A diophantine undecidable subsystem of arithmetic with no induction axioms

Richard Kaye
School of Mathematics and Statistics
The University of Birmingham
Edgbaston
Birmingham B15 2TT
U.K.

email: R.W.Kaye@bham.ac.uk
www: http://for.mat.bham.ac.uk/R.W.Kaye

1st July, 1996.

1 Introduction

Let T be a theory in the usual first-order language of arithmetic $\mathcal{L}_{\mathrm{A}}$ (with nonlogical symbols $0, 1, +, \cdot, <$) extending PA^-, the theory of the nonnegative parts of discretely ordered rings. The set of *universal consequences* of T is denoted $\forall_1$-$\mathrm{Th}(T)$.

Definition 1. An $\mathcal{L}_{\mathrm{A}}$-theory T is *diophantine undecidable* if there is no algorithm which, on input a polynomial in several variables $p(\bar{x}) \in \mathbb{Z}[\bar{x}]$, determines whether or not T has a model in which the equation $p(\bar{x}) = 0$ has a solution.

For theories T extending PA^- (as are all the theories considered here), T is diophantine undecidable iff the set $\forall_1$-$\mathrm{Th}(T)$ of universal consequences of T is recursive. In the case of $T = \mathrm{Th}(\mathbb{N})$, the complete theory of the standard model $\mathbb{N}$, the question whether T is diophantine undecidable is precisely Hilbert's 10th problem, and this was solved by the famous Matiyasevich–Robinson–Davis–Putnam (MRDP) theorem of 1970. Slightly more generally, we say that a theory T *proves the MRDP theorem* ($T \vdash \mathrm{MRDP}$) if for all $\theta(\bar{x}) \in \Sigma_1$ there is $\psi(\bar{x})$ in $\exists_1$ with the same free-variables such that $T \vdash \forall \bar{x}\,(\theta(\bar{x}) \leftrightarrow \psi(\bar{x}))$. Then $\mathrm{Th}(\mathbb{N}) \vdash \mathrm{MRDP}$, and in fact any $\mathcal{L}_{\mathrm{A}}$-theory extending PA^- which proves the MRDP theorem is diophantine undecidable. This is for example true of the theory $I\Delta_0 + \exp$ [1].

On the other hand, for very weak theories we have almost no information. In particular, the question whether or not the theory IOpen (axiomatized by PA^- together with the usual axiom scheme of induction for quantifier-free $\mathcal{L}_{\mathrm{A}}$-formulas) is diophantine undecidable is an old question studied even before the MRDP theorem was completed, and is still open. In fact it is not even known if the weakest possible theory in this context—PA^- itself—is diophantine decidable. In other words, it is not known whether or not there is an algorithm to determine if the ring $\mathbb{Z}[\bar{x}]/(p(\bar{x}))$ can be discretely ordered with each $x_i \geqslant 0$.

Another theory that has been considered in this context is IE_1—the theory of *bounded existential induction*. This theory has been shown to be diophantine undecidable [3], even though it is not known if IE_1 proves the MRDP theorem. However, this result was proved by making use of the remarkably strong induction axioms in IE_1 and the basic method of proving the MRDP theorem: the main step here [2] was to show that IE_1 together with an axiom for exponentiation is actually equivalent to the theory $I\Delta_1 + \exp$ of Dimitracopoulos and Gaifman.

With such a gap between 'strong theories' such as $I\Delta_0 + \exp$ known to prove the MRDP theorem, and IE_1 where much of the proof of the MRDP theorem can be carried out given closure under functions of fast enough growth, and 'weak theories' such as IOpen and PA^- which are definitely known not to prove the MRDP theorem, it would seem worthwhile to try to find much weaker theories T which are diophantine undecidable.

The object here is to demonstrate a rather general method of doing just this in the particular case of a finitely axiomatized $\mathcal{L}_{\mathrm{A}}$-theory T extending PA^- whose axioms all have a natural 'algebraic' character concerning exponentiation, primes, and binomal coefficients. The method provides a certain weak induction principle 'for free', and the theory discussed here has been chosen to illustrate this method, and in particular how this induction principle can be profitably used together with the axioms of T. It seems likely that the proof here could be modified to give much more interesting results, perhaps showing much weaker or more natural theories are diophantine undecidable. To do so would seem to require (just as one would expect) other elegant and powerful methods for representing recursive relations and functions (such as exponentiation, binomial coefficients, primality) in a diophantine way.

There seems to me no *obvious* reason to me why this this should not be possible by the method I am proposing for even the very weakest of theories we might like to consider (such as IOpen, or even PA^-), but of course the practical difficulties of finding such elegant diophantine representations are still very great. Against this opinion there is some evidence from much interesting work, by Wilkie and van den Dries especially [7, 5, 6], who have concentrated their efforts on providing decision methods for the solubility of certain diophantine equations. However, despite some remarkable results (in particular van den Dries's decision method for solubility of diophantine equations in two variables in models of IOpen) the evidence is not particularly compelling in either direction, and the original question on the diophantine undecidability of IOpen is still wide open.

2 The method

A general method for giving a negative answer to the diophantine problem for a given $\mathcal{L}_{\mathrm{A}}$-theory T has been given and discussed elsewhere [3, 4]. Here, I state the main definition and theorem and refer the reader to other papers for further details. Here and throughout, given a tuple of terms, $\bar{t}$, in some language $\mathcal{L}$, $u < \bar{t} < v$ is an abbreviation for the conjuction of all $u < t_i \wedge t_i < v$. Similarly for $\bar{t} < v$, $u < \bar{t}$ and for $\leqslant$ in place of $<$.

Definition 2. An $\mathcal{L}_{\mathrm{A}}$-theory T extending PA^- is *diophantine sufficient* if for all polynomials $p(\bar{x}) \in \mathbb{Z}[\bar{x}]$ there are $\exists_1$ formulas $\psi(\bar{x}, y, \bar{z})$ and $\theta(y, \bar{z})$ in the free-variables shown such that

1. $\mathbb{N} \models \forall y\, (\forall \bar{x}{<}y\, p(\bar{x}) \neq 0 \to \exists \bar{z}\, \theta(y, \bar{z}))$
2. $T \vdash \forall y{>}0\, \forall \bar{z}\, (\theta(y, \bar{z}) \to \psi(0, \ldots, 0, y, \bar{z}))$
3. $T \vdash \forall \bar{u}, \bar{v}, y, \bar{z}\, (\theta(y, \bar{z}) \wedge \bar{u}, \bar{v} < y \wedge n < y \wedge \psi(\bar{u}, 0, \bar{v}, y, \bar{z}) \to \psi(\bar{u}, n, \bar{v}, y, \bar{z}))$, for all $n \in \mathbb{N}$ and all $i = \mathrm{len}(\bar{u}) < m$
4. $T \vdash \forall \bar{x}, y, \bar{z}\, (\theta(y, \bar{z}) \wedge \bar{x} < y \wedge \psi(\bar{x}, y, \bar{z}) \to p(\bar{x}) \neq 0)$

The main theorem concerning this notion is as follows.

Theorem 3. *Let T be a consistent diophantine sufficient $\mathcal{L}_{\mathrm{A}}$-theory extending PA^-. Then T is diophantine undecidable.*

The original proof of this theorem was model-theoretic. Assuming T to be diophantine decidable, it is possible to construct a recursive e.c. model of T. Then a variation of Tennenbaum's theorem gives the theorem [3]. An alternative method is to use the diophantine sufficiency to show every recursive function is strongly represented in T by an $\exists_1$-formula. Then a variation of the diagonalization lemma gives the result [4].

