Elementary Interpretations of NP vs. P

L. Gordeev A. Krebs

Tübingen University

Abstract

We translate the P/poly vs. NP problem into algebraic environment. This is done by expressing the computation of a non-uniform polynomial time machine in terms of polynomial sized systems of linear equations (or algebraic polynomials) over real vector spaces (respectively finite fields). We reduce the question whether the co-NP complete TAU3-problem is in P/poly to the question whether the set of solutions of an exponentially sized system of linear equations (algebraic polynomial) is that of a polynomial sized system (polynomial).

1 Introduction

In the paper we examine the open problem $\mathbf{NP} \subset \mathbf{P/poly}$. In particular, we consider the question whether the co-NP-complete problem $\mathbf{TAU3} \in \mathbf{P/poly}$, where **TAU3** is the set of all tautologies in 3-DNF, and construct the desired algebraic characterizations **C3L** and **C3F** (see Conditions 36, 43 in the text). Now **C3L** and **C3F** both restate the open problems $\mathbf{NP} \subset \mathbf{P/poly}$ and $\mathbf{NP} \neq \mathbf{P}$ as purely algebraic questions over real vector spaces and finite fields, respectively. To put it more exactly, we prove that **C3L** (**C3F**) infers $\mathbf{NP} \neq \mathbf{P}$, whereas non-**C3L** (non-**C3F**) infers $\mathbf{NP} \subset \mathbf{P/poly}$ (see Theorems 37, 38, 44, Corollary 45 and Remark 46 in the text).

Loosely speaking, **C3L** (respectively **C3F**) characterizes **P** (in fact **P/poly**) vs. **NP** question as classical algebraic question about zero-sets of "small" vs. "large" systems of linear equations in the real spaces (respectively polynomials in the finite field domains). To this end, we introduce two algebraic measures of complexity - *graph-complexity* (a.k.a. *circuit-complexity*) and *norm-complexity*.

Email addresses: gordeew@informatik.uni-tuebingen.de (L. Gordeev), mail@krebs-net.de (A. Krebs).

The former provides us with purely syntactical characteristics of a term describing a computation, whereas the latter one refers to the bounds of the term's computational features.

In order to make the transition from computations to these algebraic conditions, we use an intermediate condition **C3** (see Condition 18 in the text) having special combinatorial ingredients given by the "definition-by-cases" operation. We prove that **C3** infers $\mathbf{NP} \neq \mathbf{P}$, whereas non-**C3** infers $\mathbf{NP} \subset \mathbf{P/poly}$ (see Condition 18 and Theorems 21, 22 in the text). To this end, our first step converts computations into **C3**, while using a special quasi-algebraic polynomial, or *quasi-polynomial*, $\Phi_n^?$ (see Definition 3 in the text) that characterizes TAU3 problem in the algebraic language extended by the "definition-by-cases" operation.

The second step is crucial for the proof - there we remove the combinatorial ingredient that is still used by **C3**, namely the "definition-by-cases". To achieve this goal, we on one hand investigate the topological structure of the set of solutions to the TAU3-problem and use induction over the term structure to eliminate "definition-by-cases", which results in the characterization **C3L**. On the other hand, instead of using the real numbers, we develop the corresponding characterizations over finite fields or the complex numbers and replace "definition-by-cases" by multiplication, which results in the characterization **C3F**. In contrast to the familiar first-order characteriazations leading to Bounded Arithmetic and related proof-theoretical open problems, ours are elementary-algebraic (in the sense of Tarski), in that they refer to algebraic structures whose algebraic semantic does not require quantifiers. This allows us to hope that well-developed methods of linear algebra, algebraic geometry and/or finite fields can better contribute to the desired solution of the open problem $\mathbf{NP} \subset \mathbf{P/poly}$ and/or $\mathbf{NP} \neq \mathbf{P}$.

Our paper is structured as follows. In section 2 we introduce the *quasi-polynomials* that are used in **C3**. Section 3 contains the definitions and examples of our measures of complexity. The translation from Turing machines to condition **C3** is done in section 4, and elimination of the "definition-by-cases"is presented in section 5. In the final two section we consider characterizations over the complex numbers (these are not properly elaborated yet) and finite fields, respectively. Sections 1, 6, 7 and many simplifications of the basic formalisms are due to the second author, other parts are elaborated by the first author.

Note: It turns out that **C3L** can be further reduced to purely combinatorial Ramsey-style conditions which are sufficient for $\mathbf{NP} \neq \mathbf{P}$. This work will be presented elsewhere.

2 Preliminaries

Symbol	Meaning
$\mathbb{N}$	$\{0, 1, 2, \cdots\}$ the natural numbers
$\mathbb{N}^+$	$\{1, 2, \cdots\}$ the positive natural numbers
$\mathbb{P}$	the prime numbers
$\mathbb{N}_{\lvert m\rvert}$	$\{x \in \mathbb{N} : x \leq m\}$
$\mathbb{Z}$	the integers
$\mathbb{Z}_{\lvert m\rvert}$	$\{x \in \mathbb{Z} : \lvert x\rvert \leq m\}$
$\mathbb{Z}_n$	$\mathbb{Z}/n\mathbb{Z}$
$\mathbb{R}$	the reals
$\mathbb{C}$	the complex numbers
$K[x_1, \cdots, x_\ell]$	the polynomials in $x_1, \cdots, x_\ell$ over K
$K^{(1)}[x_1, \cdots, x_\ell]$	$\{f \in K[x_1, \cdots, x_\ell] : \deg(f) \leq 1\}$ the linear polynomials (vectors) in $x_1, \cdots, x_\ell$ over K
$[\![\alpha_1, \cdots, \alpha_m]\!]$	the linear combinations of $\alpha_1, \cdots, \alpha_m \in K[x_1, \cdots, x_\ell]$

Definition 1 ***Basic languages*** $\mathcal{L}^?$, $\mathcal{L}^?_n$. *The algebraic language* $\mathcal{L}^?$ *includes:*

(1) variables
(2) one constant 1
(3) three binary operations $+$, $-$, $?$

As for parentheses, we adopt usual abbreviations concerning $+$ *and* $-$*, and assume that* $?$ *has priority over* $+$ *and* $-$*; thus e.g. a term* $x?y?z + u?z - v?w$ *is understood as* $((x?(y?z)) + (u?z)) - (v?w)$.

Terms of $\mathcal{L}^?$ *are called* ***quasi-polynomials****. Any quasi-polynomial with at most* m *distinct variables is also called* m*-ary quasi-polynomial. By adding zero-summands* $x - x$ *for failing variables* x *we can just as well assume that* m*-ary quasi-polynomials contain exactly* m *distinct variables.*

For any $n \in \mathbb{N}^+$*, denote by* $\mathcal{L}^?_n$ *the* ***sublanguage*** *of* $\mathcal{L}^?$ *that contains only* $3n$ *variables* $\{x_{i,j} \mid 0 < i \leq 3 \wedge 0 < j \leq n\}$*. By a natural renaming* $x_{i,j} \rightleftharpoons x_{i+3(j-1)}$ *we can just as well consider the list of* $\mathcal{L}^?_n$*-variables* $\{x_k \mid 0 < k \leq 3n\}$*. It is assumed that* $+$ *is associative and commutative, while* $?$ *being only associative (see the definition and lemma below).*

Thus arbitrary terms of $\mathcal{L}_n^?$ are $3n$-ary quasi-polynomials. In $\mathcal{L}^?$ ($\mathcal{L}_n^?$), we let 0 and $-x$ be abbreviations of quasi-polynomials $1-1$ and $(1-1)-x$, respectively.

Definition 2 *The following $\Phi_n^?$ is a $3n$-ary quasi-polynomial, where $[\mathbf{n} \to \mathbf{3}] :=$ the set of all functions from $\mathbf{n} := \{1, \cdots, n\}$ to $\mathbf{3} := \{1, 2, 3\}$.*

$$\Phi_n^? := \sum_{f \in [\mathbf{n} \to \mathbf{3}]} \left(\mathop{?}_{i \leq j \in \mathbf{n}} \left(x_{f(i),i} + x_{f(j),j} \right) \right) ?1$$

Example 3 *For $n = 2$ this yields:*

$$\begin{aligned}
\Phi_2^? = {} & (x_{1,1} + x_{1,1})?\,(x_{1,2} + x_{1,2})?\,(x_{1,1} + x_{1,2})?1 \\
& + (x_{1,1} + x_{1,1})?\,(x_{2,2} + x_{2,2})?\,(x_{1,1} + x_{2,2})?1 \\
& + (x_{1,1} + x_{1,1})?\,(x_{3,2} + x_{3,2})?\,(x_{1,1} + x_{3,2})?1 \\
& + (x_{2,1} + x_{2,1})?\,(x_{1,2} + x_{1,2})?\,(x_{2,1} + x_{1,2})?1 \\
& + (x_{2,1} + x_{2,1})?\,(x_{2,2} + x_{2,2})?\,(x_{2,1} + x_{2,2})?1 \\
& + (x_{2,1} + x_{2,1})?\,(x_{3,2} + x_{3,2})?\,(x_{2,1} + x_{3,2})?1 \\
& + (x_{3,1} + x_{3,1})?\,(x_{1,2} + x_{1,2})?\,(x_{3,1} + x_{1,2})?1 \\
& + (x_{3,1} + x_{3,1})?\,(x_{2,2} + x_{2,2})?\,(x_{3,1} + x_{2,2})?1 \\
& + (x_{3,1} + x_{3,1})?\,(x_{3,2} + x_{3,2})?\,(x_{3,1} + x_{3,2})?1
\end{aligned}$$

And for $n = 3$:

$$\begin{aligned}
\Phi_3^? = {} & (x_{1,1} + x_{1,1})?\,(x_{1,2} + x_{1,2})?\,(x_{1,3} + x_{1,3}) \\
& ?\,(x_{1,1} + x_{1,2})?\,(x_{1,1} + x_{1,3})?\,(x_{1,2} + x_{1,3})?1 \\
& + (x_{1,1} + x_{1,1})?\,(x_{1,2} + x_{1,2})?\,(x_{2,3} + x_{2,3}) \\
& ?\,(x_{1,1} + x_{1,2})?\,(x_{1,1} + x_{2,3})?\,(x_{1,2} + x_{2,3})?1 \\
& \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \\
& + (x_{3,1} + x_{3,1})?\,(x_{3,2} + x_{3,2})?\,(x_{2,3} + x_{2,3}) \\
& ?\,(x_{3,1} + x_{3,2})?\,(x_{3,1} + x_{2,3})?\,(x_{3,2} + x_{2,3})?1 \\
& + (x_{3,1} + x_{3,1})?\,(x_{3,2} + x_{3,2})?\,(x_{3,3} + x_{3,3}) \\
& ?\,(x_{3,1} + x_{3,2})?\,(x_{3,1} + x_{3,3})?\,(x_{3,2} + x_{3,3})?1
\end{aligned}$$

Definition 4 ***Semantics.*** *A structure D of signature $\langle 1, +, - \rangle$ is called* ***basic domain*** *iff D is an abelian group with respect to $+$ and $0 := 1 - 1$ such that $1 \neq 0$ and $x - y = x + (-y) = x + y^{-1}$. In any basic domain D, we extend basic signature $\langle +, -, 1 \rangle$ to the required $\mathcal{L}^?$ -signature $\langle +, -, ?, 1 \rangle$ by setting*

$$x?y := \begin{cases} 0 & \text{if} \quad x = 0 \\ y & \text{if} \quad x \neq 0 \end{cases}$$

An integral domain (hence basic domain) D such that either $\mathrm{char}\,(D) = 0$ or else $\mathrm{char}\,(D) > m$ is called m -ary normal domain (or just ***normal domain****, if m is clear from the context). Furthermore, we call m-ary* ***normed domain*** *any m-ary normal domain D supplied with an additive norm $\| \,.\, \| : D \to \mathbb{R}$*

that satisfies 1-5 below.

(1) $\| 0\| = 0$
(2) $x \neq 0 \to \| x \| > 0$
(3) $\| x + y \| \leq \| x \| + \| y\|$
(4) $\|-x \| = \| x \|$
(5) $\underbrace{\|1 + \cdots + 1\|}_{k} = k \in \mathbb{N}^+$, *provided that* $char\,(D) = 0$ *or else* $k \leq m$.

For any $m \in \mathbb{N}^+$, *denote by* $\mathfrak{D}_m$ *the class of all* m *-ary normed domains.*

Example 5 $\mathbb{Z}$ *and* $\mathbb{R}$ *with standard norm* $\| x\| := |x|$ *and* $\mathbb{C}$ *with standard norm* $\| x + i \cdot y\| := \sqrt{x^2 + y^2}$ *are infinite* m *-ary normed domains, for all* $m \in \mathbb{N}^+$. *Same holds true for standard* k*-dim normed vector spaces* $\mathbb{R}^k$, $\mathbb{C}^k$. $\mathbb{Z}_p$ *with* $\|[x]\| := \left\{ \begin{array}{lll} x & if & 2x < p \\ p - x & else & \end{array} \right\}$ *is a finite* $3n$*- ary normed domain, for any* $\mathbb{P} \ni p > 6n$. *By the same token, so is any finite field of characteristic* $p > 6n$.

Lemma 6 *The following conditions hold in every basic domain* D.

(1) $x?\,(y?z) = (x?y)?z$
(2) $x?\,(y \pm z) = x?y \pm x?z$
(3) $0?x = x?0 = 0$
(4) $1?x = x$
(5) $x?1 = \left\{ \begin{array}{lll} 0 & if & x = 0 \\ 1 & else & \end{array} \right.$
(6) $y + x?\,(z - y) = \left\{ \begin{array}{lll} y & if & x = 0 \\ z & else & \end{array} \right.$
(7) $x?y = 0 \leftrightarrow x = 0 \vee y = 0$
(8) $1 - x?1 = 0 \leftrightarrow x \neq 0$
(9) $x?x + y?y + x?y - y?x = 0 \leftrightarrow x = 0 \wedge y = 0$, *provided that* $D \neq GF(2)$ *is normal.*
(10) $y_1?y_2?\cdots?y_k?1 = \left\{ \begin{array}{lll} 0 & if & y_1 = 0 \vee y_2 = 0 \vee \cdots \vee y_k = 0 \\ 1 & else & \end{array} \right.$
(11) $\Phi_n^? = 0 \leftrightarrow (\forall f \in [\mathbf{n} \to \mathbf{3}])\,(\exists i, j \in \mathbf{n})\left(x_{f(i),i} + x_{f(j),j} = 0\right)$
(12) $\left\langle \mathbb{Z}_{|m|}, +, - \right\rangle$ *is contained (modulo isomorphism) in* D, *provided that* $D \in \mathfrak{D}_m$ *(this embedding must not preserve the norm* $\| \,.\, \|$*).*

Proof. 1-8 are readily seen. 10 follows by 5, 7. 11 follows by 10. Consider 9. By 2, we have

$$x?x+y?y+x?y-y?x=x?\left(x+y\right)+y?\left(y-x\right)$$
$$=\left\{\begin{array}{lll} 0 & \text{if} & x=0 \\ x+y & \text{if} & x\neq 0 \end{array}\right. + \left\{\begin{array}{lll} 0 & \text{if} & y=0 \\ y-x & \text{if} & y\neq 0 \end{array}\right.$$
$$=\left\{\begin{array}{ll} 0 & \text{if} \quad x=0\wedge y=0 \\ y-x=y\neq 0 & \text{if} \quad x=0\wedge y\neq 0 \\ x+y=x\neq 0 & \text{if} \quad x\neq 0\wedge y=0 \\ 2y\neq 0 & \text{if} \quad x\neq 0\wedge y\neq 0 \end{array}\right.$$

since $2y=0\leftrightarrow y=0$ holds in any integral domain $D\neq GF(2)$, and hence

$$x?x+y?y+x?y-y?x=0\leftrightarrow x=0\wedge y=0$$

Consider 12. The required isomorphic embedding $h:\mathbb{Z}_{|m|}\rightarrow D$ is given by

$$h\left(z\right):=\left\{\begin{array}{ll} \underbrace{1+\cdots+1}_{z} & \text{if} \quad z>0 \\ 0 & \text{if} \quad z=0 \\ -h\left(-z\right) & \text{if} \quad z<0 \end{array}\right.$$

□

Corollary 7 ***Quasi-polynomials are closed under boolean operations.*** *To put it more precisely, the following holds. Let F be any propositional formula with atoms $s_1=0,\cdots,s_k=0$, for any quasi-polynomials $s_1,\cdots,s_k$ whose variables occur in the list $\overrightarrow{x}$. There exists a quasi-polynomial t with variables from $\overrightarrow{x}$, such that $F\leftrightarrow t=0$ in every basic domain D. Moreover, if F is positive and 0 does not occur in $s_1,\cdots,s_k$, i.e. $s_1,\cdots,s_k$ are constant-free, then there is a constant-free t as above for which $F\leftrightarrow t=0$ in every field D.*

Proof. This readily follows from 7-9 of the lemma. □

Corollary 8 ***Arbitrary definitions-by-cases are admissible in $\mathcal{L}^?$.*** *That is, let $t_1,\cdots,t_{q+1}$ and $F_1,\cdots,F_q$ be quasi-polynomials and propositional formulas (as above), respectively, whose variables occur in the list $\overrightarrow{x}$. There exists a quasi-polynomial t with variables from $\overrightarrow{x}$, such that in every basic domain D*

$$t=\{\texttt{if } F_1 \texttt{ then } t_1,\texttt{else if } F_2 \texttt{ then } t_2,\ldots,\texttt{else if } F_q \texttt{ then } t_q,\texttt{else } t_{q+1}\}$$

Proof. By induction on q from previous corollary and 6 of the lemma. □

3 Notions of complexity

3.1 Graph-complexity

By the *graph-complexity* of a given algebraic term t we understand the minimal number of vertices of a graph (not necessarily a tree!) that represents t. To put it more exactly, this notion is specified as follows.

