Logical Methods in Computer Science
Volume 21, Issue 4, 2025, pp. 1:1–1:19
https://lmcs.episciences.org/

Submitted Nov. 12, 2024
Published Oct. 03, 2025

DECIDABILITY OF EXTENSIONS OF PRESBURGER ARITHMETIC BY GENERALISED POLYNOMIALS

JAKUB KONIECZNY

Department of Computer Science, University of Oxford, Wolfson Building, Parks Road, Oxford OX1 3QD, UK
e-mail address: jakub.konieczny@gmail.com

Abstract. We show that the extension of Presburger arithmetic by a quadratic generalised polynomial of a specific form is undecidable.

1. Introduction

1.1. **Background.** Presburger arithmetic, that is, the first-order theory of natural numbers with addition $\mathrm{Th}(\mathbb{N};+)$, is well-known to be decidable. This is in contrast with Peano arithmetic, which also includes multiplication and is well-known to be undecidable. It is not hard to see that if we extend Presburger arithmetic by adding the square function, then we obtain Peano arithmetic; indeed, it is enough to notice that $a \times b = c$ if and only if $(a+b)^2 - a^2 - b^2 = 2c$ (for a survey of relations between different extensions of Presburger arithmetic, see e.g. [Kor01]). On the other hand, the extension of Presburger arithmetic by an exponential function is decidable [Sem84, CP86]. We are thus led to ask: Which functions can we add to Presburger arithmetic and still obtain a decidable theory? For the sake of the discussion below, we point out that the first-order theory of integers with addition and order $\mathrm{Th}(\mathbb{Z};<,+)$ is definitionally equivalent with Presburger arithmetic; we will consider extensions of either $\mathrm{Th}(\mathbb{N};+)$ or $\mathrm{Th}(\mathbb{Z};<,+)$ depending on which is more natural in the given context.

Results concerning decidability of extensions of Presburger arithmetic connected with the multiplicative structure are surveyed in [Bès01]. A wide class of decidable extensions of Presburger arithmetic was investigated by Semenov [Sem80, Sem84]. He showed that $\mathrm{Th}(\mathbb{N};+,f)$ is decidable for each $f\colon \mathbb{N}\to\mathbb{N}$ which fulfils the condition of *effective compatibility with addition*, which asserts, roughly speaking, that f increases rapidly enough and is periodic modulo any integer. An alternative proof of this result was obtained by Cherlin and Point [CP86]. In particular, letting E_k denote the exponential function $E_k(n) = k^n$, this result implies that $\mathrm{Th}(\mathbb{N};+,E_k)$ is decidable. Similarly, letting F denote the factorial $F(n) = n!$, we have that $\mathrm{Th}(\mathbb{N};+,F)$ is decidable.

A *k-automatic sequence* is a sequence $f\colon \mathbb{N}\to\Sigma$, taking values in a finite alphabet Σ, such that $f(n)$ can be computed by a finite automaton given the base-k expansion of n as input. For more background on automatic sequences, see [AS03]. It was shown by Büchi

Key words and phrases: Presburger arithmetic, generalised polynomial, decidability.

DOI:10.46298/LMCS-21(4:1)2025

[Büc62] (with later corrections, for further discussion see e.g. [BHMV94b, BHMV94a]) that for each $k \geq 2$ and each k-automatic sequence $f\colon \mathbb{N} \to \Sigma$ the first-order theory $\mathrm{Th}(\mathbb{N}; +, f)$ is decidable[1]. In fact, it is known that $\mathrm{Th}(\mathbb{N}; +, V_k)$ is decidable and k-automatic sequences are precisely the sequences whose level sets are definable in $(\mathbb{N}; +, V_k)$. Here, $V_k\colon \mathbb{N} \to \mathbb{N}$ denotes the map which takes $k^i n$ to k^i, where $i \in \mathbb{N}$, $n \in \mathbb{N}$ and $k \nmid n$. For further discussion of extensions of Presburger arithmetic related to digital expansions, we refer to the survey paper [BHMV94b] (cf. [BHMV94a]) and to more recent publications such as [HS22] and [Sch23]. More exotic numeration systems are also studied for instance in [MSS16, DMSS16, DMR+17] and [BS19].

A *Sturmian sequence* is a sequence $s_{\alpha,\rho}\colon \mathbb{N} \to \{0, 1\}$ given by

$$s_{\alpha,\rho}(n) = \lfloor \alpha(n+1) + \rho \rfloor - \lfloor \alpha n + \rho \rfloor, \qquad n \in \mathbb{N}, \tag{1.1}$$

where $\alpha \in (0, 1) \setminus \mathbb{Q}$ and $\rho \in [0, 1)$. The first-order theory $\mathrm{Th}(\mathbb{N}; +, s_{\alpha,0})$ is decidable if α is a quadratic irrational and undecidable if the continued fraction expansion is not computable [HT18]. A more comprehensive treatment of Sturmian sequences was carried out in [HMO+22]. The authors prove, among other things, that the first-order theory $\mathrm{Th}(\{(\mathbb{N}; +, s_{\alpha,\rho}) \mid \alpha \in (0, 1) \setminus \mathbb{Q},\ \rho \in [0, 1)\})$ is decidable[2].

As already alluded to earlier, for each polynomial sequence $f\colon \mathbb{Z} \to \mathbb{Z}$ of degree at least 2, multiplication is definable in the language of $(\mathbb{Z}; +, f)$. It follows that $\mathrm{Th}(\mathbb{Z}; +, f)$ is undecidable, and so is $\mathrm{Th}(\mathbb{Z}; <, +, f)$.

1.2. **New results.** In this paper, we are interested in generalised polynomials, that is, expressions built up from the usual real polynomials with the use of the integer part function $\lfloor x \rfloor$, addition and multiplication. For instance, the map $f\colon \mathbb{Z} \to \mathbb{Z}$ given by $f(n) = \left\lfloor \sqrt{2} n^2 \left\lfloor \sqrt{3} n \right\rfloor \right\rfloor + \lfloor \pi n \rfloor \left\lfloor n^3/10 \right\rfloor$ is a generalised polynomial. Generalised polynomials can also be thought of as a far-reaching generalisation of the notion of a Sturmian sequence. These sequences have been extensively studied, see e.g. [BL07, Lei12, AK23] and references therein.

In analogy with polynomials, we expect that the extension of Presburger arithmetic by a given generalised polynomial with at least quadratic rate of growth should be undecidable.

Conjecture 1.1. Let $g\colon \mathbb{Z} \to \mathbb{Z}$ be a generalised polynomial such that

$$\liminf_{n \to \infty} |g(n)| / n^2 > 0. \tag{1.2}$$

Then the first-order theory of $(\mathbb{Z}; <, +, g)$ is undecidable.

As a first step in this direction, we verify this expectation for a specific generalised polynomial with quadratic growth. We believe that similar techniques should work with many other explicit examples, but a fully general result remains elusive. Below, for technical reasons, it will be more convenient to work with the nearest integer operation $\lfloor \cdot \rceil$, given by $\lfloor x \rceil = \lfloor x + 1/2 \rfloor$, rather than with $\lfloor \cdot \rfloor$.

Theorem A. *Let $\alpha, \beta \in \mathbb{R}$, $\beta \neq 0$, be such that $1, \alpha, \alpha^2$ are linearly independent over $\mathbb{Q}$ and let $g\colon \mathbb{Z} \to \mathbb{Z}$ be the generalised polynomial given by*

$$g(n) = \lfloor \beta n \lfloor \alpha n \rceil \rceil \qquad (n \in \mathbb{Z}). \tag{1.3}$$

[1]Formally, we may identify f with $|\Sigma|$ unary predicates corresponding to the level sets $f^{-1}(x)$ for $x \in \Sigma$.

[2]This first-order theory consists, by definition, of all first-order sentences in the language of $(\mathbb{N}; +, s)$ that are true, for all $\alpha \in (0, 1) \setminus \mathbb{Q}$ and $\rho \in [0, 1)$, when s is interpreted as $s_{\alpha,\rho}$; see [HMO+22] for details.

Then the first-order theory of $(\mathbb{Z}; <, +, g)$ *is undecidable.*

In fact, in the situation of Theorem A, the relation $>$ is definable in $(\mathbb{Z}; <, +, g)$. The main ingredient needed here is a result essentially due to Vicky Neale [Nea11] asserting that there exists $s \geq 1$ such that each sufficiently large integer m can be represented as $m = n_1 \lfloor \alpha n_1 \rceil + n_2 \lfloor \alpha n_2 \rceil + \cdots + n_s \lfloor \alpha n_s \rceil$. Since $|g(n) - \beta n \lfloor \alpha n \rceil| \leq 1/2$, it follows that each sufficiently large integer m can be represented as $m = g(n_1) + g(n_2) + \cdots + g(n_s) + r$ where r is bounded (in fact, we can roughly estimate $0 \leq r < r_0 := |\beta| + s$). Since $g(n) \geq 0$ for all $n \in \mathbb{Z}$, we see for all but finitely many $m \in \mathbb{Z}$ we have $m > 0$ if and only if there exist $n_1, n_2, \ldots, n_s \in \mathbb{Z}$ such that for some $0 \leq r < r_0$ we have $m = g(n_1) + g(n_2) + \cdots + g(n_s) + r$. Thus, Theorem A has the following immediate corollary.

Corollary 1.2. *Under the same assumption as in Theorem A, the first-order theory of* $(\mathbb{Z}; +, 1, g)$ *is undecidable.*

One can also construct non-trivial examples of bounded generalised polynomials. For instance, is not hard to verify that the sequence $g \colon \mathbb{Z} \to \{0, 1\}$ given by

$$g(n) = \begin{cases} 1 & \text{if } \left\|n^2\alpha\right\|_{\mathbb{R}/\mathbb{Z}} < \rho, \\ 0 & \text{otherwise,} \end{cases} \quad n \in \mathbb{Z}, \tag{1.4}$$

is a generalised polynomial for any $\alpha, \rho > 0$. The sequence g given by (1.4) can be thought of as a quadratic analogue of a Sturmian sequence. For sequences of this form, we also have an undecidability result.

Theorem B. *Let* $\alpha, \rho \in \mathbb{R}$*, be such that* $0 < \rho < 1/4$ *and* α *is not a linear combination of* 1 *and* ρ *with rational coefficients, and let* $g \colon \mathbb{Z} \to \mathbb{Z}$ *be the generalised polynomial given by* (1.4)*. Then the first-order theory of* $(\mathbb{Z}; <, +, g)$ *is undecidable.*

1.3. **Proof outline.** A key idea behind the proof of Theorem A is that the generalised polynomial in question (or indeed any generalised polynomial) coincides with a polynomial on suitably constructed arbitrarily long arithmetic progressions. Indeed, if we fix an integer L and take $m \in \mathbb{N}$ such that $\|\alpha m\|_{\mathbb{R}/\mathbb{Z}}, \|\beta m\|_{\mathbb{R}/\mathbb{Z}}$ are sufficiently small as a function of L then we can ensure that for $0 \leq l < L$ we have

$$g(lm) = l^2 g(m),$$

meaning in particular that the restriction of g to the arithmetic progression

$$P = \{0, m, 2m, \ldots, (L-1)m\}$$

is a quadratic polynomial. Applying the standard ideas used to define multiplication in terms of the square function, we can then describe triples $a, b, c \in P$ such that $a = km$, $b = lm$ and $c = klm$. The operation $(m, km, lm) \mapsto klm$ can be thought of as a weak substitute of multiplication. In Section 2 we show that the first-order theory of integers equipped with addition and such "weak multiplication" is already undecidable. In Section 3 we flesh out the details of the argument, which in particular involves defining a suitably large family of arithmetic progressions in the first-order language of $(\mathbb{Z}; <, +, g)$.