Definition 2 should be thought of as a special kind of induction rule which can be added to a given theory T, with the result that if T with this rule can prove a small part of the MRDP theorem then T is diophantine undecidable. Notice that '$\exists_1$' here is for convenience only: if the hypotheses hold for certain $\exists_1$ formulas θ, ψ then by introducing new variables $\bar{z}$ if necessary, suitable *quantifier-free* formulas θ, ψ may be found.

It will be more convenient to use a variation of the basic idea of 'diophantine sufficient', which shows that in effect we can ignore finitely many natural numbers $0, 1, 2, \ldots, N-1$ in the definition.

Theorem 4. *Let T be an $\mathcal{L}_{\mathrm{A}}$-theory extending PA^- such that for some $N \in \mathbb{N}$ the following holds: for all polynomials $p(\bar{x}) \in \mathbb{Z}[\bar{x}]$ there are $\exists_1$ formulas $\psi(\bar{x}, y, \bar{z})$ and $\theta(y, \bar{z})$ in the free-variables shown such that*

1. $\mathbb{N} \models \forall y{>}N\, (\forall \bar{x}{<}y\, (p(\bar{x}) \neq 0) \to \exists \bar{z}\, \theta(y, \bar{z}))$
2. $T \vdash \forall y{>}N\, \forall \bar{z}\, (\theta(y, \bar{z}) \to \psi(N, \ldots, N, y, \bar{z}))$
3. $T \vdash \forall \bar{u}, \bar{v}, y, \bar{z}\, (\theta(y, \bar{z}) \wedge N \leqslant \bar{u}, n, \bar{v} < y \wedge \psi(\bar{u}, N, \bar{v}, y, \bar{z}) \to \psi(\bar{u}, n, \bar{v}, y, \bar{z}))$, *for all $n \in \mathbb{N}$ with $n \geqslant N$ and all $i = \mathrm{len}(\bar{u}) < m$*
4. $T \vdash \forall \bar{x}, y, \bar{z}\, (\theta(y, \bar{z}) \wedge N \leqslant \bar{x} < y \wedge \psi(\bar{x}, y, \bar{z}) \to p(\bar{x}) \neq 0)$.

Then T is diophantine sufficient.

Proof. Suppose T has the properties given. We need to show that for all polynomials $p(\bar{x})$ there are ψ and θ as in the original definition of diophantine sufficient. We argue by induction on the number of variables in $\bar{x}$; with no variables at all, p is a constant and the theorem is a triviality.

Let $p(x_0, \bar{x})$ be given, and write $p_i(\bar{x}) = p(i, \bar{x})$ for each $i < N$. By induction there are $\theta_i(y, \bar{z}_i)$ and $\psi_i(\bar{x}, y, \bar{z}_i)$ satisfying conditions 1–4 in Definition 2 for the polynomial $p_i(\bar{x})$. Take also $\theta_N(y, \bar{z}_N)$ and $\psi_N(x_0, \bar{x}, y, \bar{z}_N)$ for the polynomial $p(x_0, \bar{x})$ as in the statement of the theorem. Then the formulas $\theta(y, \bar{z}_0, \ldots, \bar{z}_N) =$

$$\bigwedge_{i \leqslant N} \theta_i(y, \bar{z}_i) \wedge \bigwedge_{\bar{u} < N} p(\bar{u}) \neq 0$$

and $\psi(x_0, \bar{x}, y, \bar{z}_0, \ldots, \bar{z}_N) =$

$$\bigwedge_{i<N} (x_0 = i \rightarrow \psi_i(\bar{x}, y, \bar{z}_i)) \wedge (x_0 \geqslant N \rightarrow \psi_N(x_0, \bar{x}, y, \bar{z}_n))$$

satisfy the required conditions 1–4 in Definition 2. □

3 Adding new function and predicate symbols

Since the method presented above for showing T to be diophantine undecidable is language dependent, but the main techniques used to prove the MRDP theorem (at least in the weaker form that every r.e. predicate is exponential-diophantine) use other functions and relations—notably binomial coefficients and factorials—it is convenient to be able to expand our language $\mathcal{L}_{\mathrm{A}}$. To reconcile these two requirements we resort to a technical device, to be explained in this section.

In this paper we regard all new function and predicate symbols as convenient abbreviations for $\mathcal{L}_{\mathrm{A}}$-formulas, so the language is 'not really' expanded at all, except in our informal notation. Moreover, we will need to be able to compute the quantifier complexity of formulas, so we insist that *all new function symbols represent recursive functions, and all new predicate letters represent r.e. relations.* Since it will be important that the formulas are $\exists_1$, we stipulate: *When we introduce a new predicate letter $P(x_1, \ldots, x_n)$ we fix an $\exists_1$ $\mathcal{L}_{\mathrm{A}}$-formula $\delta_P(x_1, \ldots, x_n)$ such that, $\delta_P(x_1, \ldots, x_n)$ represents the intended meaning of P in the standard model $\mathbb{N}$.* (Such δ_P exists by the MRDP theorem in $\mathbb{N}$.) Then $P(x_1, \ldots, x_n)$ is from now on just an abbreviation for $\delta_P(x_1, \ldots, x_n)$. Similarly, *when we introduce a new function symbol $F(x_1, \ldots, x_n)$ we fix an $\exists_1$ $\mathcal{L}_{\mathrm{A}}$-formula $\delta_F(x_1, \ldots, x_n, y)$ such that $\delta_P(x_1, \ldots, x_n, y)$ represents the graph of the function intended by F in the standard model $\mathbb{N}$, and we also add an axiom expressing the functionality of F*, i.e.,

$$\forall x_1, \ldots, x_n, y, y' \, (\delta_P(x_1, \ldots, x_n, y) \wedge \delta_P(x_1, \ldots, x_n, y') \rightarrow y = y').$$

(It turns out that we do not need any axiom stating that the function F is everywhere-defined.) Then any $\exists_1$ formula $\theta(\ldots, F(x_1, \ldots, x_n), \ldots)$ can be regarded as an abbreviation for

$$\exists y \, (\delta_P(x_1, \ldots, x_n, y) \wedge \theta(\ldots, y, \ldots))$$

at no extra cost in terms of complexity. Of course, we may also write down other axioms involving the new symbols, and these are again regarded as abbreviations.

For example, we may introduce the factorial function $x!$ via some polynomial $p_{\mathrm{fact}}(x, y, \bar{z})$ such that

$$\mathbb{N} \vDash m! = n \leftrightarrow \exists \bar{z} \, p_{\mathrm{fact}}(m, n, \bar{z}) = 0$$

for all $n, m \in \mathbb{N}$. Then we have axioms for functionality of this definition

$$\forall x, y, y', \bar{z}, \bar{z}' \, (p_{\text{fact}}(x, y, \bar{z}) = 0 \land p_{\text{fact}}(x, y', \bar{z}') = 0 \to y = y')$$

and to this we may add axioms for the recursive definition of factorial

$$\exists \bar{z} \, (p_{\text{fact}}(0, 1, \bar{z}) = 0)$$

and

$$\forall x, y, \bar{z} \, (p_{\text{fact}}(x, y, \bar{z}) = 0 \to \exists \bar{z}' \, p_{\text{fact}}(x + 1, y(x + 1), \bar{z}') = 0).$$

(This first of these, expressing $0! = 1$, is actually provable in PA^- since it is $\exists_1$ and true.) Also (and rather importantly) we can add an axiom for a sort of 'downwards' recursive definition,

$$\forall x, y, \bar{z} \, (p_{\text{fact}}(x, y, \bar{z}) = 0 \land x > 0 \to \exists \bar{z}', w \, (wx = y \land p_{\text{fact}}(x - 1, w, \bar{z}') = 0)).$$

It is useful to realise that the precise $\mathcal{L}_{\mathrm{A}}$-sentences given by such axioms depends of the choice of $\exists_1$ formulas representing the new predicate and function symbols, and the same axiom may give inequivalent sentences for different choices of these $\exists_1$ formulas. So when we write down the axioms of a theory T in an expanded language, we are really defining a family of theories—one for each choice of representing $\mathcal{L}_{\mathrm{A}}$-formulas. None of the results here depend on what these $\exists_1$ formulas are (except of course that they must represent the intended function or relation in the standard model $\mathbb{N}$), so our results hold for all such theories T in this family.