Definition 9 ***Graph-complexity.*** *For any given quasi-polynomial t denote by $\partial(t)$ (in words: **graph-complexity** of t) the minimal number of instances of the canonical term-building rules:*

(1) every atom (i.e. a variable or constant) is a term
(2) if s, r are terms then so is $s+r$
(3) if s, r are terms then so is $s-r$
(4) if s, r are terms then so is $s?r$

which are required in order to obtain t. It is readily seen that $\partial(t)$ can be equivalently defined by recursion on the ordinary complexity of t. For the sake of brevity, consider an algebraic language $\mathcal{L}$ with arbitrary binary function symbols, which we denote by f, g, h. Moreover, for any term t of $\mathcal{L}$, denote by $SUB(t)$ the set of all subterms of t (in transitive sense and including t), while as usual $\{\cdots\}$ denote sets, i.e. collections (of terms) modulo permutations and contractions. The recursive clauses in question are as follows.

(1) $\partial(t) := \partial\{t\}$
(2) $\partial\{a_1, \cdots, a_k\} := \#\{a_1, \cdots, a_k\}$, *provided that* $a_1, \cdots, a_k$ *are atoms*
(3) $\partial\{f(s,t), r_1, \cdots, r_k\} := 1 + \partial\{s, t, r_1, \cdots, r_k\}$, *provided that* $f(s,t) \notin SUB(r_1) \cup \cdots \cup SUB(r_k)$

Example 10 *We compute graph-complexity according to the latter definition, where f, g, h and x, y are distinct function symbols and variables, respectively.*

- *Suppose* $t = f(x,x)$. *We have* $\partial(t) = \partial\{t\} = \partial\{f(x,x)\} = 1 + \partial\{x,x\} = 1 + \#\{x,x\} = 1+1 = 2$
- *Suppose* $t = f(x,y)$. *We have* $\partial(t) = \partial\{t\} = \partial\{f(x,y)\} = 1 + \partial\{x,y\} = 1 + \#\{x,y\} = 1+2 = 3$
- *Suppose* $t = f(g(x,h(x,y)), h(x,y))$. *We have* $\partial(t) = \partial\{t\} = \partial\{f(g(x,h(x,y)), h(x,y))\} = 1 + \partial\{g(x,h(x,y)), h(x,y)\} = 2 + \partial\{x, h(x,y), h(x,y)\} = 2 + \partial\{x, h(x,y)\} = 3 + \partial\{x,x,y\} = 3 + \#\{x,y\} = 3+2 = 5$
- *Suppose* $t = f(g(x, f(y, h(x,y))), h(x,y))$. *We have* $\partial(t) = \gamma\{t\} = \partial\{f(g(x, f(y, h(x,y))), h(x,y))\} = 1 + \partial\{g(x, f(y, h(x,y))), h(x,y)\} = 2 + \partial\{x, f(y, h(x,y)), h(x,y)\} = 3 + \partial\{x, y, h(x,y), h(x,y)\} = 3 +$

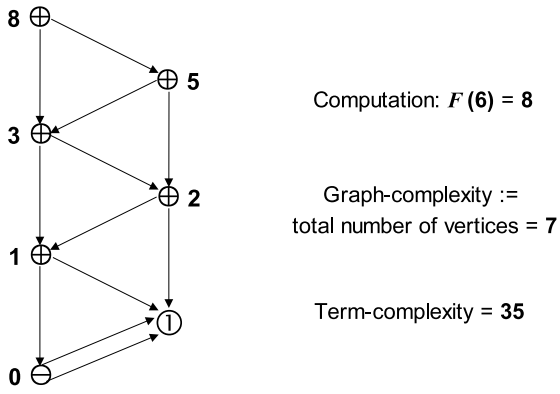

Fig. 1. Graph complexity of the Fibonacci numbers

$$\partial\{x, y, h(x, y)\} = 4 + \partial\{x, y, x, y\} = 4 + \#\{x, y\} = 4 + 2 = 6$$

Remark 11 *Recall that* ***Fibonacci numbers*** *are defined by recursive clauses:*

$$F(0) := 0,\ F(1) := 1,\ F(i+2) := F(i) + F(i+1)$$

Thus $F(i)$ *is the* ith *member in the sequence* $0, 1, 1, 2, 3, 5, 8, \cdots$. *Let* t *be a quasi-polynomial that represents* $F(6) = 8$. *We have*

$$t = (1-1)+1+(1-1)+1+1+(1-1)+1+(1-1)+1+1+(1-1)+1+1$$

and hence the ordinary complexity of t *(= total number of all occurrences of* 1, $+$ *and* $-$*) is* 35. *However, the graph-complexity of* t, $\partial(t)$, *is merely* 7 *(see Figure 1). Furthermore, let* $t(i)$ *be a quasi-polynomial corresponding to* $F(i)$. *By the same token, it is readily seen that the ordinary complexity of* $t(i)$ *is growing exponentially in* $\partial(t(i))$.

Lemma 12 *The graph-complexity of* $\Phi_n^?$ *essentially exceeds* 3^n, *i.e.* $\partial\left(\Phi_n^?\right) \gg 3^n$.

Proof. Strictly speaking, the shape of $\Phi_n^?$ depends on the chosen ordering of $[\mathbf{n} \to \mathbf{3}]$ and $\{\langle i, j\rangle \in \mathbb{N}^2 \mid i \leq j \leq n\}$, as well as the associative order in which $+$ and $?$ are used; this refers to the hidden parentheses in $\Phi_n^?$. However, we wish to merely estimate the lower bound of $\partial\left(\Phi_n^?\right)$. To this end, first observe that for different $f \in [\mathbf{n} \to \mathbf{3}]$ the summands $\left(\mathop{?}_{i \leq j \in \mathbf{n}} \left(x_{f(i),i} + x_{f(j),j}\right)\right)?1$ are different terms which, moreover, do not occur as subterms in the others. Hence different $f \in [\mathbf{n} \to \mathbf{3}]$ have different vertices in any chosen graph-representations of $\Phi_n^?$ (cf. recursive definition of $\partial(t)$, above). This yields $\partial\left(\Phi_n^?\right) \geq \#([\mathbf{n} \to \mathbf{3}]) = 3^n$. Furthermore, with different $a, b \leq 3, i \leq j \leq n$ are associated different terms $x_{a,i} + x_{b,j}$, and hence different vertices in graph-representations of $\Phi_n^?$.

Besides, there are $3n+1$ different atomic vertices for all variables and 1. This yields $\partial\left(\Phi_n^?\right) \geq 3^n + 3^2 \cdot \frac{1}{2}n\left(n-1\right) + 3n + 1 = 3^n + \frac{3}{2}n\left(3n-1\right) + 1$. Finally, there are more than $\frac{1}{2}n\left(n-1\right)-1$ different vertices corresponding to different composite proper subterms of $\underset{i\leq j\in\mathbf{n}}{\overset{?}{}}\left(x_{f(i),i} + x_{f(j),j}\right)$. Summing up, this yields $\partial\left(\Phi_n^?\right) > 3^n + \frac{3}{2}n\left(3n-1\right) + \frac{1}{2}n\left(n-1\right) = 3^n + 5n^2 - 2n \gg 3^n$. $\square$

3.2 Norm-complexity

Definition 13 ***Norm-complexity***. *Consider any m-ary quasi-polynomial $t = t\left(\overrightarrow{x}\right)$ and $D \in \mathfrak{D}_m$. Let $V := D^m$ be the m-dim vector space over D, under extended norm $\|\upsilon\| = \|\upsilon_1, \cdots, \upsilon_m\| := \max\limits_{i\leq m}\|\upsilon_i\|$, for any $\upsilon = (\upsilon_1, \cdots, \upsilon_m) \in V$. Regard $t = t\left(\overrightarrow{x}\right)$ as a functional $t : V \to D$ where $t\left(\upsilon\right) = t\left(\overrightarrow{x} := \overrightarrow{\upsilon}\right)$. With t are correlated two* ***quasi-norms*** $\|t\|_D := \sup\limits_{\|\upsilon\|\geq 1}\frac{\|t(\upsilon)\|}{\|\upsilon\|}$ *and* $\varrho_D\left(t\right) := \max\left\{\|s\|_D \mid s \in SUB\left(t\right)\right\}$. *Furthermore, call* $\varrho\left(t\right) := \sup\limits_{D\in\mathfrak{D}_m}\varrho_D\left(t\right)$ *the* ***norm-complexity*** *of t.*

Lemma 14 *The norm-complexity of $\Phi_n^?$ is 3^n, i.e. $\varrho\left(\Phi_n^?\right) = 3^n$.*

Proof. Consider any $D \in \mathfrak{D}_{3n}$ and notice $\Phi_n^? : V = D^{3n} \to \left\{i \in \mathbb{N} \mid i \leq 3^n\right\}$. Moreover, there are 3^n summands in the term $\Phi_n^?$, which, regardless of the input υ, take values 0 or 1 (see above Lemma 6 (10)). Furthermore, every summand in question is a ? -product, whose subterms take values υ_ι, $\upsilon_\iota + \upsilon_\kappa$, 0 or 1. Hence for any $s \in SUB\left(\Phi_n^?\right)$ we have

$$\|s\|_D \leq \sup_{\|\upsilon\|\geq 1}\frac{\max\left(2\|\upsilon\|, 3^n\right)}{\|\upsilon\|} \leq \max\left(2, \sup_{\|\upsilon\|\geq 1}\frac{3^n}{\|\upsilon\|}\right) \leq 3^n$$

This yields $\varrho_D\left(\Phi_n^?\right) \leq 3^n$. Now let $\upsilon := \underbrace{(1, \cdots, 1)}_{3n}$ and observe that for this input, all summands in $\Phi_n^?$ take the value 1, while $\|\upsilon\| = 1$. Arguing as above, this yields $\left\|\Phi_n^?\right\|_{\mathbb{Z}} \geq \left\|\Phi_n^?\left(\upsilon\right)\right\| = \Phi_n^?\left(\upsilon\right) = 3^n$. Hence $\varrho\left(\Phi_n^?\right) = 3^n$, Q.E.D. $\square$

Remark 15 *The complexities $\partial\left(t\right)$ and $\varrho\left(t\right)$ are mutually incomparable. To put it more precisely, it can happen that $\varrho\left(t\right)$ is exponential in $\partial\left(t\right)$, and vice versa, $\partial\left(t\right)$ can be exponential in $\varrho\left(t\right)$. The former is e.g. the case of a slightly modified Fibonacci sequence (cf. Remark 7 above): $t_1 := 1$, $t_1 := x$, $t_3 := t_1 + t_2$, $\cdots$, $t_{k+2} := t_k + t_{k+1}$, $\cdots$. The latter applies e.g. to the sequence: $t_1 := x - x$, $t_2 := (x-x) + (x-x)$, $\cdots$, $t_{k+1} := (x-x)\underbrace{+\cdots+}_{k}(x-x)$, $\cdots$.*

Definition 16 ***Alebraic complexity***. *Let t be any quasi-polynomial. We call* $\max(\partial(t), \varrho(t))$ *the* ***algebraic complexity*** *(or just* ***complexity****) of t. For any m, $\mathrm{c} \in \mathbb{N}^+$, denote by $\mathfrak{Q}_m^{(\mathrm{c})}$ the set of m-ary quasi-polynomials whose algebraic complexity does not exceed m^{c}.*

The class **P/poly** contains the PTIME Turing machines that get a polynominal size advice that depends only on the size of the input. The exact definition is given in [Ka].

Lemma 17 (Soundness) *There is a Turing machine $\mathcal{M}$ in* **P/poly** *such that the value $t(\mathbf{z}) \in \mathbb{Z}$ is computable by $\mathcal{M}$*

Proof. Recall that by definition we have $\|z_i\| = |z_i|$, and hence $\|\mathbf{z}\| = \max\limits_{1 \le i \le 3n} |z_i|$. Since $\partial(t) \le n^{\mathrm{c}}$, the graph of $t(\mathbf{z})$ has at most n^{c} vertices. Since $\varrho_{\mathbb{Z}}(t) \le \varrho(t) \le n^{\mathrm{c}}$, all vertices of $t(\mathbf{z})$ are supplied with integers $\le \|\mathbf{z}\| \cdot n^{\mathrm{c}}$. The computation of the value $t(\mathbf{z})$ runs by graph-recursion on t:

(1) fix the leafs
(2) take the next vertex of the shape $f(r, s)$
(3) go to the (at most two distinct) subterm vertices r, s
(4) take previously defined values of $r(\mathbf{z})$, $s(\mathbf{z})$ and compute the value $f(r, s)(\mathbf{z})$
(5) stop after computing the root value $t(\mathbf{z})$

By standard methods, the above procedure 1-5 can be implemented by a `register machine`[1] $\mathcal{M}$ of the weight $O(n^{\mathrm{c}})$, which is uniquely determined by t. Actually, only the `times` loops are required in $\mathcal{M}$. Furthermore, the entirely computing steps 4 refer to the operations $+$ and $-$ with integer inputs and outputs $\le \|\mathbf{z}\| \cdot n^{\mathrm{c}}$. Other steps refer merely to the search of appropriate vertices among the given $\le n^{\mathrm{c}}$ ones. Hence by previous observations, the number of $\mathcal{M}$-steps required for the computation of the value $t(\mathbf{z})$ with input $\mathbf{z}$ does not exceed $O(n^{\mathrm{c}}) \cdot O(\|\mathbf{z}\| \cdot n^{\mathrm{c}}) = O(n^{\mathrm{c}} \cdot \|\mathbf{z}\| \cdot n^{\mathrm{c}}) = O(\|\mathbf{z}\| \cdot n^{2\mathrm{c}})$. This completes the proof, since $O(n^{\mathrm{c}}) < n^{\mathrm{c}+1}$ and $O(\|\mathbf{z}\| \cdot n^{2\mathrm{c}}) < \|\mathbf{z}\| \cdot n^{2\,\mathrm{c}+1}$ holds for sufficiently large n, Q.E.D. $\square$

Note that by Lemmata 12, 14 the algebraic complexity (and in fact both the graph- and norm-component) of $\Phi_n^?$ is exponential in n. In the sequel we discuss this feature in the context of **NP** vs. **P** problem.

[1] A register machine is represented by a finite list of registers (variables) x_1, ..., x_k, a finite list of orders $\mathrm{x}_i{:=}0$, $\mathrm{x}_i{:=}\mathrm{x}_j$, $\mathrm{x}_i{:=}\mathrm{x}_j{+}1$, $\mathrm{x}_i{:=}\mathrm{x}_j{-}1$, and a finite list of while-loops in parentheses form WHILE $\mathrm{x}_i{=}0$ DO, OD. Actually in the proof we can weaken while-loops to the times-loops DO x_i TIMES, OD. The weight of a given register machine is total length of its representation.