The proof of Theorem B is shorter and conceptually simpler. The key idea is that, using equidistribution results for (generalised) polynomial sequences, we are able to define properties which are, roughly speaking, equivalent to the statements that fractional parts of

various expressions are sufficiently small. This allows us to define divisibility, which implies undecidability thanks to a classical result of Robinson [Rob49].

1.4. **Future directions.** Our main result, Theorem A, can no doubt be generalised, and is intended largely as a proof of concept. The assumption that $1, \alpha, \alpha^2$ are linearly independent is necessary in order to obtain a suitable equidistribution result in Lemma 3.4 and is most likely not necessary for the result to be true. Below we discuss several other potential future directions.

1.4.1. *Slower growth.* One could consider a stronger variant of Conjecture 1.1 where lim inf is replaced with lim sup in (1.2). The following example shows that this conjecture is false.

Proposition 1.3. *Let $g\colon \mathbb{Z} \to \mathbb{Z}$ be given by*

$$g(n) = \begin{cases} n^2 & \text{if } n = k^{k^m} \text{ for some } m \in \mathbb{N}; \\ 0 & \text{otherwise.} \end{cases}$$

Then g is a generalised polynomial and $\mathrm{Th}(\mathbb{Z}; <, +, g)$ is decidable.

Proof. It follows from [BK18, Thm. C] that g is a generalised polynomial. Letting E_k^+ denote the "exponential" map given by $E_k^+(m) := k^{|m|}$, we see that $g(n) = \ell$ if and only if there exists $m \in \mathbb{Z}$ such that $n = E_k^+(E_k^+(m))$ and $\ell = E_k^+(2E_k^+(m))$. Thus, g is definable in $(\mathbb{Z}; +, E_k^+)$. It remains to note that $\mathrm{Th}(\mathbb{Z}; <, +, E_k^+)$ is decidable because it is definitionally equivalent with $\mathrm{Th}(\mathbb{N}; +, E_k)$, which we have already noted is decidable. □

Despite examples such as the one above, it seems plausible that the condition (1.2) can be weakened to a requirement that g grows at least quadratically on a significant portion of the integers. For instance, one could require that there exists $\varepsilon > 0$ such that for each sufficiently large N there are at least εN integers n with $|n| < N$ and $|g(n)| > \varepsilon n^2$.

1.4.2. *Hardy field sequences.* Instead of generalised polynomials, one can consider other classes of integer-valued sequences whose behaviour resembles polynomials in some useful sense. A natural class of examples is provided by Hardy field sequences, whose relevant properties are discussed e.g. in [Bos94] or [Fra09]. The definition of a Hardy field function is somewhat technical, but for now suffice it to say that these functions include all logarithmic-exponential functions, i.e., functions defined on $\mathbb{R}_+$ which can be expressed using the operations $+, \times, \exp, \log$ and real constants. Thus, for instance, $x \log x$, $x^{3/2}$ and x^x are Hardy field functions of x.

If $f\colon \mathbb{R}_+ \to \mathbb{R}$ is a Hardy field function such that for some $d \in \mathbb{N}$ we have

$$\lim_{x\to\infty} \frac{f(x)}{x^d} > 0, \qquad \lim_{x\to\infty} \frac{f(x)}{x^{d+1}} = 0, \tag{1.5}$$

(including the case where the first limit is ∞), then on long intervals f can be closely approximated by a degree-d polynomial. Combining this fact with the ideas used in the proof of Theorem A, it seems plausible that one could show that for a Hardy field sequence $f\colon \mathbb{R}_+ \to \mathbb{R}$ satisfying (1.5) with $d \geq 2$, the first-order theory of $(\mathbb{Z}; <, +, \lfloor f \rceil)$ is undecidable. (Here, $\lfloor f \rceil$ denotes the sequence given by $\lfloor f \rceil(n) = \lfloor f(n) \rceil$.) A potentially more interesting question concerns the case where $d = 1$:

Question 1.4. Let $f\colon \mathbb{R}_+ \to \mathbb{R}$ be a Hardy field sequence satisfying

$$\lim_{x\to\infty} \frac{f(x)}{x} = \infty, \qquad \lim_{x\to\infty} \frac{f(x)}{x^2} = 0. \tag{1.6}$$

Is the first-order theory of $(\mathbb{Z}; <, +, \lfloor f \rceil)$ decidable?

1.4.3. *Sparse sequences.* Going a step further than Theorem B, we can find $\{0,1\}$-valued generalised polynomials g that are 0 almost everywhere but take the value 1 infinitely often (i.e., $\frac{1}{N}\sum_{n=1}^{N} g(n) \to 0$ and $\sum_{n=1}^{N} g(n) \to \infty$ as $N \to \infty$). In [BK18] we studied the properties of such generalised polynomials, which we dub *sparse*. We also constructed a number of examples. For instance, the indicator function of the Fibonacci numbers 1_{Fib} is a generalised polynomial (see [BK] for the state of the art on sparse generalised polynomials arising from linear recurrence sequences). In this particular case, it is known that the first-order theory of $(\mathbb{N}, +, 1_{\mathrm{Fib}})$ is decidable (e.g. by [Sem80]). It would be interesting to determine the extent to which this result extends to other sparse $\{0,1\}$-valued generalised polynomial sequences.

1.4.4. *Ranges of sequences.* Let $f\colon \mathbb{Z} \to \mathbb{Z}$ be a polynomial of degree at least 2. We have already pointed out that multiplication is definable in the language of $(\mathbb{Z}; <, +, f)$. In fact, it is a standard observation that somewhat more is true: Multiplication is definable in the language of $(\mathbb{Z}; <, +, f(\mathbb{Z}))$, i.e., in Presburger arithmetic extended by the unary predicate corresponding to the image of f. As a representative example, we note the for $f(n) = n^3$ we have $f(n+2) - 2f(n+1) + f(n) = 6n + 6$ so for sufficiently large n, m we have $m = f(n)$ if and only if there exist m', m'' such that m, m', m'' are consecutive elements of $f(\mathbb{Z})$ and $m'' - 2m' + m = 6n + 6$. Thus, f is definable in $(\mathbb{Z}; <, +, f(\mathbb{Z}))$, which brings us back to the result mentioned before.

One is naturally lead to ask if analogous generalisations apply to our results concerning generalised polynomials. This seems highly plausible (in the case of generalised polynomials with at least quadratic growth). Indeed, for g given by (1.3), applying a similar discrete differentiation argument as mentioned in the example above, one can define in $(\mathbb{Z}; <, +, g(\mathbb{Z}))$ a map g' that is reminiscent of g, and it seems likely that $\mathrm{Th}(\mathbb{Z}; <, +, g')$ should be undecidable. Unfortunately, thus obtained g' would be rather less elegant than g, leading to some rather unwieldy computations which we do not pursue at this time.

Acknowledgements. The author is grateful to James Worrell, George Kenison, Andrew Scoones, Mahsa Shirmohammadi, and Bertrand Teguia for many helpful conversations. The author is supported by UKRI Fellowship EP/X033813/1. For the purpose of open access, the authors have applied a Creative Commons Attribution (CC BY) licence to any Author Accepted Manuscript version arising.

Notation. We let $\mathbb{N} = \{1, 2, \dots\}$ denote the set of positive integers and put $\mathbb{N} = \mathbb{N} \cup \{0\}$. We also let $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$ denote the set of non-zero integers.

For $x \in \mathbb{R}$, we let $\lfloor x \rfloor = \max\{n \in \mathbb{Z} \mid n \leq x\}$ denote the integer part of x (also known as the floor of x), $\lceil x \rceil = -\lceil -x \rceil$ the ceiling of x, and $\lfloor x \rceil = \lfloor x + 1/2 \rfloor$ the best integer approximation. Similarly, we let $\{x\} = x - \lfloor x \rfloor \in [0, 1)$ and $\langle x \rangle = x - \lfloor x \rceil \in [-1/2, 1/2)$. Finally, we let $\|x\|_{\mathbb{R}/\mathbb{Z}} = |\langle x \rangle| = \min\{|x - n| \mid n \in \mathbb{Z}\} \in [0, 1/2]$ denote the circle norm of x. We will primarily use the operations $\lfloor \cdot \rceil$ and $\langle \cdot \rangle$ in order to avoid the practical difficulties resulting from the fact that the more commonly used operations $\lfloor \cdot \rfloor$ and $\{\cdot\}$ are discontinuous at 0.

2. Multiplication

In this section we show that the first-order theory of $(\mathbb{Z}; +, 1)$ extended by "poor man's multiplication" is undecidable. Consider a set $\mathcal{Q} \subseteq \mathbb{Z}^4$ satisfying the following properties:

- (Q_1) If $\vec{x} \in \mathcal{Q}$, then there exist $k, l, m \in \mathbb{Z}$ such that $\vec{x} = (m, km, lm, klm)$.
- (Q_2) For each finite set $F \subseteq \mathbb{Z}^2$ there exists $m \in \mathbb{Z}^*$ such that for all $(k, l) \in F$ we have $(m, km, lm, klm) \in \mathcal{Q}$.

Proposition 2.1. *For any set $\mathcal{Q} \subseteq \mathbb{Z}^4$ satisfying (Q_1) and (Q_2), the first-order theory of $(\mathbb{Z}; +, 1, \mathcal{Q})$ is undecidable.*

We can use $\mathcal{Q}$ to define a family of partial binary operators $(\times_m)_{m \in \mathbb{Z}^*}$ which are specified by the rule $a \times_m b = c$ if and only if $(m, a, b, c) \in \mathcal{Q}$. (Formally, we simply mean that we define a partial function from $\mathbb{Z}^3$ to $\mathbb{Z}$, but we find the operator notation more evocative.) Note that property (Q_1) ensures that for each $(m, a, b) \in \mathbb{Z}^* \times \mathbb{Z}^2$ there exists at most one $c \in \mathbb{Z}$ such that $(m, a, b, c) \in \mathcal{Q}$, so this definition is well-posed. In fact, c is necessarily given by $c = ab/m$, so $a \times_m b = ab/m$ if $ab/m \in \mathbb{Z}$ and $(m, a, b, ab/m) \in \mathcal{Q}$, and $a \times_m b$ is undefined otherwise. We let $\mathrm{dom}(\times_m)$ denote the domain of $\times_m$, that is, the set of pairs $(a, b) \in \mathbb{Z}^*$ such that there exists $c \in \mathbb{Z}^*$ with $(m, a, b, c) \in \mathcal{Q}$. An equivalent way of expressing property (Q_2) is that for each finite subset F of $\mathbb{Z}^2$, the dilated copy mF of F is contained in the domain of $\times_m$ for at least one $m \in \mathbb{Z}^*$. We point out that the operation $\times_m$ is commutative, associative and distributive in the sense that we have

$$\begin{aligned} a \times_m b &= b \times_m a && (= ab/m), \\ (a \times_m b) \times_m c &= a \times_m (b \times_m c) && (= abc/m^2), \\ (a + b) \times_m c &= a \times_m c + b \times_m c && (= (a + b)c/m), \end{aligned}$$

assuming that all terms are defined. However, we cannot rule out the possibility that e.g. $a \times_m b$ is defined while $b \times_m a$ is not.