4 Removing a bounded universal quantifier

The method presented in Theorem 3 involves finding an existential formula $\theta(y, \bar{z})$ which is formally equivalent to $\forall \bar{x} {<} y \, p(\bar{x}) \neq 0$ in some weak sense. The MRDP theorem presents a general method for finding such a formula θ; what is required to be able to apply Theorem 3 is to find a suitable formula θ for which the implication

$$\forall y, \bar{z} \, (\forall \bar{x} {<} y \, p(\bar{x}) \neq 0 \to \theta(y, \bar{z})) \tag{1}$$

is true in $\mathbb{N}$ and the implication

$$\forall y, \bar{z} \, (\theta(y, \bar{z}) \to \forall \bar{x} {<} y \, p(\bar{x}) \neq 0) \tag{2}$$

is provable from T together with a kind of extra induction rule. What we require here is a formula θ, which is as 'strong as possible', expressing properties of certain numbers in $\mathbb{N}$ not necessarily true in models of T, and hence making the proof of (2) as 'easy' as possible.

The disadvantage with Definition 2 as an induction rule is that it may only be used once. This causes problems—especially when you consider that all the variables x_i in $\forall \bar{x} {<} y$ have to be considered at the same time, and for this the use of pairing functions is somewhat inconvenient. To my knowledge, all published proofs of the MRDP theorem in weak systems [1, 2] have used the Chinese remainder theorem and a separate induction to treat each variable x_i. This is obviously out of the question in this setting. I am grateful for conversations on this point with Yuri Matiyasevich, who suggested several alternative methods of reducing $\forall \bar{x}<y\, p(\bar{x}) \neq 0$ to an exponential diophantine form in a uniform way, treating all the variables $\bar{x}$ together. One of his ideas is used here, and in the present section I will present it as I learnt it from him—i.e., for the standard model $\mathbb{N}$. Subsequent sections are devoted to applying Matiyasevich's method and Theorem 3 to certain weak systems of arithmetic T.

Firstly, note that we may assume without loss of generality that the polynomial $p(\bar{x})$ in question only takes nonnegative values, since if necessary we may replace it with its square, $p(\bar{x})^2$. The idea now is to consider the values

$$T_p(\alpha, q) = \sum_{x_1<\alpha} \cdots \sum_{x_m<\alpha} p(\bar{x}) q^{x_1+x_2\alpha+\cdots+x_m\alpha^{m-1}} \tag{3}$$

for some large prime q. Provided q is large enough, the values $p(\bar{x})$ for $\bar{x} < \alpha$ can be recovered from $T_p(\alpha, q)$ and checked to see if any is zero. Suppose $p(\bar{x})$ is given as

$$p(\bar{x}) = \sum_{i_1,\ldots,i_m} c_{i_1,\ldots,i_m} x^{i_1} \cdots x^{i_m}$$

with the $c_{i_1,\ldots,i_m}$s in $\mathbb{Z}$. Then (3) can be rearranged as follows:

$$\begin{aligned}
T_p(\alpha, q) &= \sum_{x_1<\alpha} \cdots \sum_{x_m<\alpha} p(\bar{x}) q^{x_1} q^{x_2\alpha} \cdots q^{x_m\alpha^{m-1}} \\
&= \sum_{x_1<\alpha} \cdots \sum_{x_m<\alpha} \sum_{i_1,\ldots,i_m} c_{i_1,\ldots,i_m} x^{i_1} \cdots x^{i_m} q^{x_1} q^{x_2\alpha} \cdots q^{x_m\alpha^{m-1}} \\
&= \sum_{i_1,\ldots,i_m} c_{i_1,\ldots,i_m} \left(\sum_{x_1<\alpha} x_1^{i_1} q^{x_1} \right) \cdots \left(\sum_{x_m<\alpha} x_m^{i_m} q^{x_m\alpha^{m-1}} \right).
\end{aligned}$$

Each individual term $\sum_{x_j<\alpha} x_j^k q^{x_j\alpha^{j-1}}$ here is a 'generalized geometric series' and can be represented as a term in the language $\mathcal{L}_{\mathrm{A}}$ together with exponentiation. Thus there is such an exponential term $T(\alpha, q)$ for $T_p(\alpha, q)$. Similarly, with the constant polynomial 1 in place of p, we can find an exponential term $S(\alpha, q)$ for

$$T_1(\alpha, q) = \sum_{x_1<\alpha} \cdots \sum_{x_m<\alpha} 1 \cdot q^{x_1+x_2\alpha+\cdots+x_m\alpha^{m-1}}. \tag{4}$$

Now we invoke a theorem due to Kummer which says that for a prime q, if $x = \sum_{i<\alpha} x_i q^i$ and $y = \sum_{i<\alpha} y_i q^i$ with $0 \leqslant x_i, y_i < q$ for all i, then

$$\binom{x}{y} \equiv \binom{x_{\alpha-1}}{y_{\alpha-1}} \cdots \binom{x_1}{y_1} \binom{x_0}{y_0} \mod q.$$

(Recall that if the upper number in a binomial coefficient is less than the lower number, the coefficient is defined to be 0.) A special case of this theorem is that

$$q \text{ divides } \binom{x}{y} \text{ if and only if } y_i > x_i \text{ for some } i.$$

We then obtain

$$\forall \bar{x}<\alpha\, p(\bar{x}) \neq 0 \Leftrightarrow \exists q \left(q > B_p(\alpha) \wedge \mathrm{Prime}(q) \wedge \binom{T(\alpha, q)}{S(\alpha, q)} \not\equiv 0 \bmod q \right)$$

where $B_p(z)$ is some polynomial term bounding all possible values of $p(\bar{x})$ with $\bar{x} < z$, for example,

$$B_p(z) = \sum_{i_1,\dots,i_m} |c_{i_1,\dots,i_m}|\, z^{i_1+\dots+i_m}. \tag{5}$$

5 RD(exp) and generalized geometric series

Fix an $\exists_1$ formula for $x^y = z$. The theory RD(exp) (for 'recursive definitions of exponentiation') is PA^- together with an axiom for the functionality of y^z together with

1. $\forall x\,(x^0 = 1)$
2. $\forall x, y, z\,(x^y = z \to x^{y+1} = xz)$
3. $\forall x, y, z\,(x^y = z \wedge y > 0 \to \exists w\,(z = xw \wedge x^{y-1} = w))$