4 Condition C3 and P-NP connections

Condition 18 *Denote by* **C3** *the following sentence. For every* $\mathrm{c} \in \mathbb{N}^+$ *there are arbitrarily large* $n \in \mathbb{N}^+$ *such that no* $3n$*-ary quasi-polynomial whose algebraic complexity does not exceed* $(3n)^{\mathrm{c}}$ *has the same zero-set as* $\Phi_n^?$ *in every* $(3n)^{\mathrm{c}}$ *-ary normed domain. That is,* **C3** *reads:*

$$(\forall \mathrm{c} \in \mathbb{N}^+)\,(\forall N \in \mathbb{N}^+)\,(\exists n > N)\left(\forall t \in \mathfrak{Q}_{3n}^{(\mathrm{c})}\right)\left(\exists D \in \mathfrak{D}_{(3n)^{\mathrm{c}}}\right)\left(\Phi_n^? = 0 \underset{D}{\Leftrightarrow} t = 0\right)$$

$$\text{where } \Phi_n^? = 0 \underset{D}{\Leftrightarrow} t = 0 \text{ stands for } (\exists \upsilon \in D^{3n})\left(\Phi_n^?(\upsilon) = 0 \nleftrightarrow t(\upsilon) = 0\right)$$

For any fixed $D \in \mathfrak{D}_{(3n)^{\mathrm{c}}}$*, denote by* $\mathbf{C3}\,[D]$ *the corresponding specification*

$$\left(\forall \mathrm{c} \in \mathbb{N}^+\right)\left(\forall N \in \mathbb{N}^+\right)(\exists n > N)\left(\forall t \in \mathfrak{Q}_{3n}^{(\mathrm{c})}\right)\left(\Phi_n^? = 0 \underset{D}{\Leftrightarrow} t = 0\right)$$

Definition 19 *Denote by* $\mathbf{TAU3} \in \mathbf{P/poly}$ *the following sentence. There exists* $\mathrm{c} \in \mathbb{N}^+$ *such that for sufficiently large* $n \in \mathbb{N}^+$ *there exists a* ***register machine*** $\mathcal{M}$ *whose weight does not exceed* n^{c} *and such that the following holds. For any* $k \in \mathbb{N}^+$ *and any* $(3 \times n)$*-dim disjunctive normal form (abbr.: DNF)* Δ *with boolean variables from the set* $\{\vartheta_1, \cdots, \vartheta_k\}$*, the corresponding tautology problem* $TAU(\Delta)$ *is decidable by* $\mathcal{M}$ *in at most* $k \cdot n^{\mathrm{c}}$ *steps.*

Remark 20 $\mathbf{TAU3} \in \mathbf{P/poly}$ *is weaker than the conjecture* $\mathbf{TAU3} \in \mathbf{P}$ *(in words: the tautology problem of DNF with 3 literals per clause is decidable by a* ***Turing machine*** *in polynomial time), since* $\mathcal{M}$ *in question might depend on the number of clauses. However, practical consequences of* $\mathbf{TAU3} \in \mathbf{P/poly}$ *hardly differ from the ones of* $\mathbf{TAU3} \in \mathbf{P}$*. Hence* $\mathbf{TAU3} \in \mathbf{P/poly}$ *is hardly more plausible than the conjecture* $\mathbf{NP} = \mathbf{P}$*.*

4.1 Soundness theorem

Theorem 21 ***Soundness****. If* **C3** *fails, then* $\mathbf{TAU3} \in \mathbf{P/poly}$*.*

Proof. Since $\mathbf{C3}\,[\mathbb{Z}]$ is stronger than **C3**, $\neg\mathbf{C3}\,[\mathbb{Z}]$ is weaker than $\neg\mathbf{C3}$. So it will suffice to prove that $\neg\mathbf{C3}\,[\mathbb{Z}]$ infers $\mathbf{TAU3} \in \mathbf{P/poly}$. By definition, $\neg\mathbf{C3}\,[\mathbb{Z}]$ reads: *There are* $\mathrm{c}, N \in \mathbb{N}^+$ *such that for every* $n > N$ *there exists quasi-polynomial* $t \in \mathfrak{Q}_{3n}^{(\mathrm{c})}$ *such that* $\Phi_n^? = 0 \underset{\mathbb{Z}}{\Leftrightarrow} t = 0$*, i.e.* $\Phi_n^? = 0 \Leftrightarrow t = 0$ *holds in* $\mathbb{Z}$. Let L be the following integers-as-literals interpretation of $\mathbb{Z}$ in

the propositional language with boolean variables $\vartheta_1, \vartheta_2, \cdots$.

$$\mathbb{Z} \ni z \mapsto L(z) := \begin{cases} \vartheta_z & \text{if} \quad z > 0 \\ \top & \text{if} \quad z = 0 \\ \neg\vartheta_{-z} & \text{if} \quad z < 0 \end{cases}$$

Take C, N as above, and let $n > N$. Consider any $(3 \times n)$-dim DNF

$$\Delta = \bigvee_{j=1}^{n} (L_{1,j} \wedge L_{2,j} \wedge L_{3,j})$$

where each $L_{i,j} \in \{\top\} \cup \{\vartheta_\iota \mid \iota \leq k\} \cup \{\neg\vartheta_\iota \mid \iota \leq k\}$ for a minimal $k \in \mathbb{N}$ of this kind. By the above interpretation, this yields $L_{i,j} = L(z_{i,j})$ for the uniquely determined $z_{i,j} \in \mathbb{Z}_{|k|}$. Let $\mathbf{z} = (z_1, \cdots, z_{3n}) \in \mathbb{Z}_{|k|}^{3n} := \left(\mathbb{Z}_{|k|}\right)^{3n}$ where $z_{i+3(j-1)} := z_{i,j}$, for all $0 < i \leq 3, 0 < j \leq n$. Hence

$$\begin{aligned} \Delta &= \bigvee_{j=1}^{n} (L(z_{1,j}) \wedge L(z_{2,j}) \wedge L(z_{3,j})) \\ &= \bigvee_{j=1}^{n} \left(L\left(z_{3(j-1)+1}\right) \wedge L\left(z_{3(j-1)+2}\right) \wedge L\left(z_{3j}\right)\right) =: \Delta(\mathbf{z}) \end{aligned}$$

By Lemma 6 (11), we have

$$\begin{aligned} &\Phi_n^?(\mathbf{z}) = 0 \\ &\leftrightarrow (\forall f \in [\mathbf{n} \to \mathbf{3}])\,(\exists i, j \in \mathbf{n})\left(z_{f(i),i} + z_{f(j),j} = 0\right) \\ &\leftrightarrow (\forall f \in [\mathbf{n} \to \mathbf{3}])\,(\exists i, j \in \mathbf{n})\left(L\left(z_{f(i),i}\right) = \neg L\left(z_{f(j),j}\right)\right) \\ &\leftrightarrow \bigvee_{j=1}^{n} (L(z_{1,j}) \wedge L(z_{2,j}) \wedge L(z_{3,j})) \equiv \top \\ &\leftrightarrow \Delta = \Delta(\mathbf{z}) \equiv \top \end{aligned}$$

Hence $TAU(\Delta)$ holds iff $\Phi_n^?(\mathbf{z}) = 0$. Now suppose $t \in \mathfrak{Q}_{3n}^{(\mathrm{C})}$ be such that $\Phi_n^? = 0 \underset{\mathbb{Z}}{\Leftrightarrow} t = 0$, and hence $TAU(\Delta) \leftrightarrow TAU(\Delta(\mathbf{z})) \leftrightarrow t(\mathbf{z}) = 0$. By the soundness lemma (see above), the value $t(\mathbf{z})$ can be uniformly computed by a `register machine` of the weight $\leq n^{\mathrm{C}+1} < n^{2\mathrm{C}+1}$ in at most $\|\mathbf{z}\| \cdot n^{2\mathrm{C}+1} \leq k \cdot n^{2\mathrm{C}+1}$ steps, provided that n is sufficiently large. Hence $\neg\mathbf{C3}\,[\mathbb{Z}]$ infers $\mathbf{TAU3} \in \mathbf{P/poly}$, Q.E.D. $\square$

4.2 Sufficiency

In the rest of this section we will establish a following inversion of the soundness theorem.

Theorem 22 ***Sufficiency***. *If* **C3** *holds, then* **TAU3** $\notin$ **P** *and hence* **NP** $\neq$ **P**.

4.2.1 Collapsing

Lemma 23 ***Collapsing***. *If* n *is sufficiently large, then there exist* $3n$ *quasi-polynomials* $t_1, \cdots, t_{3n} \in \mathfrak{Q}_{3n}^{(3)}$ *such that for every* $\iota \leq 3n$, $D \in \mathfrak{D}_{(3n)^3}$, $\mathbf{v} = (\upsilon_1, \cdots \upsilon_{3n}) \in D^{3n}$, $\mathbf{t}(\mathbf{v}) = (t_1(\mathbf{v}), \cdots, t_{3n}(\mathbf{v}))$, *the following conditions hold.*

(1) $t_\iota(\mathbf{v}) \in \mathbb{Z}_{|3n|}$
(2) $\Phi_n^?(\mathbf{v}) = 0 \leftrightarrow \Phi_n^?(\mathbf{t}(\mathbf{v})) = 0$

Proof. The required $\mathbf{t}(\mathbf{v})$ will preserve the structure $\{\upsilon_j = \upsilon_k, \upsilon_j = -\upsilon_k\}_{j,k}$ of $\mathbf{v}$, which we denote by $\mathbf{v} \cong \mathbf{t}(\mathbf{v})$. Thus $(y_1, \cdots, y_{3n}) \cong (z_1, \cdots, z_{3n}) \Leftrightarrow (\forall i, j)((y_i = y_j \leftrightarrow z_i = z_j) \wedge (y_i = -y_j \leftrightarrow z_i = -z_j))$. Clearly, $\mathbf{v} \cong \mathbf{t}(\mathbf{v})$ yields the condition 3. The corresponding collapsing algorithm $\mathbf{v} \mapsto \mathbf{t}(\mathbf{v})$ will preserve 0, while recursively replacing other values by successive small integers. Example: $n = 4$, $3n = 12$, $\mathbf{v} = (15, -47, 1, 3, 8, -102, 0, -15, -1, -8, 47, 543)$ We transform $\mathbf{v}$ as follows.

Step 1. $(1, -47, 15, 3, 8, -102, 0, -1, -15, -8, 47, 543)$
// $15 \mapsto 1, 1 \mapsto 15, -15 \mapsto -1, -1 \mapsto -15$
Step 2. $(1, 2, 15, 3, 8, -102, 0, -1, -15, -8, -2, 543)$
// $-47 \mapsto 2, 47 \mapsto -2$
Step 3. $(1, 2, 3, 15, 8, -102, 0, -1, -3, -8, -2, 543)$
// $15 \mapsto 3, 3 \mapsto 15, -15 \mapsto -3$
Step 4. $(1, 2, 3, 4, 8, -102, 0, -1, -3, -8, -2, 543)$
// $15 \mapsto 4$
Step 5. $(1, 2, 3, 4, 5, -102, 0, -1, -3, -5, -2, 543)$
// $8 \mapsto 5, -8 \mapsto -5$
Step 6. $(1, 2, 3, 4, 5, 6, 0, -1, -3, -5, -2, 543)$
// $-102 \mapsto 6$
Step 7-11. $(1, 2, 3, 4, 5, 6, 0, -1, -3, -5, -2, 543)$
// no change
Step 12. $(1, 2, 3, 4, 5, 6, 0, -1, -3, -5, -2, 12)$
// $543 \mapsto 12$

This yields the result $\mathbf{t}(\mathbf{v}) = (1, 2, 3, 4, 5, 6, 0, -1, -3, -5, -2, 12)$. Obviously, $\mathbf{v} \cong \mathbf{t}(\mathbf{v})$ and $|t_1(\mathbf{v})|, \cdots, |t_{12}(\mathbf{v})| \leq 12 = 3n$. Generally speaking, this procedure can be formalized by a suitable recursive definition (see Algorithm 22 below for the corresponding Maple program). We wish to express it in our basic language $\mathcal{L}_n^?$. To this end, first note that $\upsilon_j = \upsilon_k$ and $\upsilon_j = -\upsilon_k$ can be expressed by $\upsilon_j - \upsilon_k = 0$ and $\upsilon_j + \upsilon_k = 0$, respectively. Now consider variables $x_1, \cdots, x_{3n}$ and $X_{i,j,k}$ for all indices $0 \leq i \leq 1, 0 < k, 0 \leq j \leq k \leq 3n$. Having

in mind an interpretation $X_{i,j,k} := \mathit{coll}\left([x_1, \cdots, x_{3n}], i, j, k\right)$ (see Algorithm 24) we set:

$$(1)\ X_{0,0,k} := 0 \qquad X_{1,0,k} := x_k$$

$$(2)\ X_{1,j,j} := \left\{ \begin{array}{lll} 0 & \text{if} & x_j = 0 \\ j & \text{else if} & X_{0,j-1,j} = 0 \\ X_{1,j-1,j} & \text{else} & \end{array} \right\} \text{if } 0 < j$$

$$(3)\ X_{0,j,k} := \left\{ \begin{array}{ll} & X_{0,j-1,k} - 1 = 0 \\ 1 \quad \text{if} & \vee\ X_{1,j-1,k} - X_{1,j-1,j} = 0 \\ & \vee\ X_{1,j-1,k} + X_{1,j-1,j} = 0 \\ 0 \quad \text{else} & \end{array} \right\} \text{if } 0 < j$$

$$(4)\ X_{1,j,k} := \left\{ \begin{array}{lll} 0 & \text{if} & x_k = 0 \\ X_{1,j,j} & \text{else if} & X_{1,j-1,k} - X_{1,j-1,j} = 0 \\ -X_{1,j,j} & \text{else if} & X_{1,j-1,k} + X_{1,j-1,j} = 0 \\ X_{1,j-1,j} & \text{else if} & X_{1,j-1,k} - X_{1,j,j} = 0 \\ -X_{1,j-1,j} & \text{else if} & X_{1,j-1,k} + X_{1,j,j} = 0 \\ X_{1,j-1,k} & \text{else} & \end{array} \right\} \text{if } 0 < j < k$$

Recall that we have a 1-1 embedding $x_{i+3(j-1)} \rightleftarrows x_{i,j}$ of $x_1, \cdots, x_{3n}$ into the variables of $\mathcal{L}_n^?$. Furthermore, let x, y, z, u be arbitrary fixed distinct variables of $\mathcal{L}_n^?$ (we assume that $n > 1$). Now by Corollary 6, there are quasi-polynomials $s_{1,j},\ s_2,\ s_3$ $(0 < j \leq 3n)$ with variables from the list x, y, z, u, such that the following hold.

$$s_{1,j} = \left\{ \begin{array}{lll} 0 & \text{if} & x = 0 \\ j & \text{else if} & y = 0 \\ z & \text{else} & \end{array} \right.$$

$$s_2 = \left\{ \begin{array}{ll} 1 \quad \text{if} & y - 1 = 0 \vee z - u = 0 \vee z + u = 0 \\ 0 \quad \text{else} & \end{array} \right.$$

$$s_3 = \begin{cases} 0 & \text{if} \quad x = 0 \\ u & \text{else if} \quad y - z = 0 \\ -u & \text{else if} \quad y + z = 0 \\ z & \text{else if} \quad y - u = 0 \\ -z & \text{else if} \quad y + u = 0 \\ y & \text{else} \end{cases}$$

In fact, the most complex among them can be defined by

$$s_3 := x?(u + (y - z)?(1 - 1 - u - u + (y + z)?(z + u + (y - u)?(1 - 1 - z - z + (y + u)?\,(y + z)))))$$

