisting of the pairs (n, m) such that $\mu_0(n, m, p)$. Corollary 4.3 now translates into the following statement.

Corollary 4.4. *For each $m \in \mathbb{N}$ there exists t_m such that $[t_m, \infty) \times \{m\} \subseteq D_0$.*

Our next goal is to extend the definition of multiplication from D_0 to all of $\mathbb{Z} \times \mathbb{N}$.

4.3. **Difference sets and total multiplication.** Finally, we show that we can extend the restricted multiplication defined by μ_0 using difference sets. Informally, we rely on the fact that once we have defined nm and $n'm$ we can define $(n - n')m$ by distributivity. To this end, define the following formula:

$$\mu_1(n, m, p) \overset{\text{def}}{=} \exists n', n'', p', p'' \ (\mu_0(n', m, p') \wedge \mu_0(n'', m, p''))$$
$$\wedge \ n = n'' - n' \wedge p = p'' - p').$$

This lets us prove the following lemma.

Lemma 4.5. *Let $m \in \mathbb{N}$ and $n, p \in \mathbb{Z}$. Then the formula $\mu_1(n, m, p)$ holds if and only if $nm = p$.*

Proof. For the rightwards direction of proof, we know already that if $\mu_0(n, m, p)$ holds then $nm = p$. Given that $n'm = p'$ and $n''m = p''$, with $n = n'' - n'$ and $p = p'' - p'$, we can show by a routine computation that $nm = p$. So the rightwards direction of proof is shown.

For the leftwards direction of proof, given that $nm = p$, we fix m. By Corollary 4.4, we know there exists some natural t_m such that $[t_m, \infty) \times \{m\} \subseteq D_0$. Thus we know that multiplication on pairs (n_1, m) is defined by μ_0 when $n_1 > t_m$. So take $n' = t_m$ and $n'' = t_m + n$, and likewise take $p' = n'm$ and $p'' = n''m$. It follows that $\mu_0(n', m, p')$ and $\mu_0(n'', m, p'')$ both hold, and further that $n = n'' - n'$ and $p = p'' - p'$ hold. Therefore $\mu_1(n, m, p)$ holds, as required. $\square$

Once multiplication is defined on $\mathbb{N} \times \mathbb{Z}$ it is immediate to extend it to $\mathbb{Z} \times \mathbb{Z}$. Thus, by Lemma 4.5, we can defined multiplication over the whole domain of $\mathbb{Z} \times \mathbb{Z}$ in the theory $\text{Th}(\mathbb{Z}; <, +, \lfloor f \rfloor)$. It follows that the theory $\text{Th}(\mathbb{Z}; <, +, \lfloor f \rfloor)$ is undecidable, completing the proof of Theorem A.

5. Proof of the sub-linear case

We now move to prove Theorem B. Recall that here we assume f grows at least as fast as x^ε for some $\varepsilon > 0$ but more slowly than x. Using this, we define a function which approximates $f^{-1}(x - (1/2)) + (1/2)$. Given that the latter function is a Hardy field function which grows faster than x, we apply Theorem A and show that the theory $\text{Th}(\mathbb{Z}; <, +, f)$ is undecidable.

Note that throughout we use the fact that, if f is a Hardy field function, then so is f^{-1}; we take this fact from [AvdD04, Theorem 1.7].

Proof of Theorem B. Let $f\colon [x_0, \infty) \to \mathbb{R}$ be a Hardy field function where

$$x^{\varepsilon} \prec f(x) \quad \text{and} \quad f(x) \prec x.$$

both hold for some $\varepsilon > 0$.

Define the function $b(m) = \min\{n \in \mathbb{Z} \mid \lfloor f \rceil (n) \geq m\}$, which behaves roughly like the inverse of $\lfloor f \rceil$. Formally, we define $b(m)$ in our theory as the unique value of n satisfying the formula

$$\lfloor f \rceil (n) \geq m \wedge \forall k \, (\lfloor f \rceil (k) \geq m \to k \geq n).$$

Increasing the value of x_0 if necessary, we may freely assume that f is strictly increasing. Additionally, we define the function $g\colon [y_0, \infty) \to \mathbb{R}$ by $g(y) = f^{-1}(y - (1/2)) + (1/2)$, where y_0 is sufficiently large for the above definition to be well-posed. The main lemma we need to prove Theorem B is the following.

Lemma 5.1. *There exists an integer m_0 such that $b(m) = \lfloor g(m) \rceil$ for all integers $m \geq m_0$.*

Proof. Recall that we assume that $f\colon [x_0, \infty) \to \mathbb{R}$ is a strictly increasing function. Under this assumption, the inverse $f^{-1}\colon [f(x_0), \infty) \to \mathbb{R}$ can be characterised as $f^{-1}(y) = \min\{x \in \mathbb{R} \mid f(x) \geq y\}$. For an integer $m \geq m_0$ and real x we have $f(x) \geq m - 1/2$ if and only if $\lfloor f \rceil (x) \geq m$, directly from the definition of the nearest integer function. Thus, we know that

$$\{x \in \mathbb{R} \mid \lfloor f \rceil (x) \geq m\} = \left\{x \in \mathbb{R} \;\middle|\; f(x) \geq m - \frac{1}{2}\right\}$$
$$= \left\{x \in \mathbb{R} \;\middle|\; x \geq f^{-1}\left(m - \frac{1}{2}\right)\right\} = \left\{x \in \mathbb{R} \;\middle|\; x \geq g(m) - \frac{1}{2}\right\}.$$