Theorem 5. *For all $n \in \mathbb{N}$ there is an $\exists_1$ formula $G_n(u, v, q) = x$ for*

$$\sum_{i=u}^{v-1} i^n q^i = x$$

such that RD(exp) *proves the universal closure of the following.*

1. $u \geqslant v \to G_n(u, v, q) = 0$
2. $q = 0 \wedge u > 0 \to G_n(u, v, q) = 0$
3. $q = 0 \wedge u = 0 \to G_n(u, v, q) = 0^n$
4. $q > 0 \wedge u < v \wedge G_n(u, v, q) = x \to$
   (a) q^u, q^v *exist*
   (b) $G_n(u, v+1, q) = x + v^n q^v$
   (c) $u > 0 \to G_n(u-1, v, q) = x + (u-1)^n q^{u-1}$
   (d) $u < v \to G_n(u, v-1, q) = x - (v-1)^n q^{v-1}$
   (e) $u < v \to G_n(u+1, v, q) = x - u^n q^u$

Proof. By induction on n. For $n = 0$ define $G_0(u, v, q) = x$ to be the formula

$$\begin{array}{ll} & (q = 0 \wedge x = 0 \wedge u > 0) \\ \vee & (q = 0 \wedge x = 1 \wedge u = 0) \\ \vee & (v \leqslant u \wedge x = 0) \\ \vee & (q > 0 \wedge v > u \wedge \exists r, s\,(q^u = r \wedge q^v = s \wedge (q-1)x = s - r)) \end{array}$$

Most of the verifications are trivial; the axioms of RD(exp) are used in 4b–4e. For 4b, suppose that $(q-1)x = q^v - q^u$. Then $q^{v+1} = qq^v$ by axiom 2 of RD(exp), so $(q-1)(x+q^v) = (q-1)x + q^{v+1} - q^v = q^{v+1} - q^u$ as required. The others are similar.

Working in $\mathbb{N}$, the formula for G_{n+1} is derived from writing down an expression for $(q-1)G_{n+1}(u, v, q)$ and expanding using $G_0, \dots, G_n$. Ignoring the trivial cases such as $v \leqslant u$ and $q = 0$ (which should be incorporated as for G_0 above), we obtain for $G_{n+1}(u, v, q) = x$ the formula

$$\begin{array}{rcl} & & q^u, q^v, G_0(u+1, v, q), \ldots, G_n(u+1, v, q) \text{ all exist } \wedge \\ (q-1)x & = & (v-1)^{n+1} q^v - u^{n+1} q^u + \\ & & \sum\limits_{i=0}^{n} (-1)^{n+1-i} \binom{n+1}{i} G_i(u+1, v, q). \end{array}$$

(Note that the binomial coefficients and the bounds on the summation here are all fixed standard natural numbers.) Once again, it is necessary to verify that 4b–4e are provable as indicated.

For 4b, suppose x satisfies the formula above. Then

$$\begin{array}{l} (q-1)(x + v^{n+1} q^v) \\ \quad = \quad (v-1)^{n+1} q^v - u^{n+1} q^u + \sum\limits_{i=0}^{n} (-1)^{n+1-i} \binom{n+1}{i} G_i(u+1, v, q) \\ \qquad\quad + v^{n+1} q^{v+1} - v^{n+1} q^v \\ \quad = \quad v^{n+1} q^{v+1} - u^{n+1} q^u + \sum\limits_{i=0}^{n} (-1)^{n+1-i} \binom{n+1}{i} G_i(u+1, v, q) \\ \qquad\quad + ((v-1)^{n+1} - v^{n+1}) q^v \\ \quad = \quad v^{n+1} q^{v+1} - u^{n+1} q^u + \sum\limits_{i=0}^{n} (-1)^{n+1-i} \binom{n+1}{i} G_i(u+1, v, q) \\ \qquad\quad + \sum\limits_{i=0}^{n} (-1)^{n+1-i} \binom{n+1}{i} v^i q^v \\ \quad = \quad v^{n+1} q^{v+1} - u^{n+1} q^u + \sum\limits_{i=0}^{n} (-1)^{n+1-i} \binom{n+1}{i} G_i(u+1, v+1, q) \end{array}$$

by the induction hypotheses for G_i with $i \leqslant n$. The other verifications are similar. $\square$

The particular formulas just presented for these generalized power series have a welcome extra property.

Theorem 6. *For the formulas $G_n(u, v, q) = x$ for $\sum_{i=u}^{v-1} i^n q^i = x$ given in the previous theorem,* RD(exp) *proves the universal closure of*

$$G_n(u, v, q) = x \wedge G_n(v, w, q) = y \to G_n(u, w, q) = x + y$$

for each $n \in \mathbb{N}$.

Proof. Again we use induction on n. For $n = 0$, if $(q-1)x = q^v - q^u$ and $(q-1)y = q^w - q^u$, then clearly $(q-1)(x+y) = q^w$ by axioms of PA^-.

For $n+1$, if $G_{n+1}(u, v, q) = x$ and $G_{n+1}(v, w, q) = y$ then

$$\begin{array}{rcl} (q-1)(x+y) & = & (v-1)^{n+1} q^v - u^{n+1} q^u + \\ & & \sum\limits_{i=0}^{n} (-1)^{n+1-i} \binom{n+1}{i} G_i(u+1, v, q) + \end{array}$$

$$
\begin{aligned}
&(w-1)^{n+1}q^w - v^{n+1}q^v + \\
&\sum_{i=0}^{n}(-1)^{n+1-i}\binom{n+1}{i}G_i(v+1,w,q).
\end{aligned}
$$

But

$$((v-1)^{n+1} - v^{n+1})q^v = \sum_{i=0}^{n}(-1)^{n+1-i}\binom{n+1}{i}v^i q^v$$

and this together with the previous theorem gives

$$
\begin{aligned}
(q-1)(x+y) &= (w-1)^{n+1}q^v - u^{n+1}q^u + \\
&\quad \sum_{i=0}^{n}(-1)^{n+1-i}\binom{n+1}{i}G_i(u+1,v,q) + \\
&\quad \sum_{i=0}^{n}(-1)^{n+1-i}\binom{n+1}{i}v^i q^v + \\
&\quad \sum_{i=0}^{n}(-1)^{n+1-i}\binom{n+1}{i}G_i(v+1,w,q) \\
&= (w-1)^{n+1}q^v - u^{n+1}q^u + \\
&\quad \sum_{i=0}^{n}(-1)^{n+1-i}\binom{n+1}{i}G_i(u+1,w,q)
\end{aligned}
$$

as required. □

Rather than using the notation $G_n(u,v,q)$ we will use the more natural notation $\sum_{i=u}^{v-1} i^n q^i$ with the understanding that expressions of this form will be represented by the formulas G_n in the theorem. Note that the sentences in this theorem can be regarded as the recursive definitions of these summation symbols. In other words, Theorem 5 can be summarized by saying

$$\mathrm{RD}(\exp) \vdash \mathrm{RD}(\textstyle\sum_{i=u}^{v-1} i^n q^i : i \in \mathbb{N}) + \mathrm{A} \tag{6}$$

where A is the statement in Theorem 6. However, (6) has to be interpreted with some care, since it says that for any $\exists_1$ representation of $x^y = z$ and the corresponding axioms RD(exp), there are *particular* $\exists_1$ representations of $\sum_{i=u}^{v-1} i^n q^i$ $(i \in \mathbb{N})$ for which the axioms of $\mathrm{RD}(\sum_{i=u}^{v-1} i^n q^i : i \in \mathbb{N}) + \mathrm{A}$ are provable.