Having this we can extend s_1, s_2, s_3 to the composite quasi-polynomials $T_{i,j,k}$ such that the recursive clauses 1-4 hold for $T_{i,j,k}$, instead of $X_{i,j,k}$, in all basic domains. These $T_{i,j,k}$ are obtained by successive substitutions of previous ones for variables y, z, u, and variables (corresponding to) x_j, x_k for x, according to the notations used in 1-4. Note that there are $9n^2 + 3n$ variables $X_{i,j,k}$, while the graph-complexity of each s_ι, $\iota = 1, 2, 3$, does not exceed 26. Therefore the graph-complexity of every $T_{i,j,k}$ does not exceed $26 \cdot (9n^2 + 3n) \leq 312n^2$. (Warning: the ordinary term-complexity of $T_{i,j,k}$ is exponential in n.) Consider the norm-complexity. Let $\mathbf{v}$ be any input. It is readily seen that the norm of every subterm involved in the computation of any $T_{i,j,k}(\mathbf{v})$ does not exceed $\max(3n, 2\|\mathbf{v}\|)$, and hence $3n\|\mathbf{v}\|$, provided that $\|\mathbf{v}\| \geq 1$. Now for every $\iota = 1, \cdots, 3n$ set $t_\iota := T_{1,\iota,\iota}$. This yields $t_\iota \in \mathbb{Z}_{|3n|}$ (cf. the example above), while by previous considerations we conclude that the algebraic complexity of every t_ι does not exceed $(3n)^3$, provided that $n \geq 12$. Q.E.D. $\square$

Algorithm 1

```
collapse:= x->[seq(coll(x,1,i,i),i=1..nops(x))];
coll:= proc(x::list, i::nonnegint, j::nonnegint, k::nonnegint)
option remember;
  if j=0 then
     if i=0 then 0
     else x[k]
     fi
  elif i=1 and j=k then
     if x[j]=0 then 0
     elif coll(x,0,j-1,j)=0 then j
     else coll(x,1,j-1,j)
     fi
  elif i=0 then
    if coll(x,0,j-1,k)-1=0 or coll(x,1,j-1,k)-coll(x,1,j-1,j)=0
```

```
         or coll(x,1,j-1,k)+coll(x,1,j-1,j)=0 then 1
     else 0
    fi
  elif i=1 and j<k then
     if x[k]=0 then 0
     elif coll(x,1,j-1,k)-coll(x,1,j-1,j)=0 then coll(x,1,j,j)
     elif coll(x,1,j-1,k)+coll(x,1,j-1,j)=0 then -coll(x,1,j,j)
     elif coll(x,1,j-1,k)-coll(x,1,j,j)=0 then coll(x,1,j-1,j)
     elif coll(x,1,j-1,k)+coll(x,1,j,j)=0 then -coll(x,1,j-1,j)
     else coll(x,1,j-1,k)
     fi
   fi
end;
-------------------------------------------------
x:=[15,-47,1,3,8,-102,0,-15,-1,-8,47,543];
collapse(x)=[1, 2, 3, 4, 5, 6, 0, -1, -3, -5, -2, 12]
```

Remark 24 *This collapsing algorithm can be further optimized, in order to obtain minimal coordinates of the vector* $\mathbf{t}(\mathbf{v})$. *In the above example this would provide us with the optimal output* $(1,2,3,4,5,6,0,-1,-3,-5,-2,7)$ *instead of* $(1,2,3,4,5,6,0,-1,-3,-5,-2,12)$. *By an obvious specification of the algorithm, the lemma is also true of the corresponding optimization.*

Remark 25 *In the sequel we need a slight modification of Lemma 23. It is obtained in an obvious way by replacing every* t_ι *by two quasi-polynomials* $s'_\iota, t'_\iota \in \mathfrak{Q}^{(3)}_{3n}$ *such that for every* $\mathbf{v} \in D^{3n}$, $s'_\iota(\mathbf{v}) \in \{1,2,3\}$, $3n \geq t'_\iota(\mathbf{v}) \in \mathbb{N}$ *and*

$$t_\iota(\mathbf{v}) = 0 \leftrightarrow s'_\iota(\mathbf{v}) = 1 \wedge t'_\iota(\mathbf{v}) = 0$$
$$t_\iota(\mathbf{v}) > 0 \leftrightarrow s'_\iota(\mathbf{v}) = 2 \wedge t'_\iota(\mathbf{v}) = t_\iota(\mathbf{v})$$
$$t_\iota(\mathbf{v}) < 0 \leftrightarrow s'_\iota(\mathbf{v}) = 3 \wedge t'_\iota(\mathbf{v}) = -t_\iota(\mathbf{v})$$

4.2.2 Notations

Definition 26 *A cell of a given Post-Turing input (output)* τ, *is called an* ***outer cell*** *iff it belongs to one of the two infinite* τ*-empty tape intervals; other cells are called* ***inner cells*** *of* τ. *The number of all inner cells of* τ *is called the* ***length*** *of (written part of)* τ *and denoted by* $\#(\tau)$. *It is assumed that cells can be identified with integers and thus preserve the underlying order of* $\mathbb{Z}$. *Moreover,* 0 *is called the* ***scanning cell*** *(see [G] for more detailed tape descriptions). Generally, we express inputs (outputs)* τ *as finite strings of letters (of a given finite alphabet) printed in finite intervals* $[-m,k] = [-m,\cdots,-1,0,1,\cdots,k] \subset \mathbb{Z}$ *and put in box the* ***scanning letter*** *that is printed in the scanning cell, e.g.* $\tau = \emptyset a\boxed{b}bcad\emptyset$ *(abbr.:* $\tau = a\boxed{b}bcad$*)*

for $m = 1, k = 4, \#(\tau) = 6$.

Definition 27 *Consider any given (finite) tape alphabet* $\mathcal{A}$ *and any* $\ell \in \mathbb{N}$. *By obvious encoding, we can just as well assume* $\mathcal{A} = \{0\} \cup \mathbf{m} = \{0, 1, \cdots, m\}$, *where* 0 *denotes the empty tape symbol. A sequence*

$$\rho = \langle b_{-\ell}, x_{-\ell} \rangle, \cdots, \langle b_0, x_0 \rangle, \cdots, \langle b_\ell, x_\ell \rangle \in (\mathcal{A} \times \mathbb{N}^+)^{2\ell+1}$$

is called a $(\mathcal{A}, \ell)$***-code*** *iff the following holds.*

$$\begin{aligned}(\forall i \in [-\ell, \ell - 1])\,(b_i = b_{i+1} \to i = -1 \vee (i < -1 \wedge (\forall j \in [-\ell, i])\,(b_j = 0))\\ \vee (i \geq 0 \wedge (\forall j \in [i + 1, \ell])\,(b_j = 0)))\end{aligned}$$

Furthermore, let $\ell_- \in [-\ell, 0]$ *and* $\ell_+ \in [-1, \ell]$ *be respectively the largest and smallest indices such that* $(\forall \iota < \ell_-)\,(b_\iota = 0)$ *and* $(\forall \iota > \ell_+)\,(b_\iota = 0)$. *Call* $|\rho| := \ell$ *and* $\mathtt{lth}(\rho) := 1 + \ell_+ - \ell_-$ *the* ***scope*** *and* ***length*** *of* ρ , *respectively. Define the correlated input (output)* $\tau(\rho)$ *by*

$$\begin{aligned}\tau(\rho) &:= \underbrace{\cdots 0}_{\infty}\underbrace{b_{\ell_-} \cdots b_{\ell_-}}_{x_{\ell_-}} \cdots \underbrace{b_{-1} \cdots b_{-1}}_{x_{-1}}\underbrace{\boxed{b_0} \cdots b_0}_{x_0}\underbrace{b_1 \cdots b_1}_{x_1} \cdots \underbrace{b_{\ell_+} \cdots b_{\ell_+}}_{x_{\ell_+}}\underbrace{0 \cdots}_{\infty}\\ &= \underbrace{b_{\ell_-} \cdots b_{\ell_-}}_{x_{\ell_-}} \cdots \underbrace{b_{-1} \cdots b_{-1}}_{x_{-1}}\underbrace{\boxed{b_0} \cdots b_0}_{x_0}\underbrace{b_1 \cdots b_1}_{x_1} \cdots \underbrace{b_{\ell_+} \cdots b_{\ell_+}}_{x_{\ell_+}}\\ &= \underbrace{b_{-\ell} \cdots b_{-\ell}}_{x_{-\ell}} \cdots \underbrace{b_{-1} \cdots b_{-1}}_{x_{-1}}\underbrace{\boxed{b_0} \cdots b_0}_{x_0}\underbrace{b_1 \cdots b_1}_{x_1} \cdots \underbrace{b_\ell \cdots b_\ell}_{x_\ell}\end{aligned}$$

Hence $\#(\tau(\rho)) = \sum_{\iota=\ell_-}^{\ell_+} x_\iota$. *A* $(\mathcal{A}, \ell)$*-code* ρ *is also called a* ***code*** *of* $\tau(\rho)$. *Note that if* ρ *is any code of* τ, *then* ℓ_-, ℓ_+ *and* $\mathtt{lth}(\rho)$ *are uniquely determined by* τ. *Now let* $\mathcal{T}$ *be a* ***Turing machine*** *over tape alphabet* $\mathcal{A} = \{0\} \cup \mathbf{m}$ *and state alphabet* $\mathcal{S} = \{0\} \cup \mathbf{k}$ *for* $m, k > 0$, *where* 0 *and* 1 *are respectively the initial and the end state of* $\mathcal{T}$. *Call a* $(\mathcal{A}, \mathcal{S}, \ell)$***-code*** *a sequence*

$$\widehat{\rho} = \langle b_{-\ell}, x_{-\ell} \rangle, \cdots, \langle b_0, x_0, q \rangle, \cdots, \langle b_\ell, x_\ell \rangle$$

that extends a $(\mathcal{A}, \ell)$***-code*** $\rho = \langle b_{-\ell}, x_{-\ell} \rangle, \cdots, \langle b_0, x_0 \rangle, \cdots, \langle b_\ell, x_\ell \rangle$ *by adding a state symbol (letter)* $q \in \mathcal{S}$ *in the initial component. Set* $|\widehat{\rho}| := |\rho|$ *and* $\mathtt{lth}(\widehat{\rho}) := \mathtt{lth}(\rho)$. *The correlated labeled input (output)* $\widehat{\tau}(\widehat{\rho})$ *has the following form, where* q *shows the scanning state.*

$$\widehat{\tau}(\widehat{\rho}) := \underbrace{\cdots 0}_{\infty}\underbrace{b_{\ell_-} \cdots b_{\ell_-}}_{x_{\ell_-}} \cdots \underbrace{b_{-1} \cdots b_{-1}}_{x_{-1}}\underbrace{\overset{q}{\boxed{b_0}} \cdots b_0}_{x_0}\underbrace{b_1 \cdots b_1}_{x_1} \cdots \underbrace{b_{\ell_+} \cdots b_{\ell_+}}_{x_{\ell_+}}\underbrace{0 \cdots}_{\infty}$$

$$= \underbrace{b_{\ell_-} \cdots b_{\ell_-}}_{x_{\ell_-}} \cdots \underbrace{b_{-1} \cdots b_{-1}}_{x_{-1}} \overset{q}{\boxed{b_0}} \underbrace{\cdots b_0}_{x_0} \underbrace{b_1 \cdots b_1}_{x_1} \cdots \underbrace{b_{\ell_+} \cdots b_{\ell_+}}_{x_{\ell_+}}$$

$$= \underbrace{b_{-\ell} \cdots b_{-\ell}}_{x_{-\ell}} \cdots \underbrace{b_{-1} \cdots b_{-1}}_{x_{-1}} \overset{q}{\boxed{b_0}} \underbrace{\cdots b_0}_{x_0} \underbrace{b_1 \cdots b_1}_{x_1} \cdots \underbrace{b_{\ell} \cdots b_{\ell}}_{x_{\ell}}$$

A $(\mathcal{A}, \mathcal{S}, \ell)$*-code* $\widehat{\rho}$ *is called a* ***code*** *of* $\widehat{\tau}\,(\widehat{\rho})$ *and/or a* ***labeled code*** *of* $\tau\,(\rho)$*.*

Example 28 *Let* $\mathcal{A} = \{0,1,2,3\}$*. For any* $x \in \mathbb{N}^+$*,* $\rho = \langle 0, x\rangle$ *is a code of the empty* $\mathcal{A}$ *-input* $\tau = \boxed{0}$*; moreover* $\ell_- = 0, \ell_+ = -1$ *and* $\#(\tau) = \mathtt{lth}(\rho) = 0$*. Now consider a* $\mathcal{A}$*-input* $\tau = 113\boxed{3}301222$ *and the same input in the initial state* $\widehat{\tau} = 113\overset{0}{\boxed{3}}301222$*. Clearly* $\#(\tau) = 10$*. Some codes of this* τ *are listed below, where* $\langle 0,1\rangle^i := \underbrace{\langle 0,1\rangle, \cdots, \langle 0,1\rangle}_{i}$*. The last one is the minimal labeled code of* τ *for* $\ell = 6$*, in the initial state. Note that for any* ρ *in question we have* $\ell_- = -2$*,* $\ell_+ = 3$ *and* $\mathtt{lth}(\rho) = 6$*.*

- $\ell = 3$ *and* $\widehat{\rho} = \langle 0,1\rangle, \langle 1,2\rangle, \langle 3,1\rangle, \langle 3,2,0\rangle, \langle 0,1\rangle, \langle 1,1\rangle, \langle 2,3\rangle$
- $\ell = 4$ *and* $\rho = \langle 0,2\rangle, \langle 0,3\rangle, \langle 1,2\rangle, \langle 3,1\rangle, \langle 3,2\rangle, \langle 0,1\rangle, \langle 1,1\rangle, \langle 2,3\rangle, \langle 0,7\rangle$
- $\ell = 6$ *and* $\rho = \langle 0,1\rangle^4, \langle 1,2\rangle, \langle 3,1\rangle, \langle 3,2\rangle, \langle 0,1\rangle, \langle 1,1\rangle, \langle 2,3\rangle, \langle 0,4\rangle^2, \langle 0,1\rangle$
- $\ell = 6$ *and* $\widehat{\rho} = \langle 0,1\rangle^4, \langle 1,2\rangle, \langle 3,1\rangle, \langle 3,2,0\rangle, \langle 0,1\rangle, \langle 1,1\rangle, \langle 2,3\rangle, \langle 0,1\rangle^3$

4.2.3 Rest of the proof

Lemma 29 *Assume* **TAU3** $\in \mathbf{P}$*. There are* $\mathrm{c}_0, N_0 \in \mathbb{N}^+$ *such that for every* $n > N_0$ *there exists a quasi-polynomial* $t_0 \in \mathfrak{Q}_{6n}^{(\mathrm{c}_0)}$ *such that* $\Phi_n^?(\mathbf{z}) = 0 \leftrightarrow t_0(\mathbf{z}^*) = 0$ *holds for every* $\mathbf{z} = (z_1, \cdots, z_{3n}) \in \mathbb{Z}_{|3n|}^{3n} := \left(\mathbb{Z}_{|3n|}\right)^{3n}$*, where* $\mathbf{z}^* = (v_1, \cdots, v_{6n}) \in \mathbb{N}^{3n}$ *for* $v_{2\iota} := |z_\iota|$ *and* $v_{2\iota-1} := \begin{cases} 1 & \text{if} \quad z_\iota = 0 \\ 2 & \text{if} \quad z_\iota > 0 \\ 3 & \text{if} \quad z_\iota < 0 \end{cases}, 1 \leq \iota \leq 3n.$

Proof. We adopt from the soundness theorem (see above) a linear 1-1 correspondence $\mathbf{z} \mapsto \Delta(\mathbf{z})$ between vectors from $\mathbb{Z}_{|3n|}^{3n}$ and $(3 \times n)$-dim DNFs whose variables have indices $\leq 3n$. Hence it will suffice to infer from the assumption the following sentence.