For a term t in the language of $(\mathbb{Z}; 1, +, -, \times)$ with variables $x_1, x_2, \dots, x_s$ and for $m \in \mathbb{Z}^*$ we define t_m to be the expression obtained from t by replacing each instance of $\times$ with $\times_m$. For instance, if

$$t = (x_1 + x_2) \times (x_2 + x_3 + x_3) + (x_1 \times x_1) \times x_3 + 2, \tag{2.1}$$

(using the shorthands $x + y + z = (x + y) + z$ and $2 = 1 + 1$), then t_m is given by

$$t_m = (x_1 + x_2) \times_m (x_2 + x_3 + x_3) + (x_1 \times_m x_1) \times_m x_3 + 2. \tag{2.2}$$

For each polynomial $p \in \mathbb{Z}[x_1, x_2, \ldots, x_s]$, pick once and for all a term $t^{(p)}$ which represents it. For instance, the term t given by (2.1) represents the polynomial p given by

$$\begin{aligned} p(x_1, x_2, x_3) &= (x_1 + x_2)(x_2 + 2x_3) + x_1^2 x_3 + 2 \\ &= x_1 x_2 + x_2^2 + 2x_1 x_3 + 2x_2 x_3 + x_1^2 x_3 + 2. \end{aligned}$$

We then let p_m denote the partial function on $\mathbb{Z}^s$ represented by $t_m^{(p)}$.

Lemma 2.2. *Let $p \in \mathbb{Z}[x_1, x_2, \ldots, x_s]$. Then there exists a finite family $\mathcal{F}(p)$ of pairs of polynomials in $\mathbb{Z}[x_1, x_2, \ldots, x_s]$ such that for $m \in \mathbb{Z}^*$ and $n_1, n_2, \ldots, n_s \in \mathbb{Z}$, the value $p_m(mn_1, mn_2, \ldots, mn_s)$ is defined provided that $mq(n_1, n_2, \ldots, n_s) \in \mathrm{dom}(\times_m)$ for all $q \in \mathcal{F}(p)$, and is equal to $mp(n_1, n_2, \ldots, n_s)$ if defined.*

Proof. We proceed by structural induction. If $p(x_1, x_2, \ldots, x_s) = x_i$ for some $1 \leq i \leq s$, then the claim holds with $\mathcal{F}(p) = \emptyset$, and likewise if $p(x_1, x_2, \ldots, x_s) = 1$. Thus we may assume that p is either the sum $p^{(1)} + p^{(2)}$ or the product $p^{(1)} \times p^{(2)}$ of simpler polynomials. If $p = p^{(1)} + p^{(2)}$, we take $\mathcal{F}(p) = \mathcal{F}(p^{(1)}) \cup \mathcal{F}(p^{(2)})$ and note that by the inductive assumption for $p^{(1)}$ and $p^{(2)}$ we have

$$\begin{aligned} p_m(mn_1, mn_2, \ldots, mn_s) &= p_m^{(1)}(mn_1, mn_2, \ldots, mn_s) + p_m^{(2)}(mn_1, mn_2, \ldots, mn_s) \\ &= mp^{(1)}(n_1, n_2, \ldots, n_s) + mp^{(2)}(n_1, n_2, \ldots, n_s) \\ &= mp(n_1, n_2, \ldots, n_s), \end{aligned}$$

where defined. Similarly, if $p = p^{(1)} \times p^{(2)}$ we take $\mathcal{F}(p) = \mathcal{F}(p^{(1)}) \cup \mathcal{F}(p^{(2)}) \cup \{(p^{(1)}, p^{(2)})\}$ and compute that

$$\begin{aligned} p_m(mn_1, mn_2, \ldots, mn_s) &= p_m^{(1)}(mn_1, mn_2, \ldots, mn_s) \times_m p_m^{(2)}(mn_1, mn_2, \ldots, mn_s) \\ &= mp^{(1)}(n_1, n_2, \ldots, n_s) \times_m mp^{(2)}(n_1, n_2, \ldots, n_s) \\ &= mp(n_1, n_2, \ldots, n_s), \end{aligned}$$

where defined. □

Proof of Prop. 2.1. Let $p \in \mathbb{Z}[x_1, x_2, \ldots, x_s]$ be a polynomial. It follows from Lemma 2.2 that for $n_1, n_2, \ldots, n_s \in \mathbb{Z}$ and $m \in \mathbb{Z}^*$ such that $mq(n_1, n_2, \ldots, n_s) \in \mathrm{dom}(\times_m)$ for all $q \in \mathcal{F}(p)$, we have the equivalence

$$p(n_1, n_2, \ldots, n_s) = 0 \qquad \text{if and only if} \qquad p_m(mn_1, mn_2, \ldots, mn_s) = 0.$$

Since property (Q_2) guarantees the existence of admissible $m \in \mathbb{Z}^*$, we conclude that $p(n_1, n_2, \ldots, n_s) = 0$ if and only if there exists $m \in \mathbb{Z}^*$ such that $p_m(n_1, n_2, \ldots, n_s) = 0$. The last condition is expressible in the first-order language of $(\mathbb{Z}; +, 1, \mathcal{Q})$. Thus, if the first-order theory of $(\mathbb{Z}; +, 1, \mathcal{Q})$ was decidable, then it would also be decidable if a given polynomial equation is solvable, which is well-known to be false (see e.g. [Mat93]). □

3. Proof of Theorem A

3.1. **Setup.** Throughout this section, we let $g\colon \mathbb{Z} \to \mathbb{Z}$ be the generalised polynomial given by

$$g(n) = \lfloor \beta n \lfloor \alpha n \rceil \rceil, \qquad n \in \mathbb{Z}, \tag{3.1}$$

where $\alpha, \beta \in \mathbb{R}$, $\beta \neq 0$ and $1, \alpha, \alpha^2$ are linearly independent over $\mathbb{Q}$. For concreteness, we assume that $\alpha, \beta > 0$; the argument in the other cases is entirely analogous. Replacing $g(n)$ with $g(an)$ for suitably chosen $a \in \mathbb{N}$, we may freely assume that $\beta \in \mathbb{Z}$ or $\beta \in \mathbb{R} \setminus \mathbb{Q}$.

3.2. **Differentiation.** A key feature of generalised polynomials which we will make use of is that their iterated discrete derivatives frequently vanish. For a map $f\colon \mathbb{Z} \to \mathbb{Z}$ and $m \in \mathbb{Z}$ we define the discrete derivative $\Delta_m f\colon \mathbb{Z} \to \mathbb{Z}$ by

$$\Delta_m f(n) = f(n+m) - f(n), \tag{3.2}$$

and the symmetric discrete derivative $\mathbin{\text{\Large$\triangle$}}_m f\colon \mathbb{Z} \to \mathbb{Z}$ by

$$\mathbin{\text{\Large$\triangle$}}_m f(n) = \Delta_m \Delta_n f(0) = f(n+m) - f(n) - f(m) + f(0). \tag{3.3}$$

As an illustrative example, we point out that if f is a polynomial sequence of degree $d \geq 1$ and $m \neq 0$, then $\mathbin{\text{\Large$\triangle$}}_m f$ is a polynomial of degree $d-1$ (and if f is constant, then $\mathbin{\text{\Large$\triangle$}}_m f$ is identically zero). In order to avoid the excessive use of subscripts, and in order to emphasise the symmetry $\mathbin{\text{\Large$\triangle$}}_m f(n) = \mathbin{\text{\Large$\triangle$}}_n f(m)$, for each $r \geq 1$ and $n_0, n_1, \dots, n_r \in \mathbb{Z}$ we let

$$\mathbin{\text{\Large$\triangle$}}^r f(n_0, n_1, \dots, n_r) = \mathbin{\text{\Large$\triangle$}}_{n_r} \dots \mathbin{\text{\Large$\triangle$}}_{n_1} f(n_0). \tag{3.4}$$

Lemma 3.1. *There exists a constant $C \geq 1$, dependent only on α and β, such that the following is true. Let $n_0, n_1, n_2 \in \mathbb{N}$ satisfy $n_0, n_1/n_0, n_2/n_1 \geq C$. Then $\mathbin{\text{\Large$\triangle$}}^2 g(n_0, n_1, n_2) = 0$ if and only if*

(i) for all $I \subseteq \{0,1,2\}$ we have $\big\lfloor \sum_{i \in I} \langle \alpha n_i \rangle \big\rceil = 0$;
(ii) letting $\gamma_I := \sum_{i,j \in I} \langle \beta n_i \lfloor \alpha n_j \rceil \rangle$ for $I \subseteq \{0,1,2\}$, we have

$$\lfloor \gamma_{\{0,1,2\}} \rceil = \lfloor \gamma_{\{0,1\}} \rceil + \lfloor \gamma_{\{1,2\}} \rceil + \lfloor \gamma_{\{2,0\}} \rceil .$$

Henceforth, we let C denote a constant that is admissible in Lemma 3.1 above.