6 A diophantine undecidable theory

In order to express Matiyasevich's idea given in section 4, we need to fix further $\exists_1$ relations for primality and the binomial coefficients,

$$\mathrm{Prime}(x) \quad \text{and} \quad \binom{x}{y} = z.$$

The axiom expressing the functionality of the binomial coefficient (as discussed above) is denoted $\mathrm{F}_{\mathrm{binom}}$.

The Kummer axioms, Kum, is the following

$$\forall q, u, s_0, s_1, t_0, t_1, x, y, z \left(\begin{array}{l} \mathrm{Prime}(q) \wedge q^u \text{ exists} \wedge s_0 < q^u \wedge t_0 < q^u \\ x = \binom{s_0 + q^u s_1}{t_0 + q^u t_1} \wedge \\ y = \binom{s_0}{t_0} \wedge z = \binom{s_1}{t_1} \\ \rightarrow x \equiv yz \bmod q \end{array} \right).$$

In fact, we will only need the following information from this axiom: first, $q \not| \binom{xq^u}{q^u}$ for $Prime(q)$ and $x \geqslant 1$, and second, $q \not| \binom{t_0+q^u t_1}{s_0+q^u s_1}$ implies $q \not| \binom{q^u t_1}{q^u s_1}$ for $s_0, t_0 < q^u$.

We will also need two further axioms. The axiom for Euclidean division, Euc, is

$$\forall x, y\, (y > 0 \rightarrow \exists r, s\, (x = ys + r \wedge r < y)),$$

and the following 'distributivity' axiom for exponentiation and multiplication, $\mathrm{D_{exp}}$,

$$\forall x, y, z\, (x^{y+z} = x^y \cdot x^z).$$

This is interpreted as saying if either x^{y+z} exists or both x^y, x^z exist, then all three exist and the equation is valid. I note in passing that by a result of Wilkie, the theory PA + Euc has precisely the same $\forall_1$ consequences as IOpen [7], so the diophantine problems for these two theories are equivalent.

We note also the statement $\binom{0}{1} = 0$. As this is an $\exists_1$ sentence and true, it is provable outright in PA^-, so is not needed as an extra axiom.

Theorem 7. *The $\mathcal{L}_\mathrm{A}$-theory* $\mathrm{PA}^- + \mathrm{RD}(\exp) + \mathrm{F_{binom}} + \mathrm{Euc} + \mathrm{D_{exp}} + \mathrm{Kum}$ *is diophantine sufficient, hence diophantine undecidable.*

Proof. Let T denote the theory in question. We shall employ the method of Theorem 4 where $N = 2$, adding new formulas to θ and to ψ until we have formulas (the conjuction of all the formulas introduced along the way) which satisfy all four conditions in the theorem. The idea of Section 4 will be used which supplies us with a suitable starting point for the formula $\theta(y, q, T, S)$.

Formulas to add to θ.

$$\begin{array}{ll} & q > B_p(y) \wedge \mathrm{Prime}(q) \wedge \eta \wedge \\ \wedge & T = \sum\limits_{i_1,\ldots,i_m} c_{i_1,\ldots,i_m} \left(\sum\limits_{z_1<y} z_1^{i_1} q^{z_1} \right) \cdots \left(\sum\limits_{z_m<y} z_m^{i_m} q^{z_m y^{m-1}} \right) \\ \wedge & S = \left(\sum\limits_{z_1<y} q^{z_1} \right) \cdots \left(\sum\limits_{z_m<y} q^{z_m y^{m-1}} \right) \\ \wedge & \binom{T}{S} \not\equiv 0 \bmod q \end{array}$$

where the polynomial $p(\bar{x})$ is given as

$$p(\bar{x}) = \sum_{i_1,\ldots,i_m} c_{i_1,\ldots,i_m} x^{i_1} \cdots x^{i_m}$$

which (provably in PA^-) only takes nonnegative values, $B_p(y)$ is the polynomial bound given in (5),

$$B_p(y) = \sum_{i_1,\dots,i_m} |c_{i_1,\dots,i_m}|\, y^{i_1+\dots+i_m},$$

and η is the $\exists_1$ formula expressing the fact that the sums of all the generalized geometric series in the expressions for S, T exist, using the formulas given in section 5.

Whenever we add new formulas to θ in this way, we must check that

$$\mathbb{N} \vDash \forall y \geqslant 2\, \exists q, T, S\, \theta(y, q, T, S) \tag{7}$$

In this case, the argument in section 4 shows that (7) holds as required in Theorem 4. We will add to θ further conditions on the numbers y, q, T, S later, so that the 'real' θ will be a conjuction of the formula above with some further formulas given below. We will of course verify (7) each time this is done.

The formula ψ will be given in a similar way, by combining many 'conditions' on numbers $\bar{x}, y, q, T, S$ as we go along. In this case, we must check that 2 and 3 in Theorem 4 holds each time we add new formulas to ψ. The final part of the proof will be when we have collected together all the formulas for θ and ψ, and here we just need to verify 4 of Theorem 4.

As previously mentioned, ψ should be thought of as an 'induction formula', i.e., a formula to apply an induction rule or scheme to. Indeed, the most obvious way of showing that

$$T \vdash \forall \bar{u}, \bar{v}, y, \bar{z}\, (\theta(y, \bar{z}) \wedge 2 {\leqslant} \bar{u}{,}n{,}\bar{v} {<} y \wedge \psi(\bar{u}, 2, \bar{v}, y, \bar{z}) \rightarrow \psi(\bar{u}, n, \bar{v}, y, \bar{z}))$$

for all $n \in \mathbb{N}$ and all $i = \mathrm{len}(\bar{u}) = m - \mathrm{len}(\bar{v}) - 1 < m$ is to show

$$T \vdash \forall \bar{u}, \bar{v}, x, y, \bar{z}\, (\theta(y, \bar{z}) \wedge \bar{2} \leqslant u{,}x{,}x{+}1{,}\bar{v} < y \wedge \psi(\bar{u}, x, \bar{v}, y, \bar{z}) \rightarrow \psi(\bar{u}, x+1, \bar{v}, y, \bar{z})),$$

one of the hypotheses of an induction rule. To simplify the notation in examples like this, denote by e_k the kth 'unit vector', $(0, \cdots, 0, 1, 0, \cdots, 0)$ with the 1 in the kth position, and by S_k the kth 'successor function'

$$\bar{x} \mapsto \bar{x} + e_k$$

with componentwise addition.

For example, note that as the theory RD(exp) has no induction scheme, there is no obvious reason to expect that

$$T \vdash \forall x, y, z\, ((x^y)^z = x^{yz}). \tag{8}$$

But of course, a statement like this is necessary for understanding the idea in section 4. To get round this problem, ψ will express all instances of $(x^y)^z = x^{yz}$ that we will require. The induction step for ψ will hold for exactly the same reason that $\forall x, y, z\, ((x^y)^z = x^{yz})$ is provable in $\mathrm{RD(exp)} + \mathrm{D_{exp}}$ together with a single induction axiom.

Lemma 8. $\mathrm{RD(exp)} + \mathrm{D_{exp}}$ *proves that, for all* x, y,

1. $(x^y)^0 = x^{(y\cdot 0)}$, *and*

2. $(x^y)^z = x^{(y\cdot z)} \to (x^y)^{(z+1)} = x^{(y\cdot(z+1))}$.