There are $\mathrm{c}_0, N_0 \in \mathbb{N}^+$ *such that for every* $n > N_0$ *there exists* $t_0 \in \mathfrak{Q}_{6n}^{(\mathrm{c}_0)}$ *such that* $\Delta(\mathbf{z}) \equiv \top \leftrightarrow t_0(\mathbf{z}^*) = 0$ *holds for every* $\mathbf{z} = (z_1, \cdots, z_{3n}) \in \mathbb{Z}_{|3n|}^{3n}$*.*

Suppose $\mathcal{T}$ be a PTIME `Turing machine` such that for every $(3\times n)$-dim DNF-input $\Delta=\bigvee\limits_{j=1}^{n}\left(L_{1,j}\wedge L_{2,j}\wedge L_{3,j}\right)$, the output $\mathcal{T}\left(\Delta\right)$ is $\top$ iff $\Delta\equiv\top$, i.e. $TAU\left(\Delta\right)$. Moreover, the number of $\mathcal{T}$-steps required for passing from Δ to $\mathcal{T}\left(\Delta\right)$ is supposed to be polynomial in the length of Δ. To put it more exactly, there are constants c_1,$\mathrm{c}_2>0$ such that $\mathcal{T}$ -computation with tape-input $\tau\left(\Delta\right)$ terminates after at most $\mathrm{c}_1\cdot\#\left(\tau\left(\Delta\right)\right)^{\mathrm{c}_2}$ steps. Denote by $\mathcal{A}$ the underlying tape alphabet. Without loss of generality suppose $\mathcal{A}\supseteq\{0,1,2,3,4\}$ such that 1 stands for $\top$, 2 and 3 encode via repetitions positive and negative literals, respectively, while 4 denotes propositional connectives $\vee$ or $\wedge$. Obviously, parentheses can be omitted. Thus e.g. a (3×2)-dim DNF-input $\Delta=\left(\vartheta_3\wedge\vartheta_1\wedge\neg\vartheta_2\right)\vee\left(\neg\vartheta_1\wedge\top\wedge\neg\vartheta_4\right)$ corresponds to the tape-input $\tau\left(\Delta\right)=\overset{0}{\boxed{2}}2242433434143333$ of the length $\#\left(\tau\left(\Delta\right)\right)=17$, whose minimal labeled code is

$$\widehat{\rho}=\langle0,1\rangle^{10},\langle2,3,0\rangle,\langle4,1\rangle,\langle2,1\rangle,\langle4,1\rangle,\langle3,2\rangle,\langle4,1\rangle,\langle3,1\rangle,\langle4,1\rangle,\langle1,1\rangle,\langle4,1\rangle,\langle3,4\rangle$$

where $|\widehat{\rho}|=\mathtt{lth}\left(\widehat{\rho}\right)=10$. Analogously, the tape-output $\mathcal{T}\left(\Delta\right)$ is supposed to be $\overset{1}{\boxed{1}}$ (just) in case $\Delta\equiv\top$. Observe that for any $\mathbf{z}\in\mathbb{Z}_{|3n|}^{3n}$ and any labeled code $\widehat{\rho}$ of $\tau\left(\Delta\left(\mathbf{z}\right)\right)$, this interpretation yields

$$6n-2=|\widehat{\rho}|=\mathtt{lth}\left(\widehat{\rho}\right)\leq\#\left(\tau\left(\Delta\left(\mathbf{z}\right)\right)\right)<9n^2+3n\leq12n^2$$

Therefore, for any $\mathbf{z}\in\mathbb{Z}_{|3n|}^{3n}$, $\mathcal{T}$-computation with input $\Delta\left(\mathbf{z}\right)$ terminates after at most $\mathrm{c}_1\cdot\left(12n^2\right)^{\mathrm{c}_2}=144\mathrm{c}_1\cdot n^{2\mathrm{c}_2}$ steps. We wish to simulate this computation in the language $\mathcal{L}_n^?$. This is possible, by Corollaries 7, 8 (see above), because natural formalization of Post-Turing computations requires only definitions by-cases. To put it more exactly, suppose $\mathcal{A}=\{0\}\cup\mathbf{m}$ and $\mathcal{S}=\{0\}\cup\mathbf{k}$, where $m\geq4$ and $k\geq2$ (without loss of generality: $2\leq k\leq4$), and let T be the (finite) list of $\mathcal{T}$-orders of the either form

1. $\langle g,\alpha\rangle\hookrightarrow\langle h,\beta\rangle$
2. $\langle g,\alpha\rangle\hookrightarrow^{+}\beta$
3. $\langle g,\alpha\rangle\hookrightarrow^{-}\beta$

where $g,h\in[0,m]$, $1\neq\alpha\in[0,k]$, $\beta\in[0,k]$, and every $\langle g,\alpha\rangle$ from the domain of T occurs in exactly one rule. The intended meaning is as follows. Rules 1-3 take input in state $\alpha\neq1$ with scanning letter g and return output in state β. Moreover, rule 1 replaces scanning letter g by h, in the same scanning position, whereas rule 2 (3) just moves scanning cell one step to the right (left). To complete the proof of the lemma, it will suffice to simulate T

-computations in the language $\mathcal{L}^?$. To this end, we formalize transformations of $(\mathcal{A}, \mathcal{S}, \ell)$-codes induced by iteration of the transition rules 1-3. For any given $(\mathcal{A}, \mathcal{S}, \ell)$-code

$$\widehat{\rho} = \langle b_{-\ell}, x_{-\ell}\rangle, \cdots, \langle b_{-1}, x_{-1}\rangle, \langle b_0, x_0, q\rangle, \langle b_1, x_1\rangle, \cdots, \langle b_\ell, x_\ell\rangle$$

where $0 \leq b_\iota \leq m, 1 \neq q \leq k, x_\iota > 0$, consider the labeled input

$$\begin{aligned}\widehat{\tau}(\widehat{\rho}) &= \underbrace{b_{-\ell}\cdots b_{-\ell}}_{x_{-\ell}}\cdots\underbrace{b_{-1}\cdots b_{-1}}_{x_{-1}}\underbrace{\overset{q}{\boxed{b_0}}\cdots b_0}_{x_0}\underbrace{b_1\cdots b_1}_{x_1}\cdots\underbrace{b_\ell\cdots b_\ell}_{x_\ell}\\ &= \underbrace{b_{-\ell}\cdots b_{-\ell}}_{x_{-\ell}}\cdots\underbrace{b_{-1}\cdots b_{-1}}_{x_{-1}}\underbrace{\overset{q}{\boxed{b_0}}\cdots b_0}_{x_0}\underbrace{b_1\cdots b_1}_{x_1}\cdots\underbrace{b_\ell\cdots b_\ell}_{x_\ell}\end{aligned}$$

Suppose that $\mathrm{R} \in T$ of the either form 1-3 is applicable to $\widehat{\tau}(\widehat{\rho})$. By definition we have $g = b_0$, $\alpha = q$ and $\beta = q'$. Let $\widehat{\tau}_{\mathrm{R}}$ be the corresponding labeled output. We look for a suitable $(\mathcal{A}, \mathcal{S}, \ell')$-code

$$\widehat{\rho}_{\mathrm{R}} = \left\langle b'_{-\ell-1}, x'_{-\ell-1}\right\rangle, \cdots, \left\langle b'_{-1}, x'_{-1}\right\rangle, \langle b'_0, x'_0, q'\rangle, \langle b'_1, x'_1\rangle, \cdots, \left\langle b'_{\ell+1}, x'_{\ell+1}\right\rangle$$

such that

$$\widehat{\tau}_{\mathrm{R}} = \widehat{\tau}(\widehat{\rho}_{\mathrm{R}}) = \underbrace{b'_{-\ell-1}\cdots b'_{-\ell-1}}_{x'_{-\ell-1}}\cdots\underbrace{b'_{-1}\cdots b'_{-1}}_{x'_{-1}}\underbrace{\overset{q'}{\boxed{b'_0}}\cdots b'_0}_{x'_0}\underbrace{b'_1\cdots b'_1}_{x'_1}\cdots\underbrace{b'_{\ell+1}\cdots b'_{\ell+1}}_{x'_{\ell+1}}$$

Consider the following cases.

(1) Suppose $\mathrm{R} = \langle g, \alpha\rangle \hookrightarrow \langle h, \beta\rangle$.
  (a) Suppose $h = b_0$. Set $\left\langle b'_{-\ell-1}, x'_{-\ell-1}\right\rangle := \langle 0, 1\rangle$, $\langle b'_\iota, x'_\iota\rangle := \langle b_\iota, x_\iota\rangle$ for $-\ell \leq \iota \leq \ell$, $\left\langle b'_{\ell+1}, x'_{\ell+1}\right\rangle := \langle 0, 1\rangle$.
  (b) Suppose $h \neq b_0$.
    (i) Suppose $x_0 = 1$.
      A. Suppose $h = b_1$. Set $\left\langle b'_{-\ell-1}, x'_{-\ell-1}\right\rangle := \langle 0, 1\rangle$, $\langle b'_\iota, x'_\iota\rangle := \langle b_\iota, x_\iota\rangle$ for $-\ell \leq \iota < 0$, $\langle b'_0, x'_0\rangle := \langle b_1, x_1 + 1\rangle$, $\langle b'_\iota, x'_\iota\rangle := \langle b_{\iota+1}, x_{\iota+1}\rangle$ for $0 < \iota < \ell$, $\langle b'_\ell, x'_\ell\rangle = \left\langle b'_{\ell+1}, x'_{\ell+1}\right\rangle := \langle 0, 1\rangle$.
      B. Suppose $h \neq b_1$. Set $\left\langle b'_{-\ell-1}, x'_{-\ell-1}\right\rangle := \langle 0, 1\rangle$, $\langle b'_\iota, x'_\iota\rangle := \langle b_\iota, x_\iota\rangle$ for $-\ell \leq \iota < 0$, $\langle b'_0, x'_0\rangle := \langle h, 1\rangle$, $\langle b'_\iota, x'_\iota\rangle := \langle b_\iota, x_\iota\rangle$ for $1 \leq \iota \leq \ell$, $\left\langle b'_{\ell+1}, x'_{\ell+1}\right\rangle := \langle 0, 1\rangle$.
    (ii) Suppose $x_0 \neq 1$. Set $\left\langle b'_{-\ell-1}, x'_{-\ell-1}\right\rangle := \langle 0, 1\rangle$, $\langle b'_\iota, x'_\iota\rangle := \langle b_\iota, x_\iota\rangle$ for $-\ell \leq \iota < 0$, $\langle b'_0, x'_0\rangle := \langle h, 1\rangle$, $\langle b'_1, x'_1\rangle := \langle b_0, x_0 - 1\rangle$, $\langle b'_\iota, x'_\iota\rangle := \langle b_{\iota-1}, x_{\iota-1}\rangle$ for $1 < \iota \leq \ell + 1$.

(2) Suppose $\mathrm{R} = \langle g, \alpha \rangle \hookrightarrow^{+} \beta$.
  (a) Suppose $b_0 = b_{-1}$.
    (i) Suppose $x_0 = 1$. Set $\left\langle b'_{-\ell}, x'_{-\ell} \right\rangle := \langle 0, 1 \rangle$, $\langle b'_{\iota}, x'_{\iota} \rangle := \langle b_{\iota}, x_{\iota} \rangle$ for $-\ell \leq \iota < -1$, $\left\langle b'_{-1}, x'_{-1} \right\rangle := \langle b_{-1}, x_{-1} + 1 \rangle$, $\langle b'_{\iota}, x'_{\iota} \rangle := \langle b_{\iota+1}, x_{\iota+1} \rangle$ for $0 \leq \iota < \ell$, $\langle b'_{\ell}, x'_{\ell} \rangle = \left\langle b'_{\ell+1}, x'_{\ell+1} \right\rangle := \langle 0, 1 \rangle$.
    (ii) Suppose $x_0 \neq 1$. Set $\langle b'_{\iota}, x'_{\iota} \rangle := \langle b_{\iota}, x_{\iota} \rangle$ for $-\ell \leq \iota < -1$, $\left\langle b'_{-1}, x'_{-1} \right\rangle := \langle b_{-1}, x_{-1} + 1 \rangle$, $\langle b'_0, x'_0 \rangle := \langle b_0, x_0 - 1 \rangle$, $\langle b'_{\iota}, x'_{\iota} \rangle := \langle b_{\iota}, x_{\iota} \rangle$ for $1 \leq \iota \leq \ell$.
  (b) Suppose $b_0 \neq b_{-1}$.
    (i) Suppose $x_0 = 1$. Set $\left\langle b'_{\iota-1}, x'_{\iota-1} \right\rangle := \langle b_{\iota}, x_{\iota} \rangle$ for $-\ell \leq \iota < 0$, $\left\langle b'_{-1}, x'_{-1} \right\rangle := \langle b_0, 1 \rangle$, $\langle b'_{\iota}, x'_{\iota} \rangle := \langle b_{\iota+1}, x_{\iota+1} \rangle$ for $0 \leq \iota < \ell$, $\langle b'_{\ell}, x'_{\ell} \rangle = \left\langle b'_{\ell+1}, x'_{\ell+1} \right\rangle := \langle 0, 1 \rangle$.
    (ii) Suppose $x_0 \neq 1$. Set $\left\langle b'_{\iota-1}, x'_{\iota-1} \right\rangle := \langle b_{\iota}, x_{\iota} \rangle$ for $-\ell \leq \iota < 0$, $\left\langle b'_{-1}, x'_{-1} \right\rangle := \langle b_0, 1 \rangle$, $\langle b'_0, x'_0 \rangle := \langle b_0, x_0 - 1 \rangle$, $\langle b'_{\iota}, x'_{\iota} \rangle := \langle b_{\iota}, x_{\iota} \rangle$ for $1 \leq \iota \leq \ell$, $\left\langle b'_{\ell+1}, x'_{\ell+1} \right\rangle := \langle 0, 1 \rangle$.
(3) Suppose $\mathrm{R} = \langle g, \alpha \rangle \hookrightarrow^{-} \beta$.
  (a) Suppose $b_0 = b_{-1}$.
    (i) Suppose $x_{-1} = 1$. Set $\left\langle b'_{\iota-1}, x'_{\iota-1} \right\rangle = \left\langle b'_{-\ell}, x'_{-\ell} \right\rangle := \langle 0, 1 \rangle$, $\langle b'_{\iota}, x'_{\iota} \rangle := \langle b_{\iota-1}, x_{\iota-1} \rangle$ for $-\ell < \iota < 0$, $\langle b'_0, x'_0 \rangle := \langle b_0, x_0 + 1 \rangle$, $\langle b'_{\iota}, x'_{\iota} \rangle := \langle b_{\iota}, x_{\iota} \rangle$ for $1 \leq \iota \leq \ell$, $\left\langle b'_{\ell+1}, x'_{\ell+1} \right\rangle := \langle 0, 1 \rangle$.
    (ii) Suppose $x_{-1} \neq 1$. Set $\left\langle b'_{\iota-1}, x'_{\iota-1} \right\rangle := \langle 0, 1 \rangle$, $\langle b'_{\iota}, x'_{\iota} \rangle := \langle b_{\iota}, x_{\iota} \rangle$ for $-\ell \leq \iota < -1$, $\left\langle b'_{-1}, x'_{-1} \right\rangle := \langle b_{-1}, x_{-1} - 1 \rangle$, $\langle b'_0, x'_0 \rangle := \langle b_0, x_0 + 1 \rangle$, $\langle b'_{\iota}, x'_{\iota} \rangle := \langle b_{\iota}, x_{\iota} \rangle$ for $1 \leq \iota \leq \ell$, $\left\langle b'_{\ell+1}, x'_{\ell+1} \right\rangle := \langle 0, 1 \rangle$.
  (b) Suppose $b_0 \neq b_{-1}$.
    (i) Suppose $x_{-1} = 1$. Set $\left\langle b'_{-\ell-1}, x'_{-\ell-1} \right\rangle = \left\langle b'_{-\ell}, x'_{-\ell} \right\rangle := \langle 0, 1 \rangle$, $\langle b'_{\iota}, x'_{\iota} \rangle := \langle b_{\iota-1}, x_{\iota-1} \rangle$ for $-\ell < \iota < 0$, $\langle b'_0, x'_0 \rangle := \langle b_{-1}, 1 \rangle$, $\langle b'_{\iota}, x'_{\iota} \rangle := \langle b_{\iota-1}, x_{\iota-1} \rangle$ for $0 < \iota \leq \ell + 1$.
    (ii) Suppose $x_{-1} \neq 1$. Set $\left\langle b'_{-\ell-1}, x'_{-\ell-1} \right\rangle = \left\langle b'_{-\ell}, x'_{-\ell} \right\rangle := \langle 0, 1 \rangle$, $\langle b'_{\iota}, x'_{\iota} \rangle := \langle b_{\iota}, x_{\iota} \rangle$ for $-\ell \leq \iota < -1$, $\left\langle b'_{-1}, x'_{-1} \right\rangle := \langle b_{-1}, x_{-1} - 1 \rangle$, $\langle b'_0, x'_0 \rangle := \langle b_{-1}, 1 \rangle$, $\langle b'_{\iota}, x'_{\iota} \rangle := \langle b_{\iota-1}, x_{\iota-1} \rangle$ for $0 < \iota \leq \ell + 1$.

