Polynomial Termination over $\mathbb{N}$ is Undecidable

Fabian Mitterwallner
University of Innsbruck, Innsbruck, Austria

Aart Middeldorp
University of Innsbruck, Innsbruck, Austria

Abstract

In this paper we prove that the problem whether the termination of a given rewrite system can be shown by a polynomial interpretation in the natural numbers is undecidable.

2012 ACM Subject Classification Theory of computation → Equational logic and rewriting; Theory of computation → Rewrite systems; Theory of computation → Computability

Keywords and phrases term rewriting, polynomial termination, undecidability

Acknowledgements We thank the reviewers for critically reading the paper, and providing comments and suggestions.

1 Introduction

Proving termination of a rewrite system by using a polynomial interpretation over the natural numbers goes back to Lankford [4]. Two problems need to be addressed when using polynomial interpretations for proving termination, whether by hand or by a tool:

1. finding suitable polynomials for the function symbols,
2. showing that the induced order constraints on polynomials are valid.

The latter problem amounts to ($\star$) proving $P(x_1, \dots, x_n) > 0$ for all natural numbers $x_1, \dots, x_n \in \mathbb{N}$, for polynomials $P \in \mathbb{Z}[x_1, \dots, x_n]$. This is known to be undecidable, as a consequence of Hilbert's 10th Problem, see e.g., Zantema [6, Proposition 6.2.11]. Heuristics for the former problem are presented in [2, 6]. In this paper we prove the undecidability of the existence of a termination proof by a polynomial interpretation in $\mathbb{N}$ by a reduction from ($\star$). This result is not surprising, but we are not aware of a proof of undecidability in the literature, and the construction is not entirely obvious. We construct a family of rewrite systems $\mathcal{R}_P$ parameterized by polynomials $P \in \mathbb{Z}[x_1, \dots, x_n]$ such that $\mathcal{R}_P$ is polynomially terminating over $\mathbb{N}$ if and only if $P(x_1, \dots, x_n) > 0$ for all $x_1, \dots, x_n \in \mathbb{N}$. The construction is based on techniques from [5], in which specific rewrite rules enforce the interpretations of certain function symbols.

2 Undecidability of Polynomial Termination

We assume familiarity with term rewriting [1], but recall the definition of polynomial termination over $\mathbb{N}$. Given a signature $\mathcal{F}$, a well-founded monotone $\mathcal{F}$-algebra $(\mathcal{A}, >)$ consists of a non-empty $\mathcal{F}$-algebra $\mathcal{A} = (A, \{f_\mathcal{A}\}_{f \in \mathcal{F}})$ and a well-founded order $>$ on the carrier A of $\mathcal{A}$ such that every algebra operation is strictly monotone in all its coordinates, i.e., if $f \in \mathcal{F}$ has arity $n \geqslant 1$ then $f_\mathcal{A}(a_1, \dots, a_i, \dots, a_n) > f_\mathcal{A}(a_1, \dots, b, \dots, a_n)$ for all $a_1, \dots, a_n, b \in A$ and $i \in \{1, \dots, n\}$ with $a_i > b$. The induced order $>_\mathcal{A}$ on terms is a reduction order that ensures the termination of any compatible (i.e., $\ell >_\mathcal{A} r$ for all rewrite rules $\ell \to r$) TRS $\mathcal{R}$. We call $\mathcal{R}$ *polynomially terminating over* $\mathbb{N}$ if compatibility holds when the underlying algebra $\mathcal{A}$ is restricted to the set of natural numbers $\mathbb{N}$ with standard order $>_\mathbb{N}$ such that every n-ary function symbol f is interpreted as a monotone polynomial $f_\mathbb{N}$ in $\mathbb{Z}[x_1, \dots, x_n]$.

Table 1 The TRS $\mathcal{R}$.