Proof. For the first, $(x^y)^0 = 1 = x^0 = x^{(y\cdot 0)}$; for the second, $(x^y)^{(z+1)} = (x^y)^z(x^y) = x^{(y\cdot z)}(x^y) = x^{(y\cdot z+y)} = x^{(y\cdot(z+1))}$. (Note where the axioms of RD(exp) and $\mathrm{D}_{\exp}$ are used here.) $\square$

This provides a way to tackle the problem of the property of exponentiation expressed in (8), since (as it turns out) we will only need finitely many instances of the formula there.

Formulas to add to θ. All formulas

$$q^{y^j\cdot y^i} = \left(q^{y^j}\right)^{y^i}$$

for all i, j with $0 \leqslant i + j < m$. (By equations such as these, I always mean the $\exists_1$ statement that all subterms here exist and of course that the equation is true.)

These new formulas are obviously true, so (7) still holds.

Formulas to add to ψ. All formulas

$$q^{x_j y^{j-1}} = \left(q^{y^{j-1}}\right)^{x_j}$$

for all j in $\{1, 2, \ldots, m\}$. (Again, by this equation I include the statement expressing the existence of all subterms.)

Conditions 2 and 3 in Theorem 4 are rapidly verified for these statements in ψ, by the lemma.

Next, we require some bounds on the size of the terms $\sum_{z<x_i} z^n q^{zy^{i-1}}$ and $\sum_{z<y} z^n q^{zy^{i-1}}$ of $\mathrm{RD}(\sum_i i^n q^i)$.

Lemma 9. $\mathrm{RD(exp)} + \mathrm{D}_{\exp}$ *proves the following for any $p > 2$, $y \geqslant 1$ and any $n \in \mathbb{N}$.*

1. $\sum_{z<1} z^n p^z < 2 \cdot 1^n \cdot p^0$

2. $\sum_{z<y} z^n p^z < 2y^n p^{y-1} \to \sum_{z<y+1} z^n p^z < 2(y+1)^n p^y$

Proof. For the first, $\sum_{z<1} z^n p^z$ is 0 or 1 which is less than $2 = 2 \cdot 1^n \cdot p^0$. For the second, $\sum_{z<y+1} z^n p^z < 2y^n p^{y-1} = \sum_{z<y} z^n p^z + y^n p^y < 2y^n p^{y-1} + y^n p^y \leqslant 2y^n p^y$, since $p \geqslant 2$, which is in turn less than or equal to $2(y+1)^n p^y$. (Note $\forall x\,((x+1)^n \geqslant x^n)$ for all standard $n \in \mathbb{N}$ is a theorem of PA^-, and this is all that's required here. The status of this formula for possibly nonstandard n in RD(exp) seems to be a rather differnet matter.) $\square$

Formulas to add to θ. All statements

$$\sum_{z<y} z^n q^{zy^{i-1}} < 2y^n q^{(y-1)y^{i-1}}$$

for all $i \leqslant m$ and all $n \in \mathbb{N}$ that appears as some exponent i_j in $p(\bar{x}) = \sum_{\bar{\imath}} c_{\bar{\imath}} x_1^{i_1} \cdots x_m^{i_m}$.

Clearly, there are only finitely many such statements, and they are all true by the lemma, for $y \geqslant 2$ at least.

Similarly,

Formulas to add to ψ. All statements

$$\sum_{z<x_i} z^n q^{zy^{i-1}} < 2x_i^n q^{(x_i-1)y^{i-1}}$$

for all $i \leqslant m$ and all $n \in \mathbb{N}$ as before.

Again, by the lemma, the conditions 2 and 3 in Theorem 4 are satisfied individually for each of these statements in ψ.

In the rest of the proof of Theorem 7, I need to add further statements to θ and ψ to enable us to 'decode' the information already present in θ and obtain the information $p(\bar{x}) \neq 0$ that we require. For this, it will be convenient to use the lexicographic order relation $<$ on m-tuples by

$$\begin{aligned} &\langle r_1, r_2, \ldots, r_m \rangle < \langle s_1, s_2, \ldots, s_m \rangle \\ &\quad \Leftrightarrow \quad r_1 + r_2 y + \cdots + r_m y^{m-1} < s_1 + s_2 y + \cdots + s_m y^{m-1} \end{aligned}$$

so

$$\langle r_1, r_2, \ldots, r_m \rangle < \langle r_1, r_2, \ldots, r_m \rangle \Leftrightarrow \begin{array}{l} r_m < s_m \text{ or} \\ r_m = s_m \wedge r_{m-1} < s_{m-1} \text{ or} \\ \ldots \text{ or} \\ r_m = s_m \wedge \cdots \wedge r_2 = s_2 \wedge r_1 < s_1. \end{array}$$

If y is understood from the context, I shall use $\langle r_1, r_2, \ldots, r_m \rangle$ for the number $r_1 + r_2 y + \cdots + r_m y^{m-1}$.

Now, for each $\bar{\imath} = (i_1, \ldots, i_m) \in \mathbb{N}^m$ such that $c_{\bar{\imath}} x_1^{i_1} \cdots x_m^{i_m}$ appears as a term in $p(\bar{x})$ and $\bar{x} = (x_1, \ldots, x_m)$, define $T_{\bar{\imath}}(\bar{x}) =$

$$\begin{aligned} & \sum_{z_1} z_1^{i_1} q^{z_1} \cdots \sum_{z_{m-1}} z_{m-1}^{i_{m-1}} q^{z_{m-1} y^{m-2}} \sum_{z_m > x_m} z_{m-1}^{i_{m-1}} q^{z_m y^{m-2}} \\ + \; & \sum_{z_1} z_1^{i_1} q^{z_1} \cdots \sum_{z_{m-1} > x_{m-1}} z_{m-1}^{i_{m-1}} q^{z_{m-1} y^{m-2}} \sum_{z_m = x_m} z_{m-1}^{i_{m-1}} q^{z_m y^{m-2}} \\ + \; & \cdots \\ + \; & \cdots \\ + \; & \sum_{z_1 = x_1} z_1^{i_1} q^{z_1} \cdots \sum_{z_{m-1} = x_{m-1}} z_{m-1}^{i_{m-1}} q^{z_{m-2} y^{m-2}} \sum_{z_m = x_m} z_{m-1}^{i_{m-1}} q^{z_{m-2} y^{m-2}}, \end{aligned}$$

where the summations are from 0 to $y-1$ unless further restricted—note in particular that some summations are of the form $\sum_{z_i = x_i} (\cdots)$ and are over one term only! Here and throughout the rest of the proof, a term with a summation subterm such as

$$\cdots \sum z_{m-1}^{i_{m-1}} q^{z_{m-1} y^{m-2}} \cdots$$

is implicitly bracketed as

$$\cdots \left(\sum z_{m-1}^{i_{m-1}} q^{z_{m-1} y^{m-2}} \right) \cdots.$$

Informally, the intention of the definition $T_{\bar{\imath}}(\bar{x})$ above is that

$$T_{\bar{\imath}}(\bar{x}) = \sum_{\langle \bar{z} \rangle \geqslant \langle \bar{x} \rangle} z_i^{i_1} \cdots z_m^{i_m} q^{\langle z_1, \ldots, z_m \rangle},$$

but of course we have no expression for sums like this in our formal language. However, the original expression for $T_{\bar{\imath}}(\bar{x})$ is well defined. Using it we also define

$$T(\bar{x}) = \sum_{\bar{\imath}} c_{\bar{\imath}} T_{\bar{\imath}}(\bar{x})$$

(where the $\bar{\imath}$ and $c_{\bar{\imath}}$ come from the expression for the polynomial $p(\bar{x})$ of course) and the analogous expression for the constant polynomial with value 1,

$$S(\bar{x}) = T_{\bar{0}}(\bar{x}).$$

Formulas to add to θ.