Note that every single step of computation yields $|\widehat{\rho}_{\mathrm{R}}| = |\widehat{\rho}| + 1$. Hence, by iteration, $|\widehat{\rho}| \leq 6n - 2 + 144\mathrm{C}_1 \cdot n^{2\mathrm{C}_2}$ holds for every $\widehat{\rho}$ involved in the computation of $\mathcal{T}(\Delta(\mathbf{z}))$. Let $u := 6n - 2$ and $w := 144\mathrm{C}_1 \cdot n^{2\,\mathrm{C}_2}$. In order to obtain a required polynomial graph of computation, we fix a sequence of labeled meta-codes

$\widehat{\mathfrak{C}}_0, \widehat{\mathfrak{C}}_1, \cdots, \widehat{\mathfrak{C}}_w$, such that for each $i \leq w$,
$\widehat{\mathfrak{C}}_i = \left\langle Y^i_{-u-i}, X^i_{-u-i} \right\rangle, \cdots, \langle Y^i_0, X^i_0, Z^i \rangle, \cdots, \left\langle Y^i_{u+i}, X^i_{u+i} \right\rangle$

where Y^i_j, X^i_j, Z^i for $j \in [-u-i, u+i]$ are distinct metavariables. Geometrically speaking, we consider Y^i_j, X^i_j, Z^i as distinct vertices placed at level i. The correlated labeled codes

$$\widehat{\rho}_i = \left\langle b^i_{-u-i}, x^i_{-u-i} \right\rangle, \cdots, \langle b^i_0, x^i_0, q^i \rangle, \cdots, \left\langle b^i_{u+i}, x^i_{u+i} \right\rangle$$

are obtained by meta-recursion on i, according to the above clauses 1-3 (see above), as well as a trivial repetition clause (4). Now 4 is applied to any $\widehat{\rho}$ if 1-3 do not apply, and the output $\widehat{\rho}_{\mathrm{R}}$ preserves the state, i.e. $q' = q$, and all components of $\widehat{\rho}$, i.e. $\langle b'_\iota, x'_\iota \rangle = \langle b_\iota, x_\iota \rangle$ for all $\iota \in [-\ell, \ell]$, while adding two empty components $\left\langle b'_{-\ell-1}, x'_{-\ell-1} \right\rangle = \left\langle b'_{\ell+1}, x'_{\ell+1} \right\rangle := \langle 0, 1 \rangle$. In geometrical terms, this meta-recursion results in adding new vertices and links placed between levels i and $i+1$, which express constructions by-cases used at recursion step $i+1$. To put it more precisely, the construction runs as follows.

Step 0. Consider labeled meta-code

$$\widehat{\mathfrak{C}}_0 = \left\langle Y^0_{-u}, X^0_{-u} \right\rangle, \cdots, \langle Y^0_0, X^0_0, Z^0 \rangle, \cdots, \langle Y^0_u, X^0_u \rangle$$

For any given $\mathbf{z} = (z_1, \cdots, z_{3n}) \in \mathbb{Z}^{3n}_{|3n|}$ and correlated $\mathbf{z}^* = (v_1, \cdots, v_{6n}) \in \mathbb{N}^{3n}$, set $Z^0 := 0$, and for every $-u \leq \iota \leq u$:

$$Y^0_\iota := b^0_\iota = \begin{cases} 0 & \text{if} \quad \iota < 0 \\ v_{\iota+1} & \text{else if} \quad \iota \equiv 0 \mod 2 \\ 4 & \text{else} \end{cases}$$

$$X^0_\iota := x^0_\iota = \begin{cases} 1 & \text{if} \quad \iota < 0 \vee \iota \equiv 1 \mod 2 \\ 1 + v_\iota ? \, (v_\iota - 1) & \text{else} \end{cases}$$

Obviously, the resulting $\widehat{\rho}_0 = \left\langle b^0_{-u}, x^0_{-u} \right\rangle, \cdots, \langle b^0_0, x^0_0, 0 \rangle, \cdots, \langle b^0_u, x^0_u \rangle$ provides us with the labeled code of the input $\tau(\Delta(\mathbf{z}))$, in the initial state 0. To put it in geometrical terms corresponding to the language $\mathcal{L}^?$, we replace metavariable Z^0 by 0, while adding to old vertices Y^0_ι, X^0_ι new vertices and edges (links) which realize in $\mathcal{L}^?$ substitutions $Y^0_\iota := b^0_\iota$ and $X^0_\iota := x^0_\iota$. Such construction is called graph-realization of $\widehat{\mathfrak{C}}_0$. Note that each term b^0_ι, x^0_ι, 0 occurring in this realization requires at most 5 vertices, in case $x^0_\iota = 1 + v_\iota ? \, (v_\iota - 1)$. In fact, total number of vertices used in the realization $\widehat{\rho}_0$ is $21n - 2$.

Step i+1. Consider labeled meta-codes

$$\widehat{\mathfrak{C}}_i = \left\langle Y^i_{-u-i}, X^i_{-u-i} \right\rangle, \cdots, \langle Y^i_0, X^i_0, Z^i \rangle, \cdots, \left\langle Y^i_{u+i}, X^i_{u+i} \right\rangle$$
$$\widehat{\mathfrak{C}}_{i+1} = \left\langle Y^{i+1}_{-u-i-1}, X^{i+1}_{-u-i-1} \right\rangle, \cdots, \left\langle Y^{i+1}_0, X^{i+1}_0, Z^{i+1} \right\rangle, \cdots, \left\langle Y^{i+1}_{u+i+1}, X^{i+1}_{u+i+1} \right\rangle$$

By previous steps, we already constructed the graph-realizations of $\widehat{\mathfrak{C}}_0, \cdots, \widehat{\mathfrak{C}}_i$ corresponding to labeled codes $\widehat{\rho}_0, \cdots, \widehat{\rho}_i$. In order to obtain a required realization of $\widehat{\mathfrak{C}}_{i+1}$, observe that all components of $\widehat{\rho}_{i+1}$ are obtained from the corresponding components of $\widehat{\rho}_i$ by definition-by-cases clauses 1-4 (see above). As for crucial clauses 1-3, note that finite list of orders T provides us with a constant $\mathrm{C}_3 > 0$ such that recursive definition-by-cases of any b_j^{i+1}, x_j^{i+1} and (obviously) q^{i+1} requires (see Corollaries 7, 8) graph-realization with at most C_3 new vertices. For example, consider definition of x_0^{i+1}. Let $\mathrm{R}_1^1, \cdots, \mathrm{R}_\zeta^1$, $\mathrm{R}_1^2, \cdots, \mathrm{R}_\theta^2$ and $\mathrm{R}_1^3, \cdots, \mathrm{R}_\xi^3$ $(\zeta, \theta, \xi \geq 0)$ be the $\mathcal{T}$-orders of the form 1, 2 and 3, respectively, occurring in the list T. Let $g_1^1, \alpha_1^1, h_1^1, \beta_1^1, \cdots, g_\zeta^1, \alpha_\zeta^1, h_\zeta^1, \beta_\zeta^1$, $g_1^2, \alpha_1^2, \beta_1^2, \cdots, g_\theta^2, \alpha_\theta^2, \beta_\theta^2$ and $g_1^3, \alpha_1^3, \beta_1^3, \cdots, g_\xi^3, \alpha_\xi^3, \beta_\xi^3$ be the corresponding parameters occurring in these orders. Now x_0^{i+1} is constructed by the following cases (cf. clauses 1-3 above).

$$
\begin{array}{lll}
x_0^{i+1} := & & \\
x_1^i + 1 & \text{if} & x_0^i = 1 \wedge \bigvee\limits_{\iota=1}^{\zeta} \left(g_\iota^1 = b_0^i \neq h_\iota^1 = b_1^i \wedge \alpha_\iota^1 = q^i\right) \\
1 & \text{if} & \left(x_0^i = 1 \wedge \bigvee\limits_{\iota=1}^{\zeta} \left(g_\iota^1 = b_0^i \neq h_\iota^1 \neq b_1^i \wedge \alpha_\iota^1 = q^i\right)\right) \\
\multicolumn{3}{l}{\quad \vee \left(x_0^i \neq 1 \wedge \bigvee\limits_{\iota=1}^{\zeta} \left(g_\iota^1 = b_0^i \neq h_\iota^1 \wedge \alpha_\iota^1 = q^i\right)\right) \vee \bigvee\limits_{\iota=1}^{\xi} \left(g_\iota^3 = b_0^i \neq b_{-1}^i \wedge \alpha_\iota^3 = q^i\right)} \\
x_1^i & \text{if} & x_0^i = 1 \wedge \bigvee\limits_{\iota=1}^{\theta} \left(g_\iota^2 = b_0^i \wedge \alpha_\iota^2 = q^i\right) \\
x_0^i - 1 & \text{if} & x_0^i \neq 1 \wedge \bigvee\limits_{\iota=1}^{\theta} \left(g_\iota^2 = b_0^i \wedge \alpha_\iota^2 = q^i\right) \\
x_0^i + 1 & \text{if} & \bigvee\limits_{\iota=1}^{\xi} \left(g_\iota^3 = b_0^i = b_1^i \wedge \alpha_\iota^3 = q^i\right) \\
x_0^i & \text{else} &
\end{array}
$$

All in all, the required labeled code

$$
\widehat{\rho}_{i+1} = \left\langle b_{-u-i-1}^{i+1}, x_{-u-i-1}^{i+1} \right\rangle, \cdots, \left\langle b_0^{i+1}, x_0^{i+1}, q^{i+1} \right\rangle, \cdots, \left\langle b_{u+i+1}^{i+1}, x_{u+i+1}^{i+1} \right\rangle
$$

can be obtained by adding at most $\mathrm{C}_3 \cdot (4(u+i+1)+3)$ new vertices to $4(u+i+1)+3$ vertices of $\widehat{\mathfrak{C}}_{i+1}$ together with the vertices of previous realizations of $\widehat{\mathfrak{C}}_0, \cdots, \widehat{\mathfrak{C}}_i$. Summing up, the realization $\widehat{\rho}_0, \widehat{\rho}_1, \cdots, \widehat{\rho}_w$ of the sequence $\widehat{\mathfrak{C}}_0, \widehat{\mathfrak{C}}_1, \cdots, \widehat{\mathfrak{C}}_w$ requires less than

$$
\begin{array}{l}
21n - 2 + (\mathrm{C}_3 + 1)\left(4\left(u(w-1) + \frac{1}{2}w(w+1) - 1\right) + 3(w-1)\right) \\
\quad < 41472\,(\mathrm{C}_1)^2\,(2\mathrm{C}_3 + 1)\,n^{4\mathrm{C}_2}
\end{array}
$$

vertices. Finally, the alleged tautology test can be expressed in form $\widehat{\tau}\left(\widehat{\rho}_w\right) = \overset{1}{\boxed{1}}$, since $\mathcal{T}\left(\Delta\left(\mathbf{z}\right)\right) = \widehat{\tau}\left(\widehat{\rho}_w\right)$. So from the assumption of the lemma we obtain

$$\Delta\left(\mathbf{z}\right) \equiv \top \leftrightarrow q^w = 1 \wedge b_0^w = 1 \wedge x_0^w = 1 \wedge \bigwedge_{0 \neq \iota = -(u+w)}^{u+w} \left(b_\iota^w = 0 \wedge x_\iota^w = 1\right)$$

where $u + w = 144\mathrm{C}_1 \cdot n^{2\mathrm{C}_2} + 6n - 2$. Now by Lemma 6 (8, 10), there exists a quasi-polynomial t_0 such that

$$\begin{aligned} & t_0\left(\mathbf{z}^*\right) = 0 \\ \leftrightarrow\ & q^w - 1 = 0 \wedge b_0^w - 1 = 0 \wedge x_0^w - 1 = 0 \wedge \bigwedge_{0 \neq \iota = -(u+w)}^{u+w} \left(b_\iota^w = 0 \wedge x_\iota^w - 1 = 0\right) \end{aligned}$$

and (by previous estimates)

$$\begin{aligned} \partial\left(t_0\right) &< 41472\left(\mathrm{C}_1\right)^2\left(2\mathrm{C}_3 + 1\right) n^{4\mathrm{C}_2} + 3\left(u + w + 2\right) \\ &= 41472\left(\mathrm{C}_1\right)^2\left(2\mathrm{C}_3 + 1\right) n^{4\mathrm{C}_2} + 3\left(144\mathrm{C}_1 \cdot n^{2\mathrm{C}_2} + 6n\right) \\ &< \left(6n\right)^{4\mathrm{C}_2+1}, \text{ provided that } n > \frac{165888\left(\mathrm{C}_1\right)^2\left(\mathrm{C}_3 + 2\right)}{6^{4\mathrm{C}_2+1}} \end{aligned}$$

Moreover, every clause 1-3 can raise any given x_ι at most by 1 Hence $x_j^i \leq 3n + w$ holds for every x_j^i involved in the construction of $t_0\left(\mathbf{z}^*\right)$. Other parameters, i.e. b_j^i and q^i are bounded by $\max\left(m, k\right)$. Hence $t_0 \in \mathfrak{Q}_{6n}^{(\mathrm{C}_0)}$ for $\mathrm{C}_0 := 4\mathrm{C}_2 + 1$ and $n > N_0 := \max\left(m, k, \left\lfloor 165888\left(\mathrm{C}_1\right)^2\left(\ \mathrm{C}_3 + 2\right) 6^{-\mathrm{C}_0}\right\rfloor + 1\right)$, Q.E.D. $\square$

In order to complete the proof of Theorem 22, it will suffice to combine Lemma 30 and Remark 26 to Lemma 23. To this end, we argue *ad contrario*. Suppose $\mathbf{TAU3} \leq \mathbf{P}$. Starting from this assumption we have to refute **C3**. So let C_0 and N_0 be as in Lemma 30. Set $c := 2\ c_0$ and $N := N_0$, and let $n > N$. Take $s'_\iota, t'_\iota \in \mathfrak{Q}_{3n}^{(3)}$, $1 \leq \iota \leq 3n$, as in Remark 26, and quasi-polynomial t_0 from Lemma 30. Let $t := t_0\left(v_1 := t'_1, v_2 := s'_1, \cdots, v_{6n-1} := t'_{3n}, v_{6n} := s'_{3n}\right)$ and observe that $\partial\left(t\right) < \left(6n\right) \cdot n^3 + \left(6n\right)^{\mathrm{C}_0} < \left(3n\right)^{2\mathrm{C}_0} = \left(3n\right)^{\mathrm{C}}$, while $\varrho\left(t\right) < n^3 + \left(6n\right)^{\mathrm{C}_0} < \left(3n\right)^{2\ \mathrm{C}_0} = \left(3n\right)^{\mathrm{C}}$. That zero-set of such quasi-polynomial t coincides with the one of $\Phi_n^?$ on every $D \in \mathfrak{D}_{(3n)^{\mathrm{C}}}$ follows by Lemma 6 (12), Lemma 30, Lemma 23 and Remark 26. Hence **C3** fails. Q.E.D. ■

Remark 30 *Lemma 30 holds true in the sublanguage $\mathcal{L}_0^? \subset \mathcal{L}^?$ that includes only ? and unary operations $x + 1$ and $x - 1$, instead of binary operations $x + y$ and $x - y$. In the only non-trivial cases concerning conditions $b_i = b_{\iota+1}$ and $b_i \neq b_{\iota+1}$ from clauses 1-3, the corresponding tests can be carried out by separate recursion, without using $b_i - b_{\iota+1}$. However, $x + y$ and $x - y$ are*

essential for Lemma 23.