$\mathsf{g}(\mathsf{s}(x)) \to \mathsf{s}(\mathsf{s}(\mathsf{g}(x)))$	(A)	$\mathsf{s}(\mathsf{s}(\mathsf{0})) \to \mathsf{q}(\mathsf{s}(\mathsf{0}))$	(G)
$\mathsf{q}(\mathsf{g}(x)) \to \mathsf{g}(\mathsf{g}(\mathsf{q}(x)))$	(B)	$\mathsf{s}(\mathsf{0}) \to \mathsf{q}(\mathsf{0})$	(H)
$\mathsf{g}(x) \to \mathsf{a}(x,x)$	(C)	$\mathsf{q}(\mathsf{s}(\mathsf{0})) \to \mathsf{0}$	(I)
$\mathsf{s}(x) \to \mathsf{a}(\mathsf{0},x)$	(D)	$\mathsf{s}^5(\mathsf{0}) \to \mathsf{q}(\mathsf{s}(\mathsf{s}(\mathsf{0})))$	(J)
$\mathsf{s}(x) \to \mathsf{a}(x,\mathsf{0})$	(E)	$\mathsf{q}(\mathsf{s}(\mathsf{s}(\mathsf{0}))) \to \mathsf{s}^3(\mathsf{0})$	(K)
$\mathsf{a}(\mathsf{q}(x),\mathsf{g}(x)) \to \mathsf{q}(\mathsf{s}(x))$	(F)	$\mathsf{s}(\mathsf{a}(x,x)) \to \mathsf{d}(x)$	(L)
		$\mathsf{s}(\mathsf{d}(x)) \to \mathsf{a}(x,x)$	(M)
		$\mathsf{s}(\mathsf{a}(\mathsf{q}(\mathsf{a}(x,y)),\mathsf{d}(\mathsf{a}(x,y)))) \to \mathsf{a}(\mathsf{a}(\mathsf{q}(x),\mathsf{q}(y)),\mathsf{d}(\mathsf{m}(x,y)))$	(N)
		$\mathsf{s}(\mathsf{a}(\mathsf{a}(\mathsf{q}(x),\mathsf{q}(y)),\mathsf{d}(\mathsf{m}(x,y)))) \to \mathsf{a}(\mathsf{q}(\mathsf{a}(x,y)),\mathsf{d}(\mathsf{a}(x,y)))$	(O)

Whereas well-founded monotone algebras are complete for termination, polynomial termination gives rise to a much more restricted class of TRSs. For instance, Hofbauer and Lautemann [3] proved that polynomially terminating TRSs induce a double-exponential upper bound on the derivational complexity.

Our rewrite systems $\mathcal{R}_P$ consists of three parts: a fixed component $\mathcal{R}$, which is extended to $\mathcal{R}_n$ for some $n \in \mathbb{N}$ depending on the exponents in P, and a single rewrite rule that encodes the positiveness of P. For the latter we need function symbols that are interpreted as addition and multiplication. That is the purpose of the TRS $\mathcal{R}$, whose rules are presented in Table 1. It is a simplified and modified version of the TRS $\mathcal{R}_2$ in [5]. Since multiplication is not strictly monotone on $\mathbb{N}$, the rules (N) and (O) restrict the interpretation of m to $xy + x + y$, which suffices for the reduction.

▶ **Lemma 1.** *The* TRS $\mathcal{R}$ *is polynomially terminating over* $\mathbb{N}$.

Proof. The well-founded algebra $(\mathbb{N}, >_{\mathbb{N}})$ with interpretations

$$\mathsf{0}_{\mathbb{N}} = 0 \qquad \mathsf{s}_{\mathbb{N}}(x) = x+1 \qquad \mathsf{a}_{\mathbb{N}}(x,y) = x+y \qquad \mathsf{q}_{\mathbb{N}}(x) = x^2$$
$$\mathsf{d}_{\mathbb{N}}(x) = 2x \qquad \mathsf{g}_{\mathbb{N}}(x) = 4x+6 \qquad \mathsf{m}_{\mathbb{N}}(x,y) = xy+x+y$$

is monotone and compatible with $\mathcal{R}$. Hence $\mathcal{R}$ is polynomially terminating. ◀

Note that this polynomial interpretation is found by the termination tool $\mathsf{T_TT_2}$ with the strategy `poly -direct -nl2 -ib 4 -ob 6`.

More importantly, to ensure termination in $(\mathbb{N}, >_{\mathbb{N}})$, the rewrite rules of $\mathcal{R}$ mandate that the interpretation of some of the function symbols is unique. The proof of the following lemma closely follows the reasoning in [5, Lemmata 4.4 and 5.2].