$$q \not\mid \binom{T(\bar{2})}{S(\bar{2})}. \tag{9}$$

This formula can be added to θ safely, since we may assume $y > 2$ and in $\mathbb{N}$,

$$T = T(\bar{0}) = \sum_{\langle \bar{z} \rangle \geqslant \langle \bar{2} \rangle} p(\bar{z}) q^{\langle z_1, \ldots, z_m \rangle} + \sum_{\langle \bar{z} \rangle < \langle \bar{2} \rangle} p(\bar{z}) q^{\langle z_1, \ldots, z_m \rangle}$$

and each $p(\bar{z}) < q$ for $\langle \bar{z} \rangle < \langle \bar{2} \rangle$, thus

$$T = \sum_{\langle \bar{z} \rangle \geqslant \langle \bar{2} \rangle} p(\bar{z}) q^{\langle z_1, \ldots, z_m \rangle} + r = T(\bar{2}) + r$$

with $q^{\langle \bar{2} \rangle}$ dividing $T(\bar{2})$ and $r < q^{\langle \bar{2} \rangle}$. Similarly,

$$S = S(\bar{2}) + s$$

with $q^{\langle \bar{2} \rangle}$ dividing $S(\bar{2})$ and $s < q^{\langle \bar{2} \rangle}$, thus (9) holds in $\mathbb{N}$ by the Kummer axiom.

The 'most important' formula to add to ψ is given next.

Formulas to add to ψ.

$$q \not\mid \binom{T(\bar{x})}{S(\bar{x})}. \tag{10}$$

We need to show that the conditions required in 2 and 3 of Theorem 4 are satisfied, by the new formula added to ψ, and this is the main part of the whole argument. It is not so much difficult as 'technical'; the reader will see that the formulas previously added to ψ were introduced simply to make this part of the argument go through.

Lemma 10. *If $\psi(\bar{x}, y, q, S, T)$ is the conjunction of all the formulas added to ψ so far, then by adding certain new formulas to θ satisfying the condition in (7) we can show that T proves*

1. *$\forall y, q, S, T\, (\theta(y, q, S, T) \wedge y > 2 \rightarrow \psi(2, 2, \ldots, 2, y, \bar{z}))$ and*
2. *$\forall \bar{x}, y, q, S, T\, (\theta(y, q, S, T) \wedge y > 2 \wedge 2 \leqslant \bar{x}, S_k(\bar{x}) < y \wedge \psi(\bar{x}, y, q, T, S) \rightarrow \psi(S_k(\bar{x}), y, q, T, S))$.*

Proof. The first part is a triviality from the new formula just added to θ. For the second part, we freely use Theorem 5 and Theorem 6, as well as all the statements in $\psi(\bar{x}, y, q, T, S)$. By Lemmas 8 and 9, we may also assume all statements in $\psi(S_k(\bar{x}), y, q, T, S)$—except of course the one from (10) which is what we want to verify.

Consider a single $\bar{\imath} \in \mathbb{N}^m$ occuring as a tuple of exponents in $p(\bar{x})$ first. I shall temporarily abbreviate $z_j^{i_j} q^{z_j y^{j-1}}$ by Z_j, and use the convention of omitting the brackets around summations $\sum_{z_j} Z_j$ as previously mentioned, and also abbreviate the following product of 'trivial' sums of length one,

$$\sum_{z_{k+1}=x_{x+1}} Z_{k+1} \cdots \sum_{z_m=x_m} Z_m$$

by Q. Then write

$$T_{\bar{\imath}}(\bar{x}) = T_{\bar{\imath}}(S_k(\bar{x})) + U_{\bar{\imath}}^k(\bar{x}) + V_{\bar{\imath}}^k(\bar{x}) \tag{11}$$

where the $U_{\bar{\imath}}^k(\bar{x})$ collects terms involving $z_k = x_k + 1$ but $z_i < x_i$ for some $i < k$, and the $V_{\bar{\imath}}^k(\bar{x})$ collects terms with $z_k = x_k$.

Specifically, in equation (11), we have $U_{\bar{\imath}}^k(\bar{x}) =$

$$\begin{aligned}
& \sum_{z_1<x_1} Z_1 \sum_{z_2=x_2} Z_2 \cdots \sum_{z_{k-1}=x_{k-1}} Z_{k-1} \sum_{z_k=x_k+1} Z_k \; Q \\
+ \; & \sum_{z_1} Z_1 \sum_{z_2<x_2} Z_2 \cdots \sum_{z_{k-1}=x_{k-1}} Z_{k-1} \sum_{z_k=x_k+1} Z_k \; Q \\
+ \; & \cdots \\
+ \; & \sum_{z_1} Z_1 \sum_{z_2} Z_2 \cdots \sum_{z_{k-1}<x_{k-1}} Z_{k-1} \sum_{z_k=x_k+1} Z_k \; Q
\end{aligned}$$

and $V_{\bar{\imath}}^k(\bar{x}) =$

$$\begin{aligned}
& \sum_{z_1} Z_1 \sum_{z_2} Z_2 \cdots \sum_{z_{k-2}} Z_{k-2} \sum_{z_{k-1}>x_{k-1}} Z_{k-1} \sum_{z_k=x_k} Z_k \; Q \\
+ \; & \cdots \\
+ \; & \sum_{z_1>x_1} Z_1 \sum_{z_2=x_2} Z_2 \cdots \sum_{z_{k-2}=x_{k-2}} Z_{k-2} \sum_{z_{k-1}=x_{k-1}} Z_{k-1} \sum_{z_k=x_k} Z_k \; Q \\
+ \; & \sum_{z_1=x_1} Z_1 \sum_{z_2=x_2} Z_2 \cdots \sum_{z_{k-2}=x_{k-2}} Z_{k-2} \sum_{z_{k-1}=x_{k-1}} Z_{k-1} \sum_{z_k=x_k} Z_k \; Q
\end{aligned}$$

Of course, equation (11) can be proved directly using Theorem 5 using these definitions of $U_{\bar{\imath}}^k(\bar{x})$ and $V_{\bar{\imath}}^k(\bar{x})$.

Think of $U_{\bar{\imath}}^k(\bar{x}) + V_{\bar{\imath}}^k(\bar{x})$ as the '$\bar{\imath}$th difference', $T_{\bar{\imath}}(\bar{x}) - T_{\bar{\imath}}(S_k(\bar{x}))$. We aim to show first that

$$\sum_{\bar{\imath}} c_{\bar{\imath}}(U_{\bar{\imath}}^k(\bar{x}) + V_{\bar{\imath}}^k(\bar{x})) < q^{\langle S_k(\bar{x}) \rangle},$$

where $\langle \bar{x} \rangle$ is as usual the number $x_1 + x_2 y + \cdots + x_m y^{m-1}$. These will require the following

Formulas to add to θ.

$$q > 2^{m+2} m y^n, \qquad q > 4(k-1) B_p(y),$$

where n is the total degree of $p(\bar{x})$, i.e., $n = \max_{\bar{\imath}}(i_1 + \cdots + i_m)$.

This can be added to θ since the only requirement on q up to now is that it is a sufficiently large prime.