Remark 31 *It is readily seen that Lemma 30 admits a following generalization, where* $\mathbb{N}^m_{|n|} = \left(\mathbb{N}_{|n|}\right)^m$*, while specifying plain upper bounds as upper bounds with respect to plain input length* $\#(x_1, \cdots, x_m) := m-1+x_1+\cdots+x_m$*. Suppose* $\varphi : \mathbb{N}^m \to \mathbb{N}$ *be any m-ary total recursive function with polynomial-time plain upper bound. There are* $\mathrm{C}, N \in \mathbb{N}^+$ *such that for any* $n > N$*, the restriction of* φ *to* $\mathbb{N}^m_{|n|}$ *is representable by a m-ary quasi-polynomial (in fact, in* $\mathcal{L}^?_0$*) whose computable complexity does not exceed* n^{C} *. On the other hand, recall (see Lemma 17 above) that every quasi-polynomial whose computable complexity is polynomial in n is computable by a register machine whose weight is polynomial in n. Summing up, this shows that the notion of computable complexity, in* $\mathcal{L}^?$ *, provides us with a plausible algebraic characterization of polynomial-time complexity.*

4.3 Conclusions

Theorems 21, 22 show that **C3** is an approximation of the natural conjecture $\mathbf{P} \neq \mathbf{NP}$. For if **C3** holds, then $\mathbf{P} \neq \mathbf{NP}$ (see Theorem 22). Should otherwise **C3** fail then, by Theorem 21, holds a suitable weak form of $\mathbf{P} = \mathbf{NP}$. This approximation is purely algebraic by nature, except that the underlying language includes one non-familiar operation ?. Now **C3** says that for arbitrarily large natural numbers n, no quasi-polynomial of small complexity has the same zero-set as a distinguished very complex quasi-polynomial $\Phi^?_n$, in every normed domain D of a suitable characteristic. Thus in order to establish **C3**, it would suffice to prove its specification to simplest zero-characteristic cases $D := \mathbb{R}$ or $D := \mathbb{C}$, or else any finite field D. To this end, in each case in question, we will try to convert quasi-polynomials to ordinary polynomials and/or systems of polynomial equations which may include multiplication instead of ?. This thread is called ?-elimination below.

5 ?-elimination in $\mathbb{R}$

In this section we consider zero-sets of quasi-polynomials in the normed domain $\mathbb{R}$. This domain, as well as $\mathbb{C}$ (see next section), is supplied with natural topology that could provide background for a proof of the desired contradiction. Now, in $\mathbb{R}$, an obvious distinction between polynomials and quasi-polynomials is that polynomials are continuous, whereas quasi-polynomials generally are not. For example, no real polynomial has the same values as

quasi-polynomial $x?1$ representing plain characteristic function

$$\chi(x) = \begin{cases} 0 & \text{if} \quad x = 0 \\ 1 & \text{else} \end{cases}$$

However, its zero-set $\{x \in \mathbb{R} \mid \chi(x) = 0\}$ coincides with the one of polynomial x. That is, $\chi(x) = 0 \Leftrightarrow x = 0$ holds in $\mathbb{R}$, although $\chi(x) \equiv x$ obviously fails. Analogously, our basic quasi-polynomials $\Phi_n^?$ are discrete-valued, and hence they cannot be fully converted to real polynomials. On the other hand, $\Phi_n^? = 0 \underset{\mathbb{R}}{\Leftrightarrow} \Phi_n^* = 0$ holds for real polynomials $\Phi_n^* := \sum\limits_{f \in [\mathbf{n} \to \mathbf{3}]} \prod\limits_{i \leq j \in \mathbf{n}} \left(x_{f(i),i} + x_{f(j),j}\right)^2$. Keeping this in mind, for any $\ell \in \mathbb{N}^+$, denote by $\Sigma\Pi_{\ell,?}$ the set of ℓ-ary quasi-polynomials $t = t(\overrightarrow{x})$ such that $t = 0 \underset{\mathbb{R}}{\Leftrightarrow} g = 0$ holds for some real polynomial $g = g(\overrightarrow{x})$ of the form $\sum\limits_{i \in I} \prod\limits_{j \in J(i)} f_{i,j}^2$ for $f_{i,j} \in \mathbb{R}^1[x_1, \cdots, x_\ell]$. Thus, in particular, $\Phi_n^? \in \Sigma\Pi_{3n,?}$. Now suppose $t = t(\overrightarrow{x}) \in \Sigma\Pi_{\ell,?}$. We wish to construct a special solution $h = h(\overrightarrow{x}) \in \mathbb{R}[x_1, \cdots, x_\ell]$ to the equation $t = 0 \underset{\mathbb{R}}{\Leftrightarrow} h = 0$, whose shape explicitly depends on the one of t. Loosely speaking, we argue by recursion on the number of ?-occurrences in t. Note that a natural zero-set preserving translation of $\alpha?\beta+\gamma$ as, say, $(\alpha^2+\gamma^2)\left((\beta+\gamma)^2+\overline{\alpha}^2\right)$, where $\overline{\alpha} = 0 \underset{\mathbb{R}}{\Leftrightarrow} \alpha \neq 0$, is not possible in language of algebra. However, we can actually get rid of $\overline{\alpha}$ and replace $\alpha?\beta+\gamma$ by $(\alpha^2+\gamma^2)(\beta+\gamma)$, provided that $\alpha?\beta+\gamma$ is a subterm of t in question. This is where topological structure of the chosen normed domain becomes crucial. To grasp the method, consider an example, as follows.

Example 32 *Suppose* $t = \alpha?\beta?(\beta-\gamma)+(\beta-\gamma+\gamma?\delta)?\gamma?\delta \in \Sigma\Pi_{\ell,?}$, *where* $\alpha, \beta, \gamma, \delta \in \mathbb{R}^{(1)}[x_1, \cdots, x_\ell]$ *(Figure 2 shows the graph of* t*). For the sake of brevity we assume that* $\alpha, \beta, \gamma, \delta$ *are linear independent.*

First off, we assign labels ε_1, ε_2, ε_3, ε_4 *to the roots of the four ?-subterms* $\alpha?\beta$, $\gamma?\delta$, $\alpha?\beta?(\beta-\gamma)$, $(\beta-\gamma+\gamma?\delta)?\gamma?\delta$, *respectively (see Figure 2 for the associative order). Regard* ε_i, $i = 1, 2, 3, 4$, *as boolean variables ranging over* $\{0, 1\}$ *. Denote by* $\overline{\varepsilon_1}$, $\overline{\varepsilon_2}$, $\overline{\varepsilon_3}$, $\overline{\varepsilon_4}$ *negative (dual) literals such that* $\overline{\varepsilon_i} = 1 - \varepsilon_i$. *We wish to convert* $t = 0$ *to a natural system of linear equations enriched by coefficients from the set* $\{\varepsilon_i, \overline{\varepsilon_j} \mid i, j = 1, 2, 3, 4\}$. *These* ***defining equations*** *are as follows.*

[0] $\varepsilon_1 \cdot \alpha = 0$
[1] $\varepsilon_2 \cdot \gamma = 0$
[2] $\varepsilon_3 \cdot \overline{\varepsilon_1} \cdot \beta = 0$
[3] $\varepsilon_4 \cdot (\beta - \gamma + \overline{\varepsilon_2} \cdot \delta) = 0$
[4] $\overline{\varepsilon_3} \cdot (\beta - \gamma) + \overline{\varepsilon_4} \cdot \overline{\varepsilon_2} \cdot \delta = 0$

Explanation. [0] *means that* $\alpha = 0$ *is included in the list of defining equations*

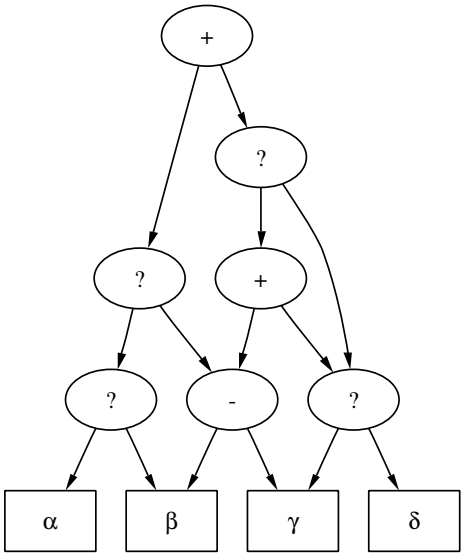

Fig. 2. Structure of the example

iff $\varepsilon_1 = 1$ *(dual option* $\varepsilon_1 = 0$ *corresponds to non-algebraic inequation* $a \neq 0$*, which will be eliminated later). Note that* α *is the value of the main left-hand side subterm of the subterm* $\alpha?\beta$ *labeled by* ε_1*. Analogously,* [1] *means that* $\gamma = 0$ *is a defining equation iff* $\varepsilon_1 = 1$*, where* γ *is the value of the main left-hand side subterm of the subterm* $\gamma?\delta$ *labeled by* ε_2 *.* [2] *means that* $\overline{\varepsilon_1} \cdot \beta = 0$*, i.e.* $0 = 0$ *or* $\beta = 0$*, is included in the list of defining equations iff* $\varepsilon_3 = 1$*. Note that* $\overline{\varepsilon_1} \cdot \beta$ *is the value(s) of the main left-hand side subterm of the subterm* $\alpha?\beta?\,(\beta - \gamma)$ *labeled by* ε_3*.* [3] *means that* $\beta - \gamma + \overline{\varepsilon_2} \cdot \delta = 0$ *, i.e.* $\beta - \gamma = 0$ *or* $\beta - \gamma + \delta = 0$*, is included in the list of defining equations iff* $\varepsilon_4 = 1$*. Note that* $\beta - \gamma + \overline{\varepsilon_2} \cdot \delta$ *is the value(s) of the main left-hand side subterm of the subterm* $(\beta - \gamma + \gamma?\delta)?\gamma?\delta$ *labeled by* ε_4*. Finally,* [4] *yields the last defining equation* $\overline{\varepsilon_3} \cdot (\beta - \gamma) + \overline{\varepsilon_4} \cdot \overline{\varepsilon_2} \cdot \delta = 0$*, i.e.* $0 = 0$*,* $\beta - \gamma + \delta = 0$*,* $\beta - \gamma = 0$ *or* $\delta = 0$*, whose left-hand side provides us with the value(s) of* t*. The correlated table of equations and inequations is attached below.*

ε_1	ε_2	ε_3	ε_4	[0]	[1]	[2]	[3]	[4]
0	0	0	0	$\alpha \neq 0$	$\gamma \neq 0$	$\beta \neq 0$	$\beta-\gamma+\delta \neq 0$	$\beta-\gamma+\delta=0$
0	0	0	1	$\alpha \neq 0$	$\gamma \neq 0$	$\beta \neq 0$	$\beta-\gamma+\delta=0$	$\beta-\gamma=0$
0	0	1	0	$\alpha \neq 0$	$\gamma \neq 0$	$\beta=0$	$\beta-\gamma+\delta \neq 0$	$\delta=0$
0	0	1	1	$\alpha \neq 0$	$\gamma \neq 0$	$\beta=0$	$\beta-\gamma+\delta=0$	$0=0$
0	1	0	0	$\alpha \neq 0$	$\gamma=0$	$\beta \neq 0$	$\beta-\gamma \neq 0$	$\beta-\gamma=0$
0	1	0	1	$\alpha \neq 0$	$\gamma=0$	$\beta \neq 0$	$\beta-\gamma=0$	$\beta-\gamma=0$
0	1	1	0	$\alpha \neq 0$	$\gamma=0$	$\beta=0$	$\beta-\gamma \neq 0$	$0=0$
0	1	1	1	$\alpha \neq 0$	$\gamma=0$	$\beta=0$	$\beta-\gamma=0$	$0=0$
1	0	0	0	$\alpha=0$	$\gamma \neq 0$	$0 \neq 0$	$\beta-\gamma+\delta \neq 0$	$\beta-\gamma+\delta=0$
1	0	0	1	$\alpha=0$	$\gamma \neq 0$	$0 \neq 0$	$\beta-\gamma+\delta=0$	$\beta-\gamma=0$
1	0	1	0	$\alpha=0$	$\gamma \neq 0$	$0=0$	$\beta-\gamma+\delta \neq 0$	$\delta=0$
1	0	1	1	$\alpha=0$	$\gamma \neq 0$	$0=0$	$\beta-\gamma+\delta=0$	$0=0$
1	1	0	0	$\alpha=0$	$\gamma=0$	$0 \neq 0$	$\beta-\gamma \neq 0$	$\beta-\gamma=0$
1	1	0	1	$\alpha=0$	$\gamma=0$	$0 \neq 0$	$\beta-\gamma=0$	$\beta-\gamma=0$
1	1	1	0	$\alpha=0$	$\gamma=0$	$0=0$	$\beta-\gamma \neq 0$	$0=0$
1	1	1	1	$\alpha=0$	$\gamma=0$	$0=0$	$\beta-\gamma=0$	$0=0$

It is readily seen that for all $x_1, \cdots, x_\ell \in \mathbb{R}$

$$t=0 \Leftrightarrow (\exists \varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4 \in \{0,1\})\,([0] \wedge [1] \wedge [2] \wedge [3] \wedge [4]) \qquad (*)$$

Moreover, we can exclude 8 vectors $(\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4)$*:* $(0,0,0,0)$*,* $(0,1,0,0)$*,* $(0,1,0,1)$*,* $(0,1,1,0)$*,* $(1,0,0,0)$*,* $(1,0,0,1)$*,* $(1,1,0,0)$ *,* $(1,1,0,1)$*, whose rows* $[0], [1], [2], [3], [4]$ *are inconsistent (see the table). Furthermore, in each of the remaining 8 rows we can delete all inequations (see the lemma below), and afterwards delete also the last row, as it strengthens the (previous) raw of* $(1,1,1,0)$*. Thus* $(*)$ *actually reduces to*

$$t=0 \Leftrightarrow (\beta-\gamma=0 \wedge \delta=0) \vee (\beta=0 \wedge \gamma-\delta=0) \vee (\alpha=0 \wedge \beta-\gamma+\delta=0) \vee (\beta=0 \wedge \delta=0) \vee (\beta=0 \wedge \gamma=0) \vee (\alpha=0 \wedge \delta=0) \vee (\alpha=0 \wedge \gamma=0)$$

which yields a desired simple polynomial solution

$$t = 0 \underset{\mathbb{R}}{\Leftrightarrow} (\alpha^2+\gamma^2)\cdot(\alpha^2+\delta^2)\cdot\left(\alpha^2+(\beta-\gamma+\delta)^2\right)\cdot(\beta^2+\gamma^2)\cdot(\beta^2+\delta^2)\cdot \left(\beta^2+(\gamma-\delta)^2\right)\cdot\left(\delta^2+(\beta-\gamma)^2\right)=0 \qquad (**)$$

Furthermore, we wish to express this expansion in algebraic-combinatorial terms. Consider five collections $\mathfrak{F}_0 - \mathfrak{F}_5$ *of sets of natural numbers:*

$$\mathfrak{F}_0 := \{\emptyset\} \qquad \mathfrak{F}_1 := \{\emptyset\} \qquad \mathfrak{F}_2 := \{\{\emptyset\}, \{1\}\} \qquad \mathfrak{F}_3 := \{\{\emptyset\}, \{2\}\},$$
$$\mathfrak{F}_4 := \{\{\emptyset\}, \{3\}, \{2,4\}\}$$

and five functions $\mathfrak{f}_i : \mathfrak{F}_i \to \mathbb{R}^1[x_1, \cdots, x_\ell]$, $i = 0, 1, 2, 3, 4$*:*

$$\mathfrak{f}_0(\emptyset) := \alpha \qquad \mathfrak{f}_1(\emptyset) := \gamma \qquad \mathfrak{f}_2(X) := \begin{cases} 0 & \text{if} \quad X = \{\emptyset\} \\ \beta & \text{if} \quad X = \{1\} \end{cases}$$

$$\mathfrak{f}_3(X) := \begin{cases} \beta - \gamma & \text{if} \quad X = \{\emptyset\} \\ \delta & \text{if} \quad X = \{2\} \end{cases}$$

$$\mathfrak{f}_4(X) = \begin{cases} 0 & \text{if} \quad X = \{\emptyset\} \\ \beta - \gamma & \text{if} \quad X = \{3\} \\ \delta & \text{if} \quad X = \{2,4\} \end{cases}$$

For any $Y \subseteq \{1,2,3,4\}$ *and* $0 \leq k \leq 4$*, set* $\varphi_k(Y) := \sum\limits_{Y \supseteq X \in \mathfrak{F}_k} \mathfrak{f}_k(X)$*. Note that* $\mathfrak{S}(Y) := \{\varphi_k(Y) = 0 \mid k+1 \in Y \cup \{5\}\} \cup \{\varphi_k(Y) \neq 0 \mid k+1 \notin Y\}$ *coincides with the system of equations and inequations of the raw of the table (see above), given by* Y*-cocharacteristic* ε*-vector* $(\overline{\chi}_Y(1), \overline{\chi}_Y(2), \overline{\chi}_Y(3), \overline{\chi}_Y(4))$ *for* $\overline{\chi}_Y(i) := \begin{cases} 0 & \text{if} \quad i \in Y \\ 1 & \text{else} \end{cases}$*. This readily follows from* $[0] - [4]$*, since every* $\varphi_k(Y)$ *occurring in the table in question is obtained from the labeled left-hand side polynomial of* $[k]$ *by* $\varepsilon_i := \overline{\chi}_Y(i)$*, for all* $i \leq k$*, and* $\varepsilon_{k+1} := 1$*, if* $k < 4$*, - which covers our definition of* $\varphi_k(Y)$ *via* $\mathfrak{F}_k$*,* $\mathfrak{f}_k$ *(see above). Denote by* $\mathrm{Con}(Y)$ *an expression stating that system* $\mathfrak{S}(Y)$ *is consistent, i.e. has a solution in* $\mathbb{R}^\ell$*. By previous polynomial characterization of* $t = 0$*, this yields*

$$t = 0 \Leftrightarrow (\exists Y \subseteq \{1,2,3,4\})(\mathrm{Con}(Y) \wedge (\forall i \in Y \cup \{5\})(\varphi_{i-1}(Y) = 0)), \text{ in } \mathbb{R}.$$