▶ **Lemma 2.** *Any monotone polynomial interpretation* $(\mathbb{N}, >_{\mathbb{N}})$ *compatible with* $\mathcal{R}$ *must interpret the function symbols* $\mathsf{0}$, s, d, a, m *and* q *as follows:*

$$\mathsf{0}_{\mathbb{N}} = 0 \qquad \mathsf{s}_{\mathbb{N}}(x) = x+1 \qquad \mathsf{a}_{\mathbb{N}}(x,y) = x+y$$
$$\mathsf{d}_{\mathbb{N}}(x) = 2x \qquad \mathsf{m}_{\mathbb{N}}(x,y) = xy+x+y \qquad \mathsf{q}_{\mathbb{N}}(x) = x^2$$

Proof. Compatibility with (A) implies

$$\deg(\mathsf{g}_{\mathbb{N}}) \cdot \deg(\mathsf{s}_{\mathbb{N}}) \geqslant \deg(\mathsf{s}_{\mathbb{N}})^2 \cdot \deg(\mathsf{g}_{\mathbb{N}})$$

This is only possible if $\deg(\mathsf{s}_{\mathbb{N}}) \leqslant 1$. Together with the strict monotonicity of $\mathsf{s}_{\mathbb{N}}$ we obtain $\deg(\mathsf{s}_{\mathbb{N}}) = 1$. Hence s must be interpreted by a linear polynomial: $\mathsf{s}_{\mathbb{N}}(x) = s_1 x + s_0$ with $s_1 \geqslant 1$ and $s_0 \geqslant 0$. The same reasoning applied to (B) yields $\mathsf{g}_{\mathbb{N}}(x) = g_1 x + g_0$ for some $g_1 \geqslant 1$ and $g_0 \geqslant 0$. The compatibility constraint imposed by rule (A) further gives rise to the inequality

$$g_1 s_1 x + g_1 s_0 + g_0 > g_1 s_1^2 x + g_0 s_1^2 + s_1 s_0 + s_0 \tag{1}$$

for all $x \in \mathbb{N}$. Since $s_1 \geqslant 1$ and $g_1 \geqslant 1$, this only holds if $s_1 = 1$. Simplifying (1) we obtain $g_1 s_0 > 2s_0$, which implies $s_0 > 0$ and $g_1 > 2$. If $\mathsf{q}_{\mathbb{N}}$ were linear, the same reasoning could be applied to (B) resulting in $g_1 = 1$, contradicting $g_1 > 2$. Hence $\mathsf{q}_{\mathbb{N}}$ is at least quadratic.

Next we turn our attention to the rewrite rules (C) – (F). Because $\mathsf{g}_{\mathbb{N}}$ is linear, compatibility with (C) and strict monotonicity of $\mathsf{a}_{\mathbb{N}}$ ensures $\deg(\mathsf{a}_{\mathbb{N}}) = 1$. Hence, $\mathsf{a}_{\mathbb{N}} = a_2 x + a_1 y + a_0$ with $a_2 \geqslant 1$, $a_1 \geqslant 1$ and $a_0 \geqslant 0$. From compatibility with rules (D) and (E) we obtain $a_1 = 1$ and $a_2 = 1$. Using the current shapes of $\mathsf{a}_{\mathbb{N}}$, $\mathsf{g}_{\mathbb{N}}$ and $\mathsf{s}_{\mathbb{N}}$, compatibility with rule (F) yields the inequality $\mathsf{g}_{\mathbb{N}}(x) + a_0 > \mathsf{q}_{\mathbb{N}}(x + s_0) - \mathsf{q}_{\mathbb{N}}(x)$ for all $x \in \mathbb{N}$. This can only be the case if $\deg(\mathsf{g}_{\mathbb{N}}(x) + a_0) \geqslant \deg(\mathsf{q}_{\mathbb{N}}(x + s_0) - \mathsf{q}_{\mathbb{N}}(x))$, which in turn simplifies to $1 \geqslant \deg(\mathsf{q}_{\mathbb{N}}(x)) - 1$. Hence $\mathsf{q}_{\mathbb{N}}(x) = q_2 x^2 + q_1 x + q_0$ with $q_2 \geqslant 1$. From monotonicity we also have $\mathsf{q}_{\mathbb{N}}(1) > \mathsf{q}_{\mathbb{N}}(0)$, which leads to $q_2 + q_1 \geqslant 1$.