To estimate $U_{\bar{\imath}}^k(\bar{x})$, note first that

$$\sum_{z_1} Z_1 \sum_{z_2<x_2} Z_2 \leqslant 2y^{i_1}q^{y-1}\cdot 2x_2^{i_2}q^{(x_2-1)y} < q^y x_2^{i_2}q^{(x_2-1)y} = x_2^{i_2}q^{x_2y} = \sum_{z_2=x_2} Z_2$$

since $q > 4y^{i_1}$, from θ. Since we are assuming $x_1 \geqslant 2$ this gives

$$\sum_{z_1} Z_1 \sum_{z_2<x_2} Z_2 \leqslant \sum_{z_1<x_1}\sum_{z_2=x_2} Z_2$$

Other inequalities like this hold in a simliar way. Thus the first term in $U_{\bar{\imath}}^k(\bar{x})$ is the largest. As there are $k-1$ terms, we get

$$\begin{aligned}
U_{\bar{\imath}}^k(\bar{x}) &\leqslant (k-1)\sum_{z_1<x_1} Z_1 \sum_{z_2=x_1} Z_1 \cdots \sum_{z_{k-1}=x_{k-1}} Z_{k-1} \sum_{z_k=x_k+1} Z_k\ Q \\
&< (k-1)2x_1^{i_1}q^{x_1-1}x_2^{i_2}q^{x_2y}\cdots x_{k-1}^{i_{k-1}}q^{x_{k-1}y^{k-2}}(x_k+1)^{i_k}q^{(x_k+1)y^{k-1}}Q \\
&= 2(k-1)x_1^{i_1}\cdots x_{k-1}^{i_{k-1}}(x_k+1)^{i_k}x_{k+1}^{i_{k+1}}\cdots x_m^{i_m}q^{\langle S_k(x_1-1,x_2,\ldots x_m)\rangle}.
\end{aligned}$$

For $V_{\bar{\imath}}^k(\bar{x})$ we have k terms of which the first is clearly the largest, hence

$$\begin{aligned}
V_{\bar{\imath}}^k(\bar{x}) &\leqslant k\sum_{z_1} Z_1 \cdots \sum_{z_{k-1}} Z_{k-1} \sum_{z_k=x_k} Z_k\ Q \\
&< k2^{k-1}y^{i_1}q^{y-1}\cdots y^{i_{k-1}}q^{(y-1)y^{k-2}}x_k^{i_k}q^{x_ky^{k-1}}Q \\
&< x_k^{i_k}q^{(x_k+1)y^{k-1}}Q \\
&\leqslant U_{\bar{\imath}}^k(\bar{x})
\end{aligned}$$

as $q > ky^n2^{k-1}$, where n is the total degree of $p(\bar{x})$, from θ again.

Combining these, we have

$$U_{\bar{\imath}}^k(\bar{x}) + V_{\bar{\imath}}^k(\bar{x}) < 4(k-1)x_1^{i_1}\cdots x_{k-1}^{i_{k-1}}(x_k+1)^{i_k}x_{k+1}^{i_{k+1}}\cdots x_m^{i_m}q^{\langle S_k(x_1-1,x_2,\ldots x_m)\rangle}.$$

Note too that

$$\langle S_k(x_1-1,x_2,\ldots x_m)\rangle = \langle S_k(x_1,x_2,\ldots x_m)\rangle,$$

hence

$$\sum_{\bar{\imath}} c_{\bar{\imath}}(U_{\bar{\imath}}^k(\bar{x}) + V_{\bar{\imath}}^k(\bar{x})) < 4(k-1)p(S_k(\bar{x}))q^{\langle S_k(x_1,x_2,\ldots x_m)\rangle-1}.$$

Using $q > 4(k-1)B_p(y)$ from θ again, we have

$$T(\bar{x}) - T(S_k(\bar{x})) = \sum_{\bar{\imath}} c_{\bar{\imath}}(U_{\bar{\imath}}^k(\bar{x}) + V_{\bar{\imath}}^k(\bar{x})) < q^{\langle S_k(\bar{x})\rangle},$$

as claimed.

The rest of the proof of the lemma is just an application of the Kummer axiom. Since clearly

$$T(S_k(\bar{x})) \text{ is divisible by } q^{\langle S_k(\bar{x})\rangle}$$

as each $T_{\bar{\imath}}(S_k(\bar{x}))$ is, and

$$T(\bar{x}) = T(S_k(\bar{x})) + \sum_{\bar{\imath}} c_{\bar{\imath}}(U_{\bar{\imath}}^k(\bar{x}) + V_{\bar{\imath}}^k(\bar{x}))$$

writes $T(\bar{x})$ as quotient and remainder modulo $q^{\langle S_k(\bar{x})\rangle}$, similarly for

$$S(\bar{x}) = T_{\bar{0}}(\bar{x}) = T_{\bar{0}}(S_k(\bar{x})) + \sum_{\bar{\imath}} c_{\bar{\imath}}(U_{\bar{0}}^k(\bar{x}) + V_{\bar{0}}^k(\bar{x})),$$

so we have

$$\binom{T(\bar{x})}{S(\bar{x})} \equiv \binom{T(S_k(\bar{x}))}{S(S_k(\bar{x}))}\binom{t}{s} \bmod q$$

for the remainders r, s, hence

$$q \not| \binom{T(\bar{x})}{S(\bar{x})} \to q \not| \binom{T(S_k(\bar{x}))}{S(S_k(\bar{x}))}$$

as required. □

The proof of the theorem is now almost complete. We have got all the parts of θ and ψ that are required; all that is left to do is to verify part 4 in Theorem 4. This again is a simple application of the Kummer axiom, for clearly

$$T(\bar{x}) = q^{\langle \bar{x}\rangle}(p(\bar{x}) + qT')$$

and

$$S(\bar{x}) = q^{\langle \bar{x}\rangle}(1 + qS')$$

for some numbers $T', S' \geqslant 0$. From ψ we have

$$q \not| \binom{T(\bar{x})}{S(\bar{x})}.$$

Moreover, provably in PA^- we have $p(\bar{x}) < B_p(y)$, so by the Kummer axiom,

$$q \not| \binom{p(\bar{x})}{1}$$

which shows that $\binom{p(\bar{x})}{1} \neq 0$, hence $p(\bar{x}) > 0$ as required. □

References

[1] H. Gaifman and C. Dimitracopoulos. Fragments of arithmetic and the MRDP theorem. In *Logic and Algorithmic, Monographie No. 30*, pages 187–206. L'Enseignement Mathèmatique, Genève, 1982.

[2] Richard W. Kaye. Diophantine induction. *Annals of Pure and Applied Logic*, 46:1–40, 1989.

[3] Richard W. Kaye. Hilbert's tenth problem for weak theories of arithmetic. *Annals of Pure and Applied Logic*, 61:63–73, 1993.

[4] Richard W. Kaye. Diophantine undecidable theories of arithmetic. unpublished preprint, 1996.

[5] Lou van den Dries. Some model theory and number theory for models of weak systems of arithmetic. In Leszek Pacholski et al., editors, *Model theory or algebra and arithmetic, Proceedings, Karpacz 1979*, volume 834 of *Lecture Notes in Mathematics*, pages 346–362. Springer Verlag, 1980.

[6] Lou van den Dries. Which curves over $\mathbb{Z}$ have points with coordinates in a discretely ordered ring? *Transactions of the American Mathematical Society*, 264:181–189, 1981.

[7] A. J. Wilkie. Some results and problems on weak systems of arithmetic. In A. J. Macintyre et al., editors, *Logic Colloquium '77*, pages 285–296. North Holland, 1978.