Proof. We can explicitly compute that for $n, m \in \mathbb{N}$ we have

$$\begin{aligned} \mathbin{\text{\Large$\triangle$}} g(n,m) &= \big\lfloor \beta(n+m)\big(\lfloor \alpha n \rceil + \lfloor \alpha m \rceil + e(n,m)\big)\big\rceil - \lfloor \beta n \lfloor \alpha n \rceil \rceil - \lfloor \beta m \lfloor \alpha m \rceil \rceil \\ &= \lfloor \beta n \lfloor \alpha m \rceil \rceil + \lfloor \beta m \lfloor \alpha n \rceil \rceil + \lfloor \beta(n+m) \rceil e(n,m) + f(n,m), \end{aligned}$$

where $e(n,m) \in \{-1,0,1\}$ and $f(n,m) \in \{-4,-3,\dots,3,4\}$ are given by

$$\begin{aligned} e(n,m) &= \lfloor \alpha n + \alpha m \rceil - \lfloor \alpha n \rceil - \lfloor \alpha m \rceil , \\ f(n,m) &= \big\lfloor \beta(n+m)\big(\lfloor \alpha n \rceil + \lfloor \alpha m \rceil + e(n,m)\big)\big\rceil - \lfloor \beta n \lfloor \alpha n \rceil \rceil - \lfloor \beta m \lfloor \alpha m \rceil \rceil \\ &\quad - \lfloor \beta n \lfloor \alpha m \rceil \rceil - \lfloor \beta m \lfloor \alpha n \rceil \rceil - \lfloor \beta(n+m) \rceil e(n,m). \end{aligned}$$

Similarly, we can compute that for $n_0, n_1, n_2 \in \mathbb{N}$ we have

$$\begin{aligned} g(n_0+n_1+n_2) = g(n_0) + g(n_1) + g(n_2) + \textstyle\sum_{i \neq j} \lfloor \beta n_i \lfloor \alpha n_j \rceil \rceil \\ + \lfloor \beta(n_0+n_1+n_2) e(n_0,n_1,n_2) \rceil + f(n_0,n_1,n_2), \end{aligned}$$

where $e(n_0, n_1, n_2) \in \{-1, 0, 1\}$ is given by

$$\begin{aligned} e(n_0, n_1, n_2) &= \lfloor \alpha n_0 + \alpha n_1 + \alpha n_2 \rceil - \lfloor \alpha n_0 \rceil - \lfloor \alpha n_1 \rceil - \lfloor \alpha n_2 \rceil, \\ &= \lfloor \langle \alpha n_0 \rangle + \langle \alpha n_1 \rangle + \langle \alpha n_2 \rangle \rceil \end{aligned}$$

and $f(n_0, n_1, n_2)$ is given by a similar formula. We stress that $|e(n_0, n_1, n_2)| \leq 1$, which follows from the fact that $-3/2 < \langle \alpha n_0 \rangle + \langle \alpha n_1 \rangle + \langle \alpha n_2 \rangle < 3/2$.

Suppose that $\Delta^2 g(n_0, n_1, n_2) = 0$. Combining the formulas above, we see that

$$\begin{aligned} 0 = \Delta^2 g(n_0, n_1, n_2) = \beta(n_0 + n_1 + n_2) e(n_0, n_1, n_2) - \beta(n_0 + n_1) e(n_0, n_1) \\ - \beta(n_1 + n_2) e(n_1, n_2) - \beta(n_2 + n_0) e(n_2, n_0) + O(1). \end{aligned}$$

Rearranging and dividing by β we obtain

$$\begin{aligned} 0 = {} & n_2 \left(e(n_0, n_1, n_2) - e(n_1, n_2) - e(n_2, n_0) \right) \\ & + n_1 \left(e(n_0, n_1, n_2) - e(n_0, n_1) - e(n_1, n_2) \right) \\ & + n_0 \left(e(n_0, n_1, n_2) - e(n_0, n_1) - e(n_2, n_0) \right) + O(1). \end{aligned}$$

Provided that the constant C was chosen large enough, it follows that the contributions from n_2, n_1 and n_0 above must all be zero, meaning that

$$\begin{aligned} e(n_0, n_1, n_2) - e(n_1, n_2) - e(n_2, n_0) &= 0, \\ e(n_0, n_1, n_2) - e(n_0, n_1) - e(n_1, n_2) &= 0, \\ e(n_0, n_1, n_2) - e(n_0, n_1) - e(n_2, n_0) &= 0. \end{aligned}$$

Comparing the three equations above, we infer that for some $e \in \{-1, 0, 1\}$ we have

$$e(n_0, n_1) = e(n_1, n_2) = e(n_2, n_0) = e, \qquad e(n_0, n_1, n_2) = 2e.$$

Since $e(n_0, n_1, n_2) \in \{-1, 0, 1\}$, it follows that $e = 0$. This implies condition (i). In order to obtain (ii), we expand the equality $\Delta^2 g(n_0, n_1, n_2) = 0$ (using the simplifications resulting from (i)) and replace each instance of $\beta n_i \lfloor \alpha n_j \rceil$ with $\langle \beta n_i \lfloor \alpha n_j \rceil \rangle + \lfloor \beta n_i \lfloor \alpha n_j \rceil \rceil$.

The proof of the converse direction follows along similar lines. Indeed, as alluded to above, assuming condition (i), an elementary computation shows that the condition $\Delta^2 g(n_0, n_1, n_2) = 0$ is equivalent to condition (ii). □

3.3. **Fractional parts.** Our next goal is to express in the first-order logic of the theory under consideration the condition that the circle norm $\|\alpha n\|_{\mathbb{R}/\mathbb{Z}}$ is small for some $n \in \mathbb{N}$. The following lemma will be helpful.

Lemma 3.2. *Let $n_0, n_1 \in \mathbb{N}$ satisfy $n_0, n_1/n_0 \geq C$. Then the following conditions are equivalent:*

(i) there exists $n_2 \in \mathbb{N}$ with $n_2 \geq C n_1$ such that $\Delta^2 g(n_0, n_1, n_2) = 0$;
(ii) $|\langle \alpha n_0 \rangle + \langle \alpha n_1 \rangle| < 1/2$;

Proof. The implication (i) ⇒ (ii) is already contained in Lemma 3.1, so we only need to verify the converse implication (ii) ⇒ (i). It follows e.g. from the characterisation of distributions of generalised polynomials in [Lei12] that there exists a sequence $(n_2^{(k)})_{k=1}^{\infty}$ (with $n_2^{(k)} \to \infty$

as $k \to \infty$) such that all fractional parts appearing in the conditions in Lemma 3.1 and involving $n_2^{(k)}$ tend to 0 as $k \to \infty$, i.e.,

$$\begin{aligned} \left\langle \alpha n_2^{(k)} \right\rangle &\to 0, & \left\langle \beta n_2^{(k)} \left\lfloor \alpha n_2^{(k)} \right\rceil \right\rangle &\to 0, \\ \left\langle \beta n_0 \left\lfloor \alpha n_2^{(k)} \right\rceil \right\rangle &\to 0, & \left\langle \beta n_1 \left\lfloor \alpha n_2^{(k)} \right\rceil \right\rangle &\to 0, \\ \left\langle \beta n_2^{(k)} \left\lfloor \alpha n_0 \right\rceil \right\rangle &\to 0, & \left\langle \beta n_2^{(k)} \left\lfloor \alpha n_1 \right\rceil \right\rangle &\to 0. \end{aligned}$$

As a consequence, for all sufficiently large k we have

$$\left\lfloor \langle \alpha n_0 \rangle + \langle \alpha n_1 \rangle + \langle \alpha n_2^{(k)} \rangle \right\rceil = \left\lfloor \langle \alpha n_0 \rangle + \langle \alpha n_1 \rangle \right\rceil = 0,$$

and by the same token

$$\left\lfloor \langle \alpha n_0 \rangle + \langle \alpha n_2^{(k)} \rangle \right\rceil = \left\lfloor \langle \alpha n_1 \rangle + \langle \alpha n_2^{(k)} \rangle \right\rceil = 0$$

Similarly, with $\gamma_I^{(k)}$ defined as in Lemma 3.1(ii) with $n_2^{(k)}$ in place of n_2, for sufficiently large k we have

$$\left\lfloor \gamma_{\{0,1,2\}}^{(k)} \right\rceil = \left\lfloor \gamma_{\{0,1\}}^{(k)} \right\rceil, \qquad \left\lfloor \gamma_{\{0,2\}}^{(k)} \right\rceil = \left\lfloor \gamma_{\{0\}}^{(k)} \right\rceil = 0, \qquad \left\lfloor \gamma_{\{1,2\}}^{(k)} \right\rceil = \left\lfloor \gamma_{\{1\}}^{(k)} \right\rceil = 0.$$

In particular, it follows that we have

$$\left\lfloor \gamma_{\{0,1,2\}}^{(k)} \right\rceil = \left\lfloor \gamma_{\{0,1\}}^{(k)} \right\rceil + \left\lfloor \gamma_{\{1,2\}}^{(k)} \right\rceil + \left\lfloor \gamma_{\{2,0\}}^{(k)} \right\rceil.$$

Thus, Lemma 3.1 implies that $\Delta^2 g(n_0, n_1, n_2^{(k)}) = 0$ for sufficiently large k. □

Motivated by Lemma 3.2, we introduce the following properties

$$\mu(n_0, n_1): \quad (\exists\, n_2)\ (n_2 \geq C n_1) \wedge (\Delta^2 g(n_0, n_1, n_2) = 0) \qquad (n_0, n_1 \in \mathbb{N}); \tag{3.5}$$

$$\psi(m, N): \quad (\forall\, n)\ (n \leq N) \Rightarrow \mu(n, m) \qquad (m, N \in \mathbb{N}). \tag{3.6}$$

Lemma 3.3. *For each $\varepsilon > 0$ there exists $N \in \mathbb{N}$ such that for all $m \in \mathbb{N}$, if $\psi(m, N)$ holds, then $\|\alpha m\|_{\mathbb{R}/\mathbb{Z}} < \varepsilon$. Conversely, for each $N \in \mathbb{N}$ there exists $\varepsilon > 0$ such that if $\|\alpha m\|_{\mathbb{R}/\mathbb{Z}} < \varepsilon$, then $\psi(m, N)$ holds.*

Proof. It follows from Lemma 3.2 that $\psi(m, N)$ holds if and only if

$$-\frac{1}{2} - \min_{n \leq N} \langle \alpha n \rangle < \langle \alpha m \rangle < \frac{1}{2} - \max_{n \leq N} \langle \alpha n \rangle. \tag{3.7}$$

It remains to notice that the expression on the left side of (3.7) tends to 0 from below as $N \to \infty$, and the analogous statement applies to the expression on the right side. □

3.4. **Divisibility.** We will next construct a first-order formula that expresses a condition closely related to divisibility of integers. We will need the following technical lemma, which is the only place where we make use of the assumption that α^2 is linearly independent of $1, \alpha$ over $\mathbb{Q}$.