To further constrain $\mathsf{s}_{\mathbb{N}}$ we consider the rewrite rule (G). The compatibility constraint gives rise to

$$\begin{aligned}
\mathsf{0}_{\mathbb{N}} + 2s_0 &> q_2(\mathsf{0}_{\mathbb{N}} + s_0)^2 + q_1(\mathsf{0}_{\mathbb{N}} + s_0) + q_0 \\
&= q_2\,\mathsf{0}_{\mathbb{N}}^2 + q_2 s_0^2 + \mathsf{0}_{\mathbb{N}}(2q_2 s_0 + q_1) + q_1 s_0 + q_0 \\
&\geqslant q_2 s_0^2 + \mathsf{0}_{\mathbb{N}} + (1 - q_2)s_0 && (q_2 + q_1 \geqslant 1 \text{ and } q_0, q_2, s_0 \geqslant 1) \\
&= q_2 s_0(s_0 - 1) + \mathsf{0}_{\mathbb{N}} + s_0 \\
&\geqslant s_0^2 + \mathsf{0}_{\mathbb{N}} && (s_0 \geqslant 1)
\end{aligned}$$

Hence the inequality $2s_0 > s_0^2$ holds, which is only true if $s_0 = 1$. Therefore $\mathsf{s}_{\mathbb{N}}(x) = x + 1$. Compatibility with (D) now amounts to $x + 1 > \mathsf{0}_{\mathbb{N}} + x + a_0$, which implies $\mathsf{0}_{\mathbb{N}} = a_0 = 0$. At this point we have uniquely constrained $\mathsf{0}_{\mathbb{N}}$, $\mathsf{s}_{\mathbb{N}}$ and $\mathsf{a}_{\mathbb{N}}$. To fully constrain $\mathsf{q}_{\mathbb{N}}$ we turn to (H), which implies $q_0 = 0$, the rules (G) and (I), which together imply $2 > \mathsf{q}_{\mathbb{N}}(1) > 0$ and thus $\mathsf{q}_{\mathbb{N}}(1) = q_2 + q_1 = 1$, and the rules (J) and (K), which imply $5 > \mathsf{q}_{\mathbb{N}}(2) > 3$ and thus $\mathsf{q}_{\mathbb{N}}(2) = 4q_2 + 2q_1 = 4$. Consequently, $q_2 = 1$ and $q_1 = 0$. Hence $\mathsf{q}_{\mathbb{N}}(x) = x^2$. Compatibility with the rules (L) and (M) yields $x + x + 1 > \mathsf{d}_{\mathbb{N}}(x)$ and $\mathsf{d}_{\mathbb{N}}(x) + 1 > x + x$ which imply $\mathsf{d}_{\mathbb{N}}(x) = 2x$. Finally, compatibility with the rules (N) and (O) amounts to $(x + y)^2 + 2x + 2y + 1 > x^2 + y^2 + 2\,\mathsf{m}_{\mathbb{N}}(x, y) \geqslant (x + 1)^2 + 2x + 2y$, which uniquely determines $\mathsf{m}_{\mathbb{N}}(x, y) = xy + x + y$. ◀

Using the previously fixed interpretations we can now add new function symbols, and more easily mandate their interpretations. By adding the two rules

$$\mathsf{s}(t) \to u \qquad\qquad \mathsf{s}(u) \to t$$

for some terms t and u, we enforce an equality constraint on the interpretations of t and u, assuming the system remains polynomially terminating.

To represent the exponents in the polynomial P we add symbols p_i for $1 \leqslant i \leqslant n$, where n is the maximal exponent in P. To fix $(\mathsf{p}_i)_{\mathbb{N}}(x) = x^i$, we add two rules per symbol, according to the following definition.