Restricting our attention to integers, we conclude that

$$\{n \in \mathbb{Z} \mid n \geq b(m)\} = \{n \in \mathbb{Z} \mid \lfloor f(n) \rceil \geq m\}$$
$$= \left\{n \in \mathbb{Z} \;\middle|\; n + \frac{1}{2} \geq g(m)\right\} = \{n \in \mathbb{Z} \mid n \geq \lfloor g(m) \rceil\}.$$

Thus, we have $b(m) = \lfloor g(m) \rceil$, as needed. $\square$

Now, g is a Hardy field function, as f^{-1} is. Thus, Theorem A can be applied to show the theory $\mathrm{Th}(\mathbb{Z}; <, +, g)$ undecidable. We do this using the following lemma.

Lemma 5.2. *We have $g(x) \prec x$ and $g(x) \succ x^{1/\varepsilon}$.*

Proof. Increasing x_0 if necessary, we may freely assume that f is strictly increasing on $[x_0, \infty)$. We know that for each $\delta > 0$ there exists $n_0 \geq x_0$ such that $n \geq n_0$ we have $f(n) < \delta n$. Taking $m_0 = f(n_0)$, it follows that for all $m \geq m_0$ we have $f^{-1}(m) > (1/\delta)m$. Thus, $f^{-1}(x) \prec x$ and consequently $g(x) \prec x$, as needed. The proof that $g(x) \succ x^{1/\varepsilon}$ is entirely analogous. $\square$

By Lemma 5.2 the theory $\mathrm{Th}(\mathbb{Z}; <, +, g)$ is undecidable. Since by Lemma 5.1 we can define $\lfloor g \rceil$ in $\mathrm{Th}(\mathbb{Z}; <, +, \lfloor f \rceil)$, it follows that the theory $\mathrm{Th}(\mathbb{Z}; <, +, \lfloor f \rceil)$ is undecidable as well. This concludes the proof of Theorem B. $\square$

References

[AvdD04] M. Aschenbrenner and L. van den Dries. Asymptotic differential algebra. *Contemporary Mathematics*, 373:49–85, 2004.

[Bès01] A. Bès. A survey of arithmetical definability. Number suppl., pages 1–54. 2001. A tribute to Maurice Boffa.

[Bos81] M. D. Boshernitzan. An extension of Hardy's class *l* of "orders of infinity". *Journal d'Analyse Mathématique*, 39(1):235–255, December 1981.

[Bos94] M. D. Boshernitzan. Uniform distribution and Hardy fields. *J. Anal. Math.*, 62:225–240, 1994.

[Chu36] A. Church. An unsolvable problem of elementary number theory. *American Journal of Mathematics*, 58(2):345–363, 1936.

[Fra09] N. Frantzikinakis. Equidistribution of sparse sequences on nilmanifolds. *J. Anal. Math.*, 109:353–395, 2009.

[GKP90] R. L. Graham, D. E. Knuth, and O. Patashnik. *Concrete mathematics*. Addison-Wesley, Reading, Mass ;, 1990.

[KM24] J. Konieczny and C. Müllner. Bracket words along Hardy field sequences. *Ergodic Theory Dynam. Systems*, 44(9):2621–2648, 2024.

[Kon24] J. Konieczny. Decidability of extensions of presburger arithmetic by generalised polynomials, 2024.

[Kor01] I. Korec. A list of arithmetical structures complete with respect to the first-order definability. volume 257, pages 115–151. 2001. Weak arithmetics.

[Pre29] M. Presburger. Über die Vollständigkeit eines gewissen systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt. *Comptes Rendus du I congres de Mathematiciens des Pays Slaves*, pages 92–101, 1929.

[Ric22] F. K. Richter. Uniform distribution in nilmanifolds along functions from a hardy field. *Journal d'Analyse Mathématique*, 149(2):421–483, December 2022.

[Sem80] A. L. Semenov. On certain extensions of the arithmetic of addition of natural numbers. *Mathematics of the USSR-Izvestiya*, 15(2):401, apr 1980.

[Sem84] A. L. Semënov. Logical theories of one-place functions on the set of natural numbers. *Mathematics of the USSR-Izvestiya*, 22(3):587, jun 1984.

[Tar53] A. Tarski. *Undecidability of the Elementary Theory of Groups*, volume 13 of *Studies in Logic and the Foundations of Mathematics*, pages 75–86. Elsevier, 1953.

DEPARTMENT OF COMPUTER SCIENCE, UNIVERSITY OF OXFORD, WOLFSON BUILDING, PARKS ROAD, OXFORD OX1 3QD, UK

Email address: `hera.brown0707@gmail.com`

DEPARTMENT OF COMPUTER SCIENCE, UNIVERSITY OF OXFORD, WOLFSON BUILDING, PARKS ROAD, OXFORD OX1 3QD, UK

Email address: `jakub.konieczny@gmail.com`