Lemma 3.4. *Let $\alpha \in \mathbb{R}$ be such that $1, \alpha, \alpha^2$ are linearly independent over $\mathbb{Q}$. Let $\theta = \frac{a+\alpha b}{c+\alpha d}$ with $a, b, c, d \in \mathbb{Z}$, $d \neq 0$ and $\theta \notin \mathbb{Q}$. Then the sequence $(\langle \alpha n \rangle, \langle \alpha \lfloor \theta n \rceil \rangle)_{n\in\mathbb{Z}}$ is equidistributed with respect to the measure on $[-1/2, 1/2)$ which is the push-forward of the normalised Lebesgue measure on $\{0, 1, \dots, d-1\} \times [-1/2, 1/2) \times [-1/2, 1/2)$ through the map*

$$(r, x, y) \mapsto (\langle dx + \alpha r \rangle, \langle bx - cy + \alpha\theta r - \alpha \langle dy + \theta r \rangle \rangle). \tag{3.8}$$

In particular, the point $(0, 0)$ belongs to the interior of the closure of the orbit

$$\left\{ \left(\langle \alpha n \rangle, \langle \alpha \lfloor \theta n \rceil \rangle \right) \;\middle|\; n \in \mathbb{Z} \right\}.$$

Proof. Let $n \in \mathbb{Z}$ and write $n = dn' + r(n)$ where $n' \in \mathbb{Z}$ and $0 \leq r(n) < d$. Put also $x(n) = \langle \alpha n' \rangle$ and $y(n) = \langle \theta n' \rangle$. Since $1, \alpha, \theta$ are linearly independent over $\mathbb{Q}$, the sequence $(r(n), x(n), y(n))_{n\in\mathbb{Z}}$ is equidistributed in $\{0, 1, \dots, d-1\} \times [-1/2, 1/2) \times [-1/2, 1/2)$. Note that $\alpha\theta d = a + \alpha b - \theta c$. We can compute that

$$\begin{aligned}
\langle \alpha n \rangle &= \langle dx(n) + \alpha r(n) \rangle, \\
\langle \alpha \lfloor \theta n \rceil \rangle &= \langle \alpha\theta n - \alpha \langle \theta n \rangle \rangle \\
&= \left\langle (a + \alpha b - \theta c)n' + (\alpha\theta r(n)) - \alpha \left\langle \theta d n' + \theta r(n) \right\rangle \right\rangle \\
&= \langle bx(n) - cy(n) + \alpha\theta r(n) - \alpha \langle dy(n) + \theta r(n) \rangle \rangle
\end{aligned}$$

This proves the first part of the statement. For the second part, we may take $r = 0$ in (3.8); it will suffice to show that $(0, 0)$ belongs to the interior of the image of $[-1/2, 1/2) \times [-1/2, 1/2)$ through the map given by

$$(x, y) \mapsto (\langle dx \rangle, \langle bx - cy - \alpha \langle dy \rangle \rangle). \tag{3.9}$$

This can be accomplished, for instance, by noting that the point $(0, 0)$ is non-singular and is mapped to $(0, 0)$. □

Lemma 3.5. *Let $n, n' \in \mathbb{N}$ and let $h \geq 1$. Suppose that for each $\varepsilon' > 0$ there exists $\varepsilon > 0$ such that for each $m \in \mathbb{N}$ with $\|\alpha m\|_{\mathbb{R}/\mathbb{Z}} < \varepsilon$ there exists $m' \in \mathbb{N}$ with $\|\alpha m'\|_{\mathbb{R}/\mathbb{Z}} < \varepsilon'$ such that $|\, \Delta\, g(n, m') - \Delta\, g(n', m)| \leq h$. Then $\lfloor \alpha n' \rceil \,/\, \lfloor \alpha n \rceil = n'/n \in \mathbb{N}$.*

Proof. Our first goal is to show that

$$\theta := \frac{\alpha n' + \lfloor \alpha n' \rceil}{\alpha n + \lfloor \alpha n \rceil}$$

is rational. For the sake of contradiction, suppose otherwise. It follows from Lemma 3.4 that for any $x \in \mathbb{R}$ with sufficiently small absolute value we can find a sequence $(m_i)_{i=1}^{\infty}$ such that $\langle \alpha m_i \rangle \to 0$ and $\langle \alpha \lfloor \theta m_i \rceil \rangle \to x$ as $i \to \infty$. It follows from the assumptions that we can find a sequence $(m_i')_{i=1}^{\infty}$ with $\langle \alpha m_i' \rangle \to 0$ such that for all $i \in \mathbb{N}$ we have

$$\left| \Delta\, g(n, m_i') - \Delta\, g(n', m_i) \right| \leq h. \tag{3.10}$$

Restricting our attention to i such that $\langle \alpha m_i \rangle$ and $\langle \alpha m_i' \rangle$ are sufficiently small with respect to n and n', we conclude from (3.10) that

$$m_i' \lfloor \alpha n \rceil + n \left\lfloor \alpha m_i' \right\rceil = m_i \left\lfloor \alpha n' \right\rceil + n' \lfloor \alpha m_i \rceil + O(h). \tag{3.11}$$

Computing m_i' from (3.11) we obtain

$$m_i' = \theta m_i + O(h+n+n'). \tag{3.12}$$

Thus, there is a bounded sequence $(c_i)_{i=1}^{\infty}$ (with $|c_i| = O(h+n+n')$) such that $m_i' = \lfloor \theta m_i \rceil + c_i$ for all $i \in \mathbb{N}$. In particular, we have

$$\alpha m_i' = \alpha \lfloor \theta m_i \rceil + \alpha c_i. \tag{3.13}$$

Passing to a subsequence where $c_i = c$ is constant, taking (3.13) modulo 1 and letting $i \to \infty$, we conclude that

$$0 \equiv x + \alpha c \bmod 1. \tag{3.14}$$

Recall that x was arbitrary, subject only to the constraint that $|x|$ is sufficiently small. Picking any $x \in \mathbb{R} \setminus (\mathbb{Z} + \alpha\mathbb{Z})$ we reach a contradiction, proving that $\theta \in \mathbb{Q}$.

Next, we observe that θ is an integer. Indeed, if we had $\theta = a/b \in \mathbb{Q}\setminus\mathbb{Z}$ with $\gcd(a,b) = 1$, then we could run the same argument as above with $x = 1/b$, again leading to a contradiction. Since the argument is fully analogous, we omit the details. Finally, since α is irrational, $\theta \in \mathbb{N}$ implies that $\lfloor \alpha n' \rceil / \lfloor \alpha n \rceil = n'/n = \theta$. □

It is not hard to see that the converse to Lemma 3.5 also holds. Indeed, if $n, n' \in \mathbb{N}$ are such that $\lfloor \alpha n' \rceil \,/\, \lfloor \alpha n \rceil = n'/n =: t$, then for each sufficiently small $\varepsilon > 0$ and each $m \in \mathbb{N}$ and $m' := tm$ with $\|\alpha m\|_{\mathbb{R}/\mathbb{Z}} < \varepsilon$ we have

$$\begin{aligned} \beta m' \lfloor \alpha n \rceil &= \beta m \lfloor \alpha n' \rceil = t\beta m \lfloor \alpha n \rceil, \\ \beta n \lfloor a m' \rceil &= \beta n' \lfloor \alpha m \rceil = t\beta n \lfloor a m \rceil, \\ \text{and hence} \qquad \big| \mathbf{\Delta}\, g(n,m') - \mathbf{\Delta}\, g(n',m) \big| &\le 2. \end{aligned}$$

(Specifically, we need $\varepsilon < 1/(2t)$ and $\varepsilon + t\,\|\alpha n\|_{\mathbb{R}/\mathbb{Z}} < 1/2$ and $t\varepsilon + \|\alpha n\|_{\mathbb{R}/\mathbb{Z}} < 1/2$.)

Motivated by Lemma 3.5 and the discussion above, we define

$$\begin{aligned} \delta(n,n'): \qquad & (\exists\ H)\ (\forall\ M')\ (\exists\ M)\ (\forall\ m)\ \psi(m,M) \Rightarrow \\ & (\exists\ m')\ \psi(m',M') \wedge \big| \mathbf{\Delta}\, g(n,m') - \mathbf{\Delta}\, g(n',m) \big| \le H \qquad (n,n' \in \mathbb{N}). \end{aligned} \tag{3.15}$$

Lemma 3.6. *Let $n, n' \in \mathbb{N}$. Then $\delta(n,n')$ holds if and only if $\lfloor \alpha n' \rceil \,/\, \lfloor \alpha n \rceil = n'/n \in \mathbb{N}$.*

Proof. Follows by combining Lemma 3.5 with Lemma 3.3. □

For later reference, we point out that for $n' = tn$ the condition $\lfloor \alpha n' \rceil \,/\, \lfloor \alpha n \rceil = n'/n$ is equivalent to $t\,\|\alpha n\|_{\mathbb{R}/\mathbb{Z}} < 1/2$.

3.5. **Arithmetic progressions.** It follows from Lemma 3.5 that for each $k \in \mathbb{N}$, the set of $n \in \mathbb{N}$ for which $\delta(k,n)$ holds is an arithmetic progression with step k, starting at k. For $k \in \mathbb{N}$, let $\ell(k)$ be the endpoint of the aforementioned arithmetic progression; more explicitly, $\ell(k) = k\lfloor 1/(2\,\|\alpha k\|_{\mathbb{R}/\mathbb{Z}}) \rfloor$. Note that $\ell(k)$ is the unique integer $n \in \mathbb{N}$ such that $\delta(k,n)$ and $\neg\delta(k,n+k)$, and as a consequence the map $\ell\colon \mathbb{N} \to \mathbb{N}$ is defined by a first-order formula.

The discussion above allows us to talk about arithmetic progressions in the first-order language under consideration. Indeed, for $k, h \in \mathbb{N}$ with $h \le \ell(k)$ we can define the arithmetic progression

$$P_{m,h} = \{tm \mid 1 \le t \le h/m\} = \{n \in \mathbb{N} \mid (m \le n \le h) \wedge \delta(m,n)\}. \tag{3.16}$$

We are specifically interested in arithmetic progressions P such that the restriction of g to P coincides with a classical (as opposed to generalised) polynomial. This property can be expressed easily enough.

Lemma 3.7. *Let $m, h \in \mathbb{N}$ be such that $3m \leq h \leq \ell(m)$. The following conditions are equivalent*

(i) there exists a degree-2 polynomial p such that $g(n) = p(n)$ for all $n \in P_{m,h}$;
(ii) there exists $a \in \mathbb{Z}^*$ such that $\Delta_m^2 g(n) = a$ for all $n \in P_{m,h-2m}$.

Proof. The implication (i) $\Rightarrow$ (ii) holds because the application of Δ_m decreases the degree of a polynomial by 1. Conversely, if (ii) holds and p is the (unique) polynomial of degree at most 2 with $p(tm) = g(tm)$ for $t \in \{1, 2, 3\}$, then the leading coefficient of p is $a/(2m^2) \neq 0$ and a simple inductive argument shows that $g(n) = p(n)$ for all $n \in P_{m,h}$. □

We let $\pi(m, h)$ denote the assertion that the progression $P_{m,h}$ is admissible:

$$\begin{aligned} \pi(m,h): \qquad & \big(3m \leq h \leq \ell(m)\big) \wedge (\exists\ a \in \mathbb{Z}^*) \\ & (\forall\ n \in P_{m,h-2m})\ \ \Delta_m^2\, g(n) = a \qquad\qquad (m, h \in \mathbb{N}). \end{aligned} \tag{3.17}$$

We will need to know that admissible arithmetic progressions can be arbitrarily long. The following lemma gives a sufficient condition.

Lemma 3.8. *Let $m, r \in \mathbb{N}$, $r \geq 2$. Then $\pi(m, rm)$ holds provided that*

$$\|\alpha m\|_{\mathbb{R}/\mathbb{Z}} < \frac{1}{2r} \qquad\qquad \|\beta m \lfloor \alpha m \rceil\|_{\mathbb{R}/\mathbb{Z}} < \frac{1}{2r^2}. \tag{3.18}$$

Proof. Recall from earlier discussion that the first condition in (3.18) implies that $\ell(m) \geq rm$. For $t \leq r$ we now have

$$g(tm) = \lfloor \beta tm \lfloor \alpha tm \rceil \rceil = \left\lfloor \beta t^2 m \lfloor \alpha m \rceil \right\rceil = t^2 \lfloor \beta m \lfloor \alpha m \rceil \rceil\,.$$

Thus, for $n \in P_{m,h}$ we have $g(n) = (n/m)^2 g(m)$, which in particular is a polynomial in n, as needed. □

Note that for each r, there exist $m \in \mathbb{N}$ such that (3.18) holds. This can be inferred for instance from another reference to [Lei12].