▶ **Definition 3.** *We define a family of* TRS*s* $(\mathcal{R}_n)_{n\geqslant 0}$ *as follows:*

$$\mathcal{R}_0 = \mathcal{R}$$
$$\mathcal{R}_1 = \mathcal{R}_0 \cup \{\mathsf{s}(\mathsf{p}_1(x)) \to x,\ \mathsf{s}(x) \to \mathsf{p}_1(x)\}$$
$$\mathcal{R}_{n+1} = \mathcal{R}_n \cup \left\{\begin{aligned} \mathsf{s}(\mathsf{a}(\mathsf{p}_{n+1}(x), \mathsf{a}(x, \mathsf{p}_n(x)))) &\to \mathsf{m}(x, \mathsf{p}_n(x)) \\ \mathsf{s}(\mathsf{m}(x, \mathsf{p}_n(x))) &\to \mathsf{a}(\mathsf{p}_{n+1}(x), \mathsf{a}(x, \mathsf{p}_n(x)))\end{aligned}\right\}$$

▶ **Lemma 4.** *For any* $n \geqslant 0$*, the* TRS $\mathcal{R}_n$ *is polynomially terminating over* $\mathbb{N}$ *if and only if* $(\mathsf{p}_i)_\mathbb{N}(x) = x^i$ *for all* $1 \leqslant i \leqslant n$*.*

Proof. From Lemma 1 we know that $\mathcal{R}$ is polynomially terminating and the interpretations are unique due to Lemma 2. Hence the Lemma holds for $\mathcal{R}_0$. For $n \geqslant 1$, the *if* direction holds, since the interpretations $(\mathsf{p}_i)_\mathbb{N}$ are monotone and the polynomial interpretation is compatible with $\mathcal{R}_n$:

$$x + 1 > x \qquad\qquad x + 1 > x$$

for $\mathcal{R}_1 \setminus \mathcal{R}_0$ and

$$x^n + x + x^{n-1} + 1 > xx^{n-1} + x + x^{n-1} \qquad xx^{n-1} + x + x^{n-1} + 1 > xx^n + x + x^{n-1}$$

for $\mathcal{R}_n \setminus \mathcal{R}_{n-1}$. For the *only if* direction we show that compatibility with the additional rules implies $(\mathsf{p}_i)_\mathbb{N}(x) = x^i$ for all $1 \leqslant i \leqslant n$. This is done by induction on n. For $n = 1$ the two rules in $\mathcal{R}_1 \setminus \mathcal{R}$ enforce $(\mathsf{p}_i)_\mathbb{N}(x) + 1 > x$ and $x + 1 > (\mathsf{p}_i)_\mathbb{N}(x)$. Hence $(\mathsf{p}_i)_\mathbb{N}(x) = x$. For $n > 1$ the rules in $\mathcal{R}_n \setminus \mathcal{R}_{n-1}$ enforce $(\mathsf{p}_n)_\mathbb{N}(x) = x \cdot (\mathsf{p}_{n-1})_\mathbb{N}(x)$ by the same reasoning. From the induction hypothesis we obtain $(\mathsf{p}_{n-1})_\mathbb{N}(x) = x^{n-1}$ and hence $(\mathsf{p}_n)_\mathbb{N} = x^n$ as desired. ◀

The fixed interpretations can now be used to construct arbitrary polynomials. Since non-monotone operations, such as subtraction (negative coefficients) and multiplication, cannot serve as interpretations for function symbols, we model these using the difference of two terms. In the following we write $[t]_\mathbb{N}$ for the polynomial that is the interpretation of the term t, according to the interpretations stated in Lemmata 2 and 4.

▶ **Lemma 5.** *For any monomial* $M = cx_1^{i_1} \cdots x_m^{i_m}$ *with* $i_1, \ldots, i_m > 0$ *and* $c \neq 0$ *there exist terms* ℓ_M *and* r_M *over the signature of* $\mathcal{R}_{\mathsf{max}(0,i_1,\ldots,i_m)}$*, such that* $M = [\ell_M]_\mathbb{N} - [r_M]_\mathbb{N}$ *and* $\mathcal{V}\mathsf{ar}(\ell_M) = \mathcal{V}\mathsf{ar}(r_M)$*.*

Proof. First we assume the coefficient c is positive. We construct ℓ_M and r_M by induction on m. If $m = 0$ then $M = c$ and we take $\ell_M = \mathsf{s}^c(\mathsf{0})$ and $r_M = \mathsf{0}$. We trivially have $\mathcal{V}\mathsf{ar}(\ell_M) = \varnothing = \mathcal{V}\mathsf{ar}(r_M)$ and $[\ell_M]_\mathbb{N} - [r_M]_\mathbb{N} = c - 0 = M$. For $m > 0$ we have $M = M'x_m^{i_m}$ with $M' = cx_1^{i_1} \cdots x_{m-1}^{i_{m-1}}$. The induction hypothesis yields terms $\ell_{M'}$ and $r_{M'}$ with $M' = [\ell_{M'}]_\mathbb{N} - [r_{M'}]_\mathbb{N}$ and $\mathcal{V}\mathsf{ar}(\ell_{M'}) = \mathcal{V}\mathsf{ar}(r_{M'})$. Hence

$$\begin{aligned} M = M'x_m^{i_m} &= [\ell_{M'}]_\mathbb{N} x_m^{i_m} - [r_{M'}]_\mathbb{N} x_m^{i_m} \\ &= (\mathsf{m}_\mathbb{N}([\ell_{M'}]_\mathbb{N}, x_m^{i_m}) - [\ell_{M'}]_\mathbb{N} - x_m^{i_m}) - (\mathsf{m}_\mathbb{N}([r_{M'}]_\mathbb{N}, x_m^{i_m}) - [r_{M'}]_\mathbb{N} - x_m^{i_m}) \\ &= (\mathsf{m}_\mathbb{N}([\ell_{M'}]_\mathbb{N}, (\mathsf{p}_j)_\mathbb{N}(x_m)) + [r_{M'}]_\mathbb{N}) - (\mathsf{m}_\mathbb{N}([r_{M'}]_\mathbb{N}, (\mathsf{p}_j)_\mathbb{N}(x_m)) + [\ell_{M'}]_\mathbb{N}) \end{aligned}$$

and thus we can take $\ell_M = \mathsf{a}(\mathsf{m}(\ell_{M'}, \mathsf{p}_j(x_m)), r_{M'})$ and $r_M = \mathsf{a}(\mathsf{m}(r_{M'}, \mathsf{p}_j(x_m)), \ell_{M'})$. Note that $\mathcal{V}\mathsf{ar}(\ell_M) = \mathcal{V}\mathsf{ar}(\ell_{M'}) \cup \{x_m\} \cup \mathcal{V}\mathsf{ar}(r_{M'}) = \mathcal{V}\mathsf{ar}(r_M)$.

If $c < 0$ then we take $\ell_M = r_{-M}$ and $r_M = \ell_{-M}$. We obviously have $\mathcal{V}\mathsf{ar}(\ell_M) = \mathcal{V}\mathsf{ar}(r_{-M}) = \mathcal{V}\mathsf{ar}(\ell_{-M}) = \mathcal{V}\mathsf{ar}(r_M)$. Moreover, $M = -(-M) = -([\ell_{-M}]_\mathbb{N} - [r_{-M}]_\mathbb{N}) = -([r_M]_\mathbb{N} - [\ell_M]_\mathbb{N}) = [\ell_M]_\mathbb{N} - [r_M]_\mathbb{N}$. ◀

▶ **Definition 6.** *Let $P = M_1 + \cdots + M_{k-1} + M_k \in \mathbb{Z}[x_1, \ldots, x_n]$ be a sum of monomials. We denote by ℓ_P the term $\mathsf{a}(\ell_1, \cdots \mathsf{a}(\ell_{k-1}, \ell_k) \cdots)$ and by r_P the term $\mathsf{a}(r_1, \cdots \mathsf{a}(r_{k-1}, r_k) \cdots)$. Here ℓ_i and r_i are the terms from applying Lemma 5 to M_i for $1 \leqslant i \leqslant k$. Moreover, $\ell_0 = r_0 = \mathsf{0}$. We define the* TRS $\mathcal{R}_P$ *as the extension of $\mathcal{R}_n$ with the single rule $\ell_P \to r_P$. Here n is the maximal exponent occurring in P.*

Note that the rewrite rule $\ell_P \to r_P$ in $\mathcal{R}_P$ is well-defined; ℓ_P is not a variable and $\mathcal{V}\mathsf{ar}(\ell_P) = \mathcal{V}\mathsf{ar}(r_P)$ as a consequence of Lemma 5.