3.6. **Multiplicative quadruples.** With a view towards applying the results of Section 2, we are now ready to define a set of multiplicative quadruples:

$$\mathcal{Q} = \left\{ (m,a,b,c) \in \mathbb{N}^4 \;\middle|\; \begin{array}{l} (\exists\ h \in \mathbb{N})\ \pi(m,h) \wedge a, b, a+b, m+c \in P_{m,h} \\ \wedge\ \boldsymbol{\Delta}\, g(m,c) = \boldsymbol{\Delta}\, g(a,b) \end{array} \right\} \tag{3.19}$$

Since for a degree-2 polynomial $p(n) = a_2 n^2 + a_1 n_1 + a_0$ we have $\boldsymbol{\Delta}\, p(n,m) = 2a_2 nm$, it follows directly from the definition of $\mathcal{Q}$ that for all $(m,a,b,c) \in \mathcal{Q}$ we have $mc = ab$, and consequently $a = km$, $b = lm$ and $c = klm$ for some $k, l \in \mathbb{N}$. In fact, by the same argument we see that $(m,a,b,c) \in \mathcal{Q}$ if and only if $a = km$, $b = lm$ and $c = klm$ for some $k, l \in \mathbb{N}$ such that $\pi(m, (kl+1)m)$ holds. It follows from Lemma 3.8 that, given $k, l \in \mathbb{N}$, one can find $m \in \mathbb{N}$ such that $\pi(m, (kl+1)m)$ holds, and hence the set $\mathcal{Q}$ given by (3.19) satisfies condition (Q_2) restricted to $F \subseteq \mathbb{N}^2$. Let

$$\mathcal{Q}_\pm = \{(m, \sigma a, \tau b, \sigma\tau c) \mid (m,a,b,c) \in \mathcal{Q},\ \sigma, \tau = \pm 1\}\,.$$

It follows from discussion above that the set $\mathcal{Q}_\pm$ satisfies conditions (Q_1) and (Q_2). Hence, we are in position to apply Proposition 2.1, which completes the proof of Theorem A.

4. Proof of Theorem B

4.1. **Setup.** Throughout this section, we let $g\colon \mathbb{Z} \to \{0,1\}$ be the generalised polynomial given by

$$g(n) = \begin{cases} 1 & \text{if } \left\|\alpha n^2\right\|_{\mathbb{R}/\mathbb{Z}} < \rho, \\ 0 & \text{otherwise,} \end{cases} \qquad n \in \mathbb{Z}, \tag{4.1}$$

where $\alpha \in \mathbb{R}$, $\rho \in (0, 1/4)$ and α is not a linear combination of 1 and ρ with rational coefficients.

4.2. **Small fractional parts.** Our first step is to express the property that $\|2\alpha n\|_{\mathbb{R}/\mathbb{Z}}$ and $\left\|\alpha n^2\right\|_{\mathbb{R}/\mathbb{Z}}$ are both small. Consider the following property:

$$\mu(m,N): \qquad (\forall\ n \le N)\ g(n+m) = g(n) \qquad (m, N \in \mathbb{N}). \tag{4.2}$$

Lemma 4.1. *For each $\varepsilon > 0$ there exists $N \in \mathbb{N}$ such that for all $m \in \mathbb{N}$, if $\mu(m,N)$ holds, then $\|2\alpha m\|_{\mathbb{R}/\mathbb{Z}} < \varepsilon$ and $\left\|\alpha m^2\right\|_{\mathbb{R}/\mathbb{Z}} < \varepsilon$. Conversely, for each $N \in \mathbb{N}$ there exists $\varepsilon > 0$ such that if $\|2\alpha m\|_{\mathbb{R}/\mathbb{Z}} < \varepsilon$ and $\left\|\alpha m^2\right\|_{\mathbb{R}/\mathbb{Z}} < \varepsilon$, then $\mu(m,N)$ holds.*

Proof. Let $\varepsilon > 0$ and let N be a large integer, to be specified in the course of the argument. If $\mu(m,N)$ holds, then for each $n \le N$ we have the equivalence

$$\left\|\alpha n^2\right\|_{\mathbb{R}/\mathbb{Z}} < \rho \qquad \Longleftrightarrow \qquad \left\|\alpha n^2 + \langle 2\alpha m\rangle\, n + \left\langle \alpha m^2 \right\rangle\right\|_{\mathbb{R}/\mathbb{Z}} < \rho. \tag{4.3}$$

Put $\beta := \langle 2\alpha m\rangle$ and $\gamma := \left\langle \alpha m^2 \right\rangle$. Condition (4.3) implies in particular that there is no $n \le N$ such that $\left\langle \alpha n^2 \right\rangle \in (\frac{9}{10}\rho, \rho)$ and $\langle \beta n + \gamma\rangle \in (\frac{1}{10}\rho, \frac{2}{10}\rho)$. It follows that for some ρ' dependent only on ρ, using the terminology of [GT12], the sequence $\big(\big(\alpha n^2, \beta n + \gamma\big)\big)_{n=1}^N$ fails to be ρ'-equidistributed. Assuming, as we may, that N is sufficiently large, it follows (e.g. as a very special case of the quantitative Leibman theorem from [GT12]) that there exists $k \in \mathbb{N}$, bounded by a constant K dependent only on ρ, such that $\|k\beta\|_{\mathbb{R}/\mathbb{Z}} \ll_\rho 1/N$. Thus (possibly after replacing k by a factor), we may write $\beta = b/k + x/N$ where $0 \le b < k$ and $\gcd(b,k) = 1$ and $|x| \ll_\rho 1$.

We claim that $|\gamma| \le \varepsilon$. Suppose conversely that this was not the case, and for the sake of concreteness assume that $\gamma \ge \varepsilon$. Then, assuming that N is sufficiently large, we use quantitative equidistribution results for polynomial sequences (e.g. [GT12]) to find $n \in \mathbb{N}$ such that

$$\left\langle \alpha n^2 \right\rangle \in (\rho - \varepsilon, \rho), \qquad \langle \beta n\rangle \in (-\varepsilon/2, \varepsilon/2), \qquad n\,|x| < (\varepsilon/2)N. \tag{4.4}$$

This implies $\left\|\alpha n^2\right\|_{\mathbb{R}/\mathbb{Z}} < \rho$ and $\left\|\alpha n^2 + \beta n + \gamma\right\|_{\mathbb{R}/\mathbb{Z}} > \rho$, contradicting (4.3).

Next, we claim that $b = 0$, or equivalently, $k = 1$. Suppose conversely. Arguing like above, we find $n \in \mathbb{N}$ such that

$$\left\langle \alpha n^2 \right\rangle \in (\rho - \varepsilon, \rho), \qquad nb \equiv 1 \bmod k, \qquad n\,|x| < (\varepsilon/2)N. \tag{4.5}$$

It follows that $\left\|\alpha n^2\right\|_{\mathbb{R}/\mathbb{Z}} < \rho$ and, assuming, as we may, that $\varepsilon < 1/2K$, we have

$$\left\|\alpha n^2 + \beta n + \gamma\right\|_{\mathbb{R}/\mathbb{Z}} \geq \rho + \frac{1}{k} - 2\varepsilon > \rho,$$

which again contradicts (4.3), and completes the proof of the first statement.

We proceed to the proof of the second part of the lemma. Let $N \in \mathbb{N}$ and put

$$\delta = \min\left\{\left|\left\|\alpha n^2\right\|_{\mathbb{R}/\mathbb{Z}} - \rho\right| \;\middle|\; n \leq N\right\} > 0. \tag{4.6}$$

Suppose now that m is such that

$$\|2\alpha m\|_{\mathbb{R}/\mathbb{Z}} < \frac{\delta}{10N} \qquad \text{and} \qquad \left\|\alpha m^2\right\|_{\mathbb{R}/\mathbb{Z}} < \frac{\delta}{10}. \tag{4.7}$$

For $n \leq N$ we have

$$\begin{aligned}\left|\left\|\alpha(n+m)^2 - \left\|\alpha n^2\right\|_{\mathbb{R}/\mathbb{Z}}\right\|_{\mathbb{R}/\mathbb{Z}}\right| &\leq \left\|2\alpha mn + \alpha m^2\right\|_{\mathbb{R}/\mathbb{Z}} \\ &\leq N\|2\alpha m\|_{\mathbb{R}/\mathbb{Z}} + \left\|\alpha m^2\right\|_{\mathbb{R}/\mathbb{Z}} \leq \delta/5 < \delta,\end{aligned}$$

and consequently $g(n+m) = g(n)$. It follows that we may take $\varepsilon = \delta/10N$. □

Our next step is to express the property that $\|\alpha m\|_{\mathbb{R}/\mathbb{Z}}$ is small, with no restrictions on $\left\|\alpha m^2\right\|_{\mathbb{R}/\mathbb{Z}}$. This is easily achieved with the help of $\mu(m, N)$. Define

$$\lambda(m, N): \qquad (\exists\, n)\ \mu(n, N) \wedge \mu(n+m, N) \qquad (m, N \in \mathbb{N}). \tag{4.8}$$

Lemma 4.2. *For each $\varepsilon > 0$ there exists $N \in \mathbb{N}$ such that for all $m \in \mathbb{N}$, if $\lambda(m, N)$ holds, then $\|2\alpha m\|_{\mathbb{R}/\mathbb{Z}} < \varepsilon$. Conversely, for each $N \in \mathbb{N}$ there exists $\varepsilon > 0$ such that if $\|2\alpha m\|_{\mathbb{R}/\mathbb{Z}} < \varepsilon$, then $\lambda(m, N)$ holds.*

Proof. Let $\varepsilon > 0$ and pick N sufficiently large that $\mu(m, N)$ implies $\|2\alpha n\|_{\mathbb{R}/\mathbb{Z}} < \varepsilon/2$. Then $\lambda(m, N)$ implies $\|2\alpha m\|_{\mathbb{R}/\mathbb{Z}} < \varepsilon$, as needed.