▶ **Example 7.** The polynomial $P = 2x^2y - xy + 3$ is first split into its monomials $M_1 = 2x^2y$, $M_2 = -xy$ and $M_3 = 3$. Hence we obtain the TRS $\mathcal{R}_{P_1} = \mathcal{R}_2 \cup \{\mathsf{a}(\ell_{M_1}, \mathsf{a}(\ell_{M_2}, \ell_{M_3})) \to \mathsf{a}(r_{M_1}, \mathsf{a}(r_{M_2}, r_{M_3}))\}$, where

$$\ell_{M_1} = \mathsf{a}(\mathsf{m}(\underbrace{\mathsf{a}(\mathsf{m}(\mathsf{s}^2(\mathsf{0}), \mathsf{p}_2(x)), \mathsf{0})}_{\ell_{2x^2}}, \mathsf{p}_1(y)), \underbrace{\mathsf{a}(\mathsf{m}(\mathsf{0}, \mathsf{p}_2(x)), \mathsf{s}^2(\mathsf{0}))}_{r_{2x^2}})$$

$$r_{M_1} = \mathsf{a}(\mathsf{m}(\underbrace{\mathsf{a}(\mathsf{m}(\mathsf{0}, \mathsf{p}_2(x)), \mathsf{s}^2(\mathsf{0}))}_{r_{2x^2}}, \mathsf{p}_1(y)), \underbrace{\mathsf{a}(\mathsf{m}(\mathsf{s}^2(\mathsf{0}), \mathsf{p}_2(x)), \mathsf{0})}_{\ell_{2x^2}})$$

$$\ell_{M_2} = \mathsf{a}(\mathsf{m}(\underbrace{\mathsf{a}(\mathsf{m}(\mathsf{0}, \mathsf{p}_1(x)), \mathsf{s}(\mathsf{0}))}_{r_x}, \mathsf{p}_1(y)), \underbrace{\mathsf{a}(\mathsf{m}(\mathsf{s}(\mathsf{0}), \mathsf{p}_1(x)), \mathsf{0})}_{\ell_x})$$

$$r_{M_2} = \mathsf{a}(\mathsf{m}(\underbrace{\mathsf{a}(\mathsf{m}(\mathsf{s}(\mathsf{0}), \mathsf{p}_1(x)), \mathsf{0})}_{\ell_x}, \mathsf{p}_1(y)), \underbrace{\mathsf{a}(\mathsf{m}(\mathsf{0}, \mathsf{p}_1(x)), \mathsf{s}(\mathsf{0}))}_{r_x})$$

$$\ell_{M_3} = \mathsf{s}^3(\mathsf{0}) \qquad r_{M_3} = \mathsf{0}$$

Note that in the terms ℓ_{M_2} and r_{M_2} the ℓ and r of the recursive call are switched since M_2 has a negative coefficient.

▶ **Theorem 8.** *For any polynomial $P \in \mathbb{Z}[x_1, \ldots, x_n]$, the* TRS $\mathcal{R}_P$ *is polynomially terminating over $\mathbb{N}$ if and only if $P(x_1, \ldots, x_n) > 0$ for all $x_1, \ldots, x_n \in \mathbb{N}$.*

Proof. First suppose $\mathcal{R}_P$ is polynomially terminating over $\mathbb{N}$. So there exists a monotone polynomial interpretation in $(\mathbb{N}, >)$ that orients the rules of $\mathcal{R}_P$ from left to right. Let n be the maximum exponent in P. From Lemma 2 and Lemma 4 we infer that the interpretations of the function symbols $\mathsf{0}$, s, a, m, and p_i for $1 \leqslant i \leqslant n$ are fixed such that, according to Lemma 5, $P = [\ell_P]_\mathbb{N} - [r_P]_\mathbb{N}$. Since the rule $\ell_P \to r_P$ belongs to $\mathcal{R}_P$, $P(x_1, \ldots, x_n) > 0$ for all $x_1, \ldots, x_n \in \mathbb{N}$ by compatibility.