Conversely, let N be an integer. Pick $\delta > 0$ sufficiently small that if for some n we have $\|2\alpha n\|_{\mathbb{R}/\mathbb{Z}} < \delta$ and $\left\|\alpha n^2\right\|_{\mathbb{R}/\mathbb{Z}} < \delta$, then $\lambda(n, N)$ holds. Let m be an integer such that $\|2\alpha m\|_{\mathbb{R}/\mathbb{Z}} < \delta/2$ and $m > 2/\delta$. By Weyl's equidistribution theorem, there exists n such that

$$\left\|\alpha n^2\right\|_{\mathbb{R}/\mathbb{Z}} < \frac{\delta}{2} \qquad \text{and} \qquad \left|\langle 2\alpha n\rangle + \left\langle \alpha m^2\right\rangle/m\right| < \frac{\delta}{2m}. \tag{4.9}$$

Then we have

$$\|2\alpha n\|_{\mathbb{R}/\mathbb{Z}} \leq \frac{1}{m} < \delta \qquad \text{and} \qquad \|2\alpha(n+m)\|_{\mathbb{R}/\mathbb{Z}} \leq \frac{1}{m} + \frac{\delta}{2} < \delta. \tag{4.10}$$

Of course, $\left\|\alpha n^2\right\|_{\mathbb{R}/\mathbb{Z}} < \delta$. It remains to estimate $\left\|\alpha(n+m)^2\right\|_{\mathbb{R}/\mathbb{Z}}$. We have

$$\left\|\alpha(n+m)^2\right\|_{\mathbb{R}/\mathbb{Z}} = \left\|\alpha n^2 + m\left(\langle 2\alpha n\rangle + \left\langle \alpha m^2\right\rangle/m\right)\right\|_{\mathbb{R}/\mathbb{Z}} < \frac{\delta}{2} + m\frac{\delta}{2m} = \delta.$$

Thus, we have $\mu(n, N)$ and $\mu(n+m, N)$, as needed. It follows that we can take any $\varepsilon > 0$ with $\varepsilon < \delta/2$ and $\varepsilon < \|\alpha n\|_{\mathbb{R}/\mathbb{Z}}$ for all $n \leq 2/\delta$. □

Next, we express the property that $\|\alpha n^2\|_{\mathbb{R}/\mathbb{Z}}$ is small, which turns out to require more effort. Towards this goal, we introduce the following property.

$$\begin{aligned}\kappa(m,N):\qquad &(\exists\ M)\ (\forall\ h)\ \ (g(h)=1)\wedge\lambda(h,M)\Rightarrow\\ &(\forall\ L)\ (\exists\ n)\ \lambda(n,L)\wedge\mu(n,N)\wedge(g(h+m+n)=1)\qquad (m,N\in\mathbb{N}).\end{aligned}$$

Lemma 4.3. *For each $\varepsilon>0$ there exists $N\in\mathbb{N}$ such that for all $m\in\mathbb{N}$, if $\kappa(m,N)$ holds, then $\|\alpha m^2\|_{\mathbb{R}/\mathbb{Z}}<\varepsilon$. Conversely, for each $N\in\mathbb{N}$ there exists $\varepsilon>0$ such that if $\|\alpha m^2\|_{\mathbb{R}/\mathbb{Z}}<\varepsilon$, then $\kappa(m,N)$ holds.*

Proof. Let $\varepsilon>0$, and let N be such that $\mu(n,N)$ implies $\|\alpha n^2\|_{\mathbb{R}/\mathbb{Z}}<\varepsilon/2$ (which exists by Lemma 4.1). Pick $m\in\mathbb{N}$ such that $\kappa(m,N)$ holds; we aim to show that $\|\alpha m^2\|_{\mathbb{R}/\mathbb{Z}}<\varepsilon$. For the sake of contradiction, suppose that $\langle\alpha m^2\rangle\geq\varepsilon$ (the case where $\langle\alpha m^2\rangle\leq-\varepsilon$ is analogous). Let M be any integer admissible for $\kappa(m,N)$, and let h be an integer such that

$$\langle\alpha h^2\rangle\in\left(\rho-\frac{\varepsilon}{8},\rho\right),\qquad \langle 2\alpha h\rangle\in\left(0,\frac{\varepsilon}{8m}\right)\qquad \lambda(n,M),\tag{4.11}$$

which exists by Weyl's equidistribution theorem. (Note that the second and the third condition in (4.11) can be satisfied by taking h such that $\langle\alpha h\rangle$ is sufficiently small and positive.) Bearing in mind Lemma 4.2, we infer from $\kappa(m,N)$ that there exists a sequence of integers $(n_i)_{i=1}^{\infty}$ such that

$$\lim_{i\to\infty}\|\alpha n_i\|_{\mathbb{R}/\mathbb{Z}}=0,\tag{4.12}$$

$$\|\alpha n_i^2\|_{\mathbb{R}/\mathbb{Z}}<\varepsilon/2\qquad\text{for all } i\in\mathbb{N},\tag{4.13}$$

$$\|\alpha(h+m+n_i)^2\|_{\mathbb{R}/\mathbb{Z}}<\rho\qquad\text{for all } i\in\mathbb{N}.\tag{4.14}$$

Passing to a subsequence, we may assume that $\langle\alpha n_i^2\rangle$ converges to some limit $\beta\in[-\varepsilon/2,\varepsilon/2]$ as $i\to\infty$. Letting $i\to\infty$ in (4.14) we arrive at a contradiction:

$$\begin{aligned}\rho&\geq\lim_{i\to\infty}\|\alpha(h+m+n_i)^2\|_{\mathbb{R}/\mathbb{Z}}=\|\alpha(h+m)^2+\beta\|_{\mathbb{R}/\mathbb{Z}}\\ &=\|\alpha h^2+\langle 2\alpha h\rangle m+\alpha m^2+\beta\|_{\mathbb{R}/\mathbb{Z}}\geq\rho-\frac{\varepsilon}{8}-m\frac{\varepsilon}{8m}+\varepsilon-\frac{\varepsilon}{2}=\rho+\frac{\varepsilon}{8}.\end{aligned}$$

We now proceed to the proof of the converse implication. Let N be an integer and let $\varepsilon>0$ be sufficiently small that $\|\alpha n^2\|_{\mathbb{R}/\mathbb{Z}}<2\varepsilon$ and $\|2\alpha n\|_{\mathbb{R}/\mathbb{Z}}<2\varepsilon$ imply $\mu(n,N)$. Pick M sufficiently large that $\lambda(h,M)$ implies that $\|2\alpha h\|_{\mathbb{R}/\mathbb{Z}}<\varepsilon/m$, and let h satisfy $g(h)=1$ and $\lambda(h,M)$ (and hence in particular $\|2\alpha h\|_{\mathbb{R}/\mathbb{Z}}<\varepsilon/m$). We need to show that there exists a sequence of integers $(n_i)_{i=1}^{\infty}$ such that

$$\lim_{i\to\infty}\|\alpha n_i\|_{\mathbb{R}/\mathbb{Z}}=0,\tag{4.15}$$

$$\mu(n_i,N)\text{ is true}\qquad\text{for all sufficiently large } i\in\mathbb{N},\tag{4.16}$$

$$\|\alpha(h+m+n_i)^2\|_{\mathbb{R}/\mathbb{Z}}<\rho\qquad\text{for all sufficiently large } i\in\mathbb{N}.\tag{4.17}$$

(Note that in (4.16) and (4.17) it is enough to consider sufficiently large i since we can always pass to a subsequence and achieve the same condition for all i.) By Weyl's equidistribution

theorem, we can find a sequence $(n_i)_{i=1}^{\infty}$ such that

$$\lim_{i\to\infty} \langle \alpha n_i \rangle = 0, \tag{4.18}$$

$$\lim_{i\to\infty} \left\langle \alpha n_i^2 \right\rangle = -\left\langle 2\alpha h m + \alpha m^2 \right\rangle. \tag{4.19}$$

By (4.19) can estimate

$$\lim_{i\to\infty} \left\| \alpha n_i^2 \right\|_{\mathbb{R}/\mathbb{Z}} < \frac{\varepsilon}{m} m + \varepsilon = 2\varepsilon,$$

and hence (4.16) follows. It remains to deal with (4.17). We can compute

$$\lim_{i\to\infty} \left\| \alpha(h+m+n_i)^2 \right\|_{\mathbb{R}/\mathbb{Z}} = \left\| \alpha(h+m)^2 + \lim_{i\to\infty} \left\langle \alpha n_i^2 \right\rangle \right\|_{\mathbb{R}/\mathbb{Z}} = \left\| \alpha h^2 \right\|_{\mathbb{R}/\mathbb{Z}} < \rho,$$

as needed. □

The next property that we would like to express is that αn^2 and αm^2 are close modulo 1. With this goal in mind, we define

$$\begin{aligned} \nu(m,\tilde{m},N): \qquad & (\exists\ L)\ (\forall\ n)\ \lambda(n,L) \wedge \kappa(m+n,L) \Rightarrow \\ & \kappa(\tilde{m}+n,N) \qquad\qquad (m,\tilde{m},N \in \mathbb{N}). \end{aligned}$$

Lemma 4.4. *For each $\varepsilon > 0$ there exists $N \in \mathbb{N}$ such that for all $m, \tilde{m} \in \mathbb{N}$, if $\nu(m,\tilde{m},N)$ holds, then $\left\| \alpha(m^2 - \tilde{m}^2) \right\|_{\mathbb{R}/\mathbb{Z}} < \varepsilon$. Conversely, for each $N \in \mathbb{N}$ there exists $\varepsilon > 0$ such that if $\left\| \alpha(m^2 - \tilde{m}^2) \right\|_{\mathbb{R}/\mathbb{Z}} < \varepsilon$, then $\nu(m,\tilde{m},N)$ holds.*

Proof. By Lemma 4.2, condition $\nu(m,\tilde{m},N)$ is equivalent to the statement that for each sequence $(n_i)_{i=1}^{\infty}$ such that $\|\alpha n_i\|_{\mathbb{R}/\mathbb{Z}} \to 0$ and $\left\| \alpha(m+n_i)^2 \right\|_{\mathbb{R}/\mathbb{Z}} \to 0$ as $i \to \infty$ we have $\kappa(\tilde{m}+n_i,N)$ for all sufficiently large i. Consider any sequence $(n_i)_{i=1}^{\infty}$ such that $\|\alpha n_i\|_{\mathbb{R}/\mathbb{Z}} \to 0$. Then

$$\begin{aligned} \left\langle \alpha(m+n_i)^2 - \alpha m^2 - \alpha n_i^2 \right\rangle &\to 0 \qquad \text{as } i \to \infty, \\ \left\langle \alpha(\tilde{m}+n_i)^2 - \alpha \tilde{m}^2 - \alpha n_i^2 \right\rangle &\to 0 \qquad \text{as } i \to \infty. \end{aligned}$$

Thus, if $\varepsilon > 0$ and N is sufficiently large that $\kappa(m,N)$ implies $\left\| \alpha m^2 \right\|_{\mathbb{R}/\mathbb{Z}} < \varepsilon/3$, then (taking any sequence $(n_i)_{i=1}^{\infty}$ as above) $\nu(m,\tilde{m},N)$ implies

$$\begin{aligned} \left\| \alpha(m^2 - \tilde{m}^2) \right\|_{\mathbb{R}/\mathbb{Z}} \le \lim_{i\to\infty} & \left\| \alpha(m+n_i)^2 - \alpha m^2 - \alpha n_i^2 \right\|_{\mathbb{R}/\mathbb{Z}} \\ & + \left\| \alpha(\tilde{m}+n_i)^2 - \alpha \tilde{m}^2 - \alpha n_i^2 \right\|_{\mathbb{R}/\mathbb{Z}} \\ & + \left\| \alpha(m+n_i)^2 \right\|_{\mathbb{R}/\mathbb{Z}} + \left\| \alpha(\tilde{m}+h_i)^2 \right\|_{\mathbb{R}/\mathbb{Z}} \le \varepsilon/3. \end{aligned}$$

Conversely, if $N \in \mathbb{N}$ and $\varepsilon > 0$ is sufficiently small that $\left\| \alpha m^2 \right\|_{\mathbb{R}/\mathbb{Z}} < 3\varepsilon$ implies $\kappa(m,N)$, then for any $m, \tilde{m}$ with $\left\| \alpha(m^2 - \tilde{m}^2) \right\|_{\mathbb{R}/\mathbb{Z}} < \varepsilon$ and any sequence $(n_i)_{i=1}^{\infty}$ as above we have

$$\begin{aligned} \left\| \alpha(\tilde{m}+n_i)^2 \right\|_{\mathbb{R}/\mathbb{Z}} \le \lim_{i\to\infty} & \left\| \alpha(m+n_i)^2 - \alpha m^2 - \alpha n_i^2 \right\|_{\mathbb{R}/\mathbb{Z}} \\ & + \left\| \alpha(\tilde{m}+n_i)^2 - \alpha \tilde{m}^2 - \alpha n_i^2 \right\|_{\mathbb{R}/\mathbb{Z}} \\ & + \left\| \alpha(m+n_i)^2 \right\|_{\mathbb{R}/\mathbb{Z}} + \left\| \alpha(m^2 - \tilde{m}^2) \right\|_{\mathbb{R}/\mathbb{Z}} \le \varepsilon, \end{aligned}$$

and hence $\kappa(\tilde{m},N)$ holds. □

4.3. **Divisibility.** Finally, we are able to define divisibility. Consider the relation

$$\delta(m,\tilde{m}): \quad (\forall\ N)\ (\exists\ L)\ (\forall\ n)\ \nu(m+n,m,L)\wedge\kappa(n,L)\Rightarrow \nu(\tilde{m}+n,\tilde{m},N) \qquad (m,\tilde{m}\in\mathbb{N}).$$

Lemma 4.5. *For each $m,\tilde{m}\in\mathbb{N}$ we have $\delta(m,\tilde{m})$ if and only if $m\mid\tilde{m}$.*

Proof. Condition $\delta(m,\tilde{m})$ is equivalent to the statement that for each $\varepsilon>0$, for each sequence $(n_i)_{i=1}^{\infty}$, if $\left\|\alpha((m+n_i)^2-m^2)\right\|_{\mathbb{R}/\mathbb{Z}}\to 0$ and $\left\|\alpha n_i^2\right\|_{\mathbb{R}/\mathbb{Z}}\to 0$ as $i\to\infty$, then $\left\|\alpha((\tilde{m}+n_i)^2-\tilde{m}^2)\right\|_{\mathbb{R}/\mathbb{Z}}\leq\varepsilon$ for all sufficiently large i. Note that the condition that $\left\|\alpha((m+n_i)^2-m^2)\right\|_{\mathbb{R}/\mathbb{Z}}\to 0$ and $\left\|\alpha n_i^2\right\|_{\mathbb{R}/\mathbb{Z}}\to 0$ is equivalent to $\|2\alpha mn_i\|_{\mathbb{R}/\mathbb{Z}}\to 0$ and $\left\|\alpha n_i^2\right\|_{\mathbb{R}/\mathbb{Z}}\to 0$ as $i\to\infty$. If $\tilde{m}=km$ is a multiple of m, then for any sequence $(n_i)_{i=1}^{\infty}$ like above we have $\|2\alpha\tilde{m}n_i\|_{\mathbb{R}/\mathbb{Z}}\leq k\,\|2\alpha mn_i\|_{\mathbb{R}/\mathbb{Z}}\to 0$ as $i\to\infty$. Conversely, if $\tilde{m}/m=a/b$ with $\gcd(a,b)=1$, then we can find a sequence $(n_i)_{i=1}^{\infty}$ with $\|2\alpha mn_i\|_{\mathbb{R}/\mathbb{Z}}\to 0$, $\left\|\alpha n_i^2\right\|_{\mathbb{R}/\mathbb{Z}}\to 0$, and $\|2\alpha\tilde{m}n_i\|_{\mathbb{R}/\mathbb{Z}}\to 1/b$ as $i\to\infty$. □

Lemma 4.5 implies that divisibility is definable in the first-order theory under consideration. It is a classical [Rob49] result that multiplication can be defined in $(\mathbb{Z};<,+,|)$, meaning in particular that the corresponding first-order theory is undecidable. This completes the proof of Theorem B.

References

[AK23] Boris Adamczewski and Jakub Konieczny. Bracket words: a generalisation of Sturmian words arising from generalised polynomials. *Trans. Amer. Math. Soc.*, 376(7):4979–5044, 2023.

[AS03] Jean-Paul Allouche and Jeffrey Shallit. *Automatic sequences*. Cambridge University Press, Cambridge, 2003. Theory, applications, generalizations. doi:10.1017/CBO9780511546563.

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

[BHMV94a] Véronique Bruyère, Georges Hansel, Christian Michaux, and Roger Villemaire. Correction to: "Logic and p-recognizable sets of integers". *Bull. Belg. Math. Soc. Simon Stevin*, 1(4):577, 1994.

[BHMV94b] Véronique Bruyère, Georges Hansel, Christian Michaux, and Roger Villemaire. Logic and p-recognizable sets of integers. volume 1, pages 191–238. 1994. Journées Montoises (Mons, 1992). URL: http://projecteuclid.org/euclid.bbms/1103408547.

[BK] Jakub Byszewski and Jakub Konieczny. Pisot numbers, Salem numbers, and generalised polynomials. Preprint, arXiv: 2302.06242 [math.NT].

[BK18] Jakub Byszewski and Jakub Konieczny. Sparse generalised polynomials. *Trans. Amer. Math. Soc.*, 370(11):8081–8109, 2018.

[BL07] Vitaly Bergelson and Alexander Leibman. Distribution of values of bounded generalized polynomials. *Acta Math.*, 198(2):155–230, 2007. doi:10.1007/s11511-007-0015-y.

[Bos94] Michael D. Boshernitzan. Uniform distribution and Hardy fields. *J. Anal. Math.*, 62:225–240, 1994. doi:10.1007/BF02835955.

[BS19] Aseem R. Baranwal and Jeffrey Shallit. Critical exponent of infinite balanced words via the Pell number system. In *Combinatorics on words*, volume 11682 of *Lecture Notes in Comput. Sci.*, pages 80–92. Springer, Cham, 2019. doi:10.1007/978-3-030-28796-2.

[Büc62] J. Richard Büchi. On a decision method in restricted second order arithmetic. In *Logic, Methodology and Philosophy of Science (Proc. 1960 Internat. Congr.)*, pages 1–11. Stanford Univ. Press, Stanford, CA, 1962.

[CP86] Gregory Cherlin and Françoise Point. On extensions of Presburger arithmetic. In *Proceedings of the fourth Easter conference on model theory (Gross Köris, 1986)*, volume 86 of *Seminarberichte*, pages 17–34. Humboldt Univ., Berlin, 1986.

[DMR+17] Chen Fei Du, Hamoon Mousavi, Eric Rowland, Luke Schaeffer, and Jeffrey Shallit. Decision algorithms for Fibonacci-automatic words, II: Related sequences and avoidability. *Theoret. Comput. Sci.*, 657(part B):146–162, 2017. doi:10.1016/j.tcs.2016.10.005.

[DMSS16] Chen Fei Du, Hamoon Mousavi, Luke Schaeffer, and Jeffrey Shallit. Decision algorithms for Fibonacci-automatic words, III: Enumeration and abelian properties. *Internat. J. Found. Comput. Sci.*, 27(8):943–963, 2016. doi:10.1142/S0129054116500386.

[Fra09] Nikos Frantzikinakis. Equidistribution of sparse sequences on nilmanifolds. *J. Anal. Math.*, 109:353–395, 2009. doi:10.1007/s11854-009-0035-y.

[GT12] Ben Green and Terence Tao. The quantitative behaviour of polynomial orbits on nilmanifolds. *Ann. of Math. (2)*, 175(2):465–540, 2012. doi:10.4007/annals.2012.175.2.2.

[HMO+22] Philipp Hieronymi, Dun Ma, Reed Oei, Luke Schaeffer, Christian Schulz, and Jeffrey Shallit. Decidability for Sturmian words. In *30th EACSL Annual Conference on Computer Science Logic*, volume 216 of *LIPIcs. Leibniz Int. Proc. Inform.*, pages Art. No. 24, 23. Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, 2022.

[HS22] Philipp Hieronymi and Christian Schulz. A strong version of Cobham's theorem. In *STOC '22—Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*, pages 1172–1179. ACM, New York, [2022] ©2022.

[HT18] Philipp Hieronymi and Alonza Terry, Jr. Ostrowski numeration systems, addition, and finite automata. *Notre Dame J. Form. Log.*, 59(2):215–232, 2018. doi:10.1215/00294527-2017-0027.

[Kor01] Ivan Korec. A list of arithmetical structures complete with respect to the first-order definability. volume 257, pages 115–151. 2001. Weak arithmetics. doi:10.1016/S0304-3975(00)00113-4.

[Lei12] A. Leibman. A canonical form and the distribution of values of generalized polynomials. *Israel J. Math.*, 188:131–176, 2012. doi:10.1007/s11856-011-0097-2.

[Mat93] Yuri V. Matiyasevich. *Hilbert's tenth problem*. Foundations of Computing Series. MIT Press, Cambridge, MA, 1993. Translated from the 1993 Russian original by the author, With a foreword by Martin Davis.

[MSS16] Hamoon Mousavi, Luke Schaeffer, and Jeffrey Shallit. Decision algorithms for Fibonacci-automatic words, I: Basic results. *RAIRO Theor. Inform. Appl.*, 50(1):39–66, 2016. doi:10.1051/ita/2016010.

[Nea11] Victoria Ruth Neale. *Bracket quadratics as asymptotic bases for the natural numbers*. PhD thesis, Trinity College, University of Cambridge, 2011.

[Rob49] Julia Robinson. Definability and decision problems in arithmetic. *J. Symbolic Logic*, 14:98–114, 1949. doi:10.2307/2266510.

[Sch23] Christian Schulz. Undefinability of multiplication in Presburger arithmetic with sets of powers. *The Journal of Symbolic Logic*, page 1–24, 2023. doi:10.1017/jsl.2023.71.

[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. URL: https://dx.doi.org/10.1070/IM1980v015n02ABEH001252, doi:10.1070/IM1980v015n02ABEH001252.

[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. URL: https://dx.doi.org/10.1070/IM1984v022n03ABEH001456, doi:10.1070/IM1984v022n03ABEH001456.