For the if direction, we assume that $P \in \mathbb{Z}[x_1, \ldots, x_n]$ satisfies $P(x_1, \ldots, x_n) > 0$ for all $x_1, \ldots, x_n \in \mathbb{N}$. By construction of $\ell_P \to r_P$ and Lemma 5, the interpretations in Lemma 2 and Lemma 4 orient the rule $\ell_P \to r_P$ from left to right. The same holds for rules $\mathcal{R}_n$. Hence $\mathcal{R}_P$ is polynomially terminating over $\mathbb{N}$. ◀

▶ **Corollary 9.** *It is undecidable whether a finite* TRS *is polynomially terminating over $\mathbb{N}$.*

3 Conclusion

We proved the undecidability of polynomial termination over the natural numbers, by a reduction from a variant of Hilbert's 10th problem. This was done by constructing a TRS R_P, for any polynomial $P \in \mathbb{Z}[x_1, \ldots, x_n]$, which can be shown to be polynomially terminating if and only if $P(x_1, \ldots, x_n) > 0$ for all $x_1, \ldots, x_n \in \mathbb{N}$. To construct this system we used techniques from [5] to fix the interpretation of function symbols. Using the fixed interpretations we constructed two terms ℓ_P and r_P, such that $P = [\ell_P]_\mathbb{N} - [r_P]_\mathbb{N}$. This allowed us to encode the inequality $P > 0$ as the compatibility constraint associated with the rule $\ell_P \to r_P$.

In our proof we allow interpretations to be polynomials with integer coefficients. However, it equally applies if interpretations are limited to natural number coefficients, since the construction stays the same. We conclude the paper by mentioning two open questions.

1. Is polynomial termination over $\mathbb{N}$ decidable for terminating TRSs?

   The construction in this paper may produce non-terminating systems. Take for example the polynomial $P_1 = -1$. The resulting TRS $\mathcal{R}_{P_1} = \mathcal{R} \cup \{\mathsf{0} \to \mathsf{s}(\mathsf{0})\}$ is obviously not terminating.

2. Is incremental polynomial termination over $\mathbb{N}$, where we take the lexicographic extension of the order induced by the polynomial interpretations, decidable?

   We expect the answer is negative, but the construction in this paper needs to be modified. Consider for instance the polynomial $P_2 = x$. We obtain $\ell_{P_2} = \mathsf{a}(\mathsf{m}(\mathsf{s}(\mathsf{0}), \mathsf{p}_1(x)), \mathsf{0})$ and $r_{P_2} = \mathsf{a}(\mathsf{m}(\mathsf{0}, \mathsf{p}_1(x)), \mathsf{s}(\mathsf{0}))$. As a result, the TRS $\mathcal{R}_{P_2}$ is not polynomially terminating since $[\ell_{P_2}]_{\mathbb{N}} = 2x + 1 \not> x + 1 = [r_{P_2}]_{\mathbb{N}}$ for $x = 0$. However, if we take a second algebra $\mathcal{A}$ over $\mathbb{N}$ where the interpretation of m is changed to $\mathsf{m}_{\mathcal{A}}(x, y) = 2x + y$, then $[\ell_{P_2}]_{\mathcal{A}} = x + 2 > x + 1 = [r_{P_2}]_{\mathcal{A}}$ for all $x \in \mathbb{N}$. Hence the lexicographic order $(>_{\mathbb{N}}, >_{\mathcal{A}})$ is a reduction order compatible with $\mathcal{R}_{P_2}$.

References

1 Franz Baader and Tobias Nipkow. *Term Rewriting and All That.* Cambridge University Press, 1998. doi:10.1017/CBO9781139172752.

2 Ahlem Ben Cherifa and Pierre Lescanne. Termination of rewriting systems by polynomial interpretations and its implementation. *Science of Computer Programming*, 9(2):137–159, 1987. doi:10.1016/0167-6423(87)90030-X.

3 Dieter Hofbauer and Clemens Lautemann. Termination proofs and the length of derivations (preliminary version). In *Proceedings of the 3rd International Conference on Rewriting Techniques and Applications*, volume 355 of *Lecture Notes in Computer Science*, pages 167–177, 1989. doi:10.1007/3-540-51081-8_107.

4 Dallas Lankford. On proving term rewrite systems are noetherian. Technical Report MTP-3, Louisiana Technical University, Ruston, LA, USA, 1979.

5 Friedrich Neurauter and Aart Middeldorp. Polynomial interpretations over the natural, rational and real numbers revisited. *Logical Methods in Computer Science*, 10(3:22):1–28, 2014. doi:10.2168/LMCS-10(3:22)2014.

6 Hans Zantema. Termination. In *Term Rewriting Systems*, chapter 6, pages 181–259. Cambridge University Press, 2003.