Lemma 33 *Let* $t \in \Sigma\Pi_{\ell,?}$*. Suppose* $\alpha_1 \neq 0 \wedge \cdots \wedge \alpha_q \neq 0 \wedge \beta_1 = 0 \wedge \cdots \wedge \beta_m = 0 \Rightarrow t = 0$ *holds in* $\mathbb{R}$*, i.e. for all* $x_1, \cdots, x_\ell \in \mathbb{R}$*, where* $\alpha_i, \beta_j \in \mathbb{R}^1[x_1, \cdots, x_\ell]$ *are such that system* $\{\alpha_1 \neq 0, \cdots, \alpha_q \neq 0, \beta_1 = 0, \cdots, \beta_m = 0\}$ *is consistent. Then* $\beta_1 = 0 \wedge \cdots \wedge \beta_m = 0 \Rightarrow t = 0$ *also holds in* $\mathbb{R}$*.*

Proof. Obviously, we can just as well assume that t is a polynomial of the form $\sum\limits_{i \in I} \prod\limits_{j \in J(i)} f_{i,j}^2$, where $f_{i,j} = f_{i,j}(\mathbf{x}) \in \mathbb{R}^1[x_1, \cdots, x_\ell]$ and $\#(I), \#\left(\bigcup\limits_{i \in I} J(i)\right) < \infty$, $\mathbf{x} = (x_1, \cdots, x_\ell)$. For any $1 \leq k \leq q$ let $V(\alpha_k) := \left\{\mathbf{x} \in \mathbb{R}^\ell \mid \alpha_k(\mathbf{x}) = 0\right\}$, $V(\beta_1, \cdots, \beta_m) := \left\{\mathbf{x} \in \mathbb{R}^\ell \mid \beta_1(\mathbf{x}) = \cdots = \beta_m(\mathbf{x}) = 0\right\}$. Now consider any $\mathbf{x}_0 \in$

$V(\beta_1,\cdots,\beta_m)$ and $i_0 \in I$. It will suffice to show that $f_{i_0,j_0}(\mathbf{x}_0)=0$, for some $j_0 \in J(i_0)$. Let $W := V(\beta_1,\cdots,\beta_m) - (V(\alpha_k)\cup\cdots\cup V(\alpha_q))$ and note that $W \neq \emptyset$, by the last assumption. Moreover, W is open in $\mathbb{R}^\ell$. Hence there exists closed linear interval $[\mathbf{a},\mathbf{b}]$, in $\mathbb{R}^\ell$, such that $[\mathbf{a},\mathbf{b}] \subset W$ and the points $\mathbf{x},\mathbf{a},\mathbf{b}$ are collinear. Take any $\mathbf{x} \in [\mathbf{a},\mathbf{b}]$. By the first assumption, $(\forall \mathbf{x} \in [\mathbf{a},\mathbf{b}])(t(\mathbf{x})=0)$, and hence $(\forall \mathbf{x} \in [\mathbf{a},\mathbf{b}])(\exists j \in J(i_0))(f_{i_0,j}(\mathbf{x})=0)$. By $\#(J(i_0)) < \infty$, there exist $\mathbf{y} \neq \mathbf{z} \in [\mathbf{a},\mathbf{b}]$ and $j_0 \in J(i_0)$ such that $f_{i_0,j_0}(\mathbf{y}) = f_{i_0,j_0}(\mathbf{z}) = 0$. Since $\mathbf{x},\mathbf{a},\mathbf{b}$ are collinear, it holds $f_{i_0,j_0}(\mathbf{x})=0$, Q.E.D. $\square$

Definition 34 *In the sequel we use abbreviations* $\mathbf{k}=\{1,\cdots,k\}$, $\wp(X)=\{Y \mid Y \subseteq X\}$. *In particular* $\{\emptyset\}=\wp(\mathbf{0})$. *Consider* n, C *and* $m < (3n)^{\mathrm{C}}$ *and:*

- *sets* $\mathfrak{F}_0,\cdots,\mathfrak{F}_m$ *with* $(\forall 0 \leq k \leq m)(\mathfrak{F}_k \subseteq \wp(\mathbf{k}) \wedge \#(\mathfrak{F}_i) < (3n^{\mathrm{C}}))$
- *functions* $\mathfrak{f}_0,\cdots,\mathfrak{f}_m$ *with* $(\forall 0 \leq k \leq m)\left(\mathfrak{f}_k : \mathfrak{F}_k \to \mathbb{Z}^{(1)}_{\left|(3n)^{\mathrm{C}}\right|}[x_1,\cdots,x_{3n}]\right)$

For any $Y \subseteq \mathbf{m}$ *and* $0 \leq k \leq m$ *let:*

- $\varphi_k(Y) := \sum\limits_{Y \supseteq X \in \mathfrak{F}_k} \mathfrak{f}_k(X)$
- $\mathrm{Con}(Y) :\Leftrightarrow$
  $(\forall i \in Y \cup \{m+1\})(\forall 0 < j < i)(\varphi_{i-1}(Y) \in [\![\varphi_{j-1}(Y)]\!] \to j \in Y)$
  $\wedge (\forall 1 < i \leq m)(\varphi_{i-1}(Y) \in [\![\{\varphi_{j-1}(Y) \mid i > j \in Y\}]\!] \to i \in Y)$

Denote by $\Pi\Sigma^{(\mathrm{C})}_{3n,?}$ *the set of* $3n$*-ary quasi-polynomials* t *such that*

$$t=0 \Leftrightarrow \prod_{\substack{Y \subseteq \mathbf{m} \\ \mathrm{Con}(Y)}} \sum_{i \in Y \cup \{m+1\}} (\varphi_{i-1}(Y))^2 = 0, \textit{ i.e. equivalently}$$

$$t=0 \Leftrightarrow (\exists Y \subseteq \mathbf{m})(\mathrm{Con}(Y) \wedge (\forall i \in Y \cup \{m+1\})(\varphi_{i-1}(Y)=0))$$

holds in $\mathbb{R}$ *for some* $m < (3n)^{\mathrm{C}}$, $\mathfrak{F}_0,\cdots,\mathfrak{F}_m$ *and* $\mathfrak{f}_0,\cdots,\mathfrak{f}_m$, *as above.*

Denote by $\Pi\Sigma^{(\mathrm{C})}_{3n,??}$ *the set of* $3n$*-ary quasi-polynomials* $t_1?\cdots?t_\ell$ *such that* $\ell < (3n)^{\mathrm{C}}$ *and* $t_1,\cdots,t_\ell \in \Pi\Sigma^{(\mathrm{C})}_{3n,?}$. *Note that* $t_1?\cdots?t_\ell = 0 \Leftrightarrow t_1 \cdot \ldots \cdot t_\ell = 0 \Leftrightarrow t_1=0 \vee \cdots \vee t_\ell = 0$ *holds in* $\mathbb{R}$ *(see Lemma 6 (7) above).*

Lemma 35 *For any* $n,\mathrm{C} \in \mathbb{N}^+$, *it holds* $\mathfrak{Q}^{(\mathrm{C})}_{3n} \cap \Sigma\Pi_{3n,?} \subseteq \Pi\Sigma^{(\mathrm{C})}_{3n,??}$.

Proof. We argue by induction on the number of ?-occurrences in a given quasi-polynomial $t \in \mathfrak{Q}^{(\mathrm{C})}_{3n} \cap \Sigma\Pi_{3n,?}$. Obviously, if t is ?-free then t is in $\Pi\Sigma^{(\mathrm{C})}_{3n,?}$, and hence in $\Pi\Sigma^{(\mathrm{C})}_{3n,??}$. Otherwise, suppose $t = t_1?\cdots?t_\ell$ be maximal expansion of this shape. It will suffice to prove $t_\iota \in \Pi\Sigma^{(\mathrm{C})}_{3n,?}$, for all $1 \leq \iota \leq \ell < (3n)^{\mathrm{C}}$. So let $t' := t_\iota$, $1 \leq \iota \leq \ell$. Without loss of generality suppose $t' = f?g+h$. This case just summarizes Example 33 (see above). To put it more exactly, we enumerate all ?-occurrences in t' such that the root of any ?-subterm a appears later than

the roots of all ? -subterms of a. Moreover, we supply the resulting ?-numbers $0 < i \leq m$ with labels ε_i (cf. Example 33). Obviously $m < \partial(t) \leq (3n)^{\mathrm{C}}$. Furthermore, with every label ε_i we correlate a defining equation of the shape $[i-1]\ \varepsilon_i \cdot \alpha_{i-1} = 0$, and add the concluding defining equation $[m]\ \alpha_m = 0$, where α_k, $0 \leq k \leq m$, are linear polynomials which may contain as coefficients dual labels $\overline{\varepsilon}_i$ for $i \leq k$. The construction of α_k runs along the natural order on k as shown in Example 33 (cf. $[0]-[4]$), except rewriting $\mathbb{R}^{(1)}[x_1, \cdots, x_\ell]$ to $\mathbb{Z}^{(1)}[x_1, \cdots, x_{3n}]$, since coefficients of the polynomials involved are obtained from 1 by $+$ and $-$. Note that all these coefficients actually arise in the process of computation of $t' = t(x_1, \cdots, x_{3n})$ in the domain $\mathbb{Z}$. Hence we can further strengthen $\mathbb{Z}^{(1)}[x_1, \cdots, x_{3n}]$ to $\mathbb{Z}^{(1)}_{\left|(3n)^{\mathrm{C}}\right|}[x_1, \cdots, x_{3n}]$, since $\varrho(t) \leq (3n)^{\mathrm{C}}$. Note that any α_k in question arises from the main left-hand subterm of the subterm labeled by ε_{k+1}, if $k < m$, else from t', by successively adding coefficients $\overline{\varepsilon}_i$ to all vertices of the right-hand side subterms whose roots are labeled by ε_i, and simultaneously deleting all vertices occurring in the corresponding left-hand side subterms, while moving downwards from the root to the leafs. Hence every α_k is a term of the language with variables $x_1, \cdots, x_{3n}$, constant 1, operations $x + y$, $x - y$ and $\overline{\varepsilon}_i \cdot x$, where $i \leq k$. Since $\partial(t') \leq (3n)^{\mathrm{C}}$, the term-complexity of α_k in this language does not exceed $(3n)^{\mathrm{C}}$, either. This completes the construction of the system of defining equations $[0]-[m]$. The correlated table of polynomial equations and inequations is obtained by testing arbitrary assignments $\varepsilon_i \in \{0, 1\}$ as shown in Example 33. In this table, we first delete all inconsistent rows. By Lemma 34 (see above), we further delete all remaining inequations. Generally speaking, at this stage we already arrive at an expansion of t as a suitable product of polynomials of degree ≤ 2, that has the same zero-set as t. To complete the proof, we have to construct, for every t' in question, the required specification via $\mathfrak{F}_0, \cdots, \mathfrak{F}_m$ and $\mathfrak{f}_0, \cdots, \mathfrak{f}_m$. First off, we let $\mathfrak{F}_0 := \{\emptyset\}$ and $\mathfrak{f}_0(\emptyset) := \alpha_0$. Furthermore, for any $0 < k \leq m$, any α_k, we let $\{\emptyset\} \in \mathfrak{F}_k$ and set $\{i_1, \cdots, i_q\} \in \mathfrak{F}_k$ for every maximal coefficient-product $\overline{\varepsilon}_{i_1} \cdot \cdots \cdot \overline{\varepsilon}_{i_q}$ occurring in α_k (see the term-interpretation above); note that $\{i_1, \cdots, i_q\} \subseteq \mathbf{k}$. This completes our definition of $\mathfrak{F}_k \subseteq \wp(\mathbf{k})$. By $\partial(\alpha_k) \leq (3n)^{\mathrm{C}}$ (see above) we have $\#(\mathfrak{F}_k) \leq (3n)^{\mathrm{C}}$. As for the correlated function $\mathfrak{f}_k : \mathfrak{F}_k \to \mathbb{Z}^{(1)}_{\left|(3n)^{\mathrm{C}}\right|}[x_1, \cdots, x_{3n}]$, note that α_k is convertible to the uniquely determined $\beta_0 + \sum\limits_{j \in J} \overline{\varepsilon}_{i_{j_1}} \cdot \cdots \cdot \overline{\varepsilon}_{i_{j_q}} \cdot \beta_j$ such that for every $j \in J$, $\emptyset \neq \left\{i_{j_1}, \cdots, i_{j_q}\right\} \in \mathfrak{F}_k$ and $\beta_0, \beta_j \in \mathbb{Z}^{(1)}_{\left|(3n)^{\mathrm{C}}\right|}[x_1, \cdots, x_{3n}]$; moreover $1 + \#(J) = \#(\mathfrak{F}_k) \leq (3n)^{\mathrm{C}}$. We then set $\mathfrak{f}_k(\emptyset) := \beta_0$ and $\mathfrak{f}_k\left(\left\{i_{j_1}, \cdots, i_{j_q}\right\}\right) := \beta_j$, for every $j \in J$. By construction, this yields

$$t = 0 \Leftrightarrow (\exists Y \subseteq \mathbf{m})\,(\mathrm{Con}(Y) \wedge (\forall i \in Y \cup \{m+1\})\,(\varphi_{i-1}(Y) = 0))$$

(cf. analogous conclusion of Example 33). Q.E.D. $\square$

Condition 36 *Denote by* **C3L** *the following sentence. For every* $\mathrm{c} \in \mathbb{N}^+$

there are arbitrarily large $n \in \mathbb{N}^+$ *such that no quasi-polynomial from* $\Pi\Sigma^{(\mathrm{C})}_{3n,??}$ *has the same zero-set as* $\Phi^?_n$*, in* $\mathbb{R}$*. That is,* **C3L** *reads:*

$$\left(\forall \mathrm{C} \in \mathbb{N}^+\right)\left(\forall N \in \mathbb{N}^+\right)(\exists n > N)\left(\forall t \in \Pi\Sigma^{(\mathrm{C})}_{3n,??}\right)\left(\Phi^?_n = 0 \underset{\mathbb{R}}{\Leftrightarrow} t = 0\right)$$

Note that **C3L** *can be equivalently expressed in purely polynomial form:*

$$\left(\forall \mathrm{C} \in \mathbb{N}^+\right)\left(\forall N \in \mathbb{N}^+\right)(\exists n > N)\left(\forall t \in \Pi\Sigma^{(\mathrm{C})}_{3n}\right)\left(\Phi^*_n = 0 \underset{\mathbb{R}}{\Leftrightarrow} t = 0\right)$$

where $\Pi\Sigma^{(\mathrm{C})}_{3n}$ *denotes the set of real polynomials of the form* $t_1 \cdot \ldots \cdot t_\ell$ *in which every* t_ι *is* $\prod\limits_{\substack{Y \subseteq \mathbf{m} \\ \mathrm{Con}(Y)}} \sum\limits_{i \in Y \cup \{m+1\}} \left(\varphi_{i-1}(Y)\right)^2$*, for some* $\ell, m < (3n)^{\mathrm{C}}$ *and* $\mathfrak{F}_0, \cdots, \mathfrak{F}_m$*,* $\mathfrak{f}_0, \cdots, \mathfrak{f}_m$ *as in Definition 35 (see above).*

Theorem 37 ***Soundness****. If* **C3L** *fails, then* $\mathbf{TAU3} \in \mathbf{P/poly}$*.*

Proof. Since $\mathbb{Z} \subset \mathbb{R}$, we can argue as in the proof of Theorem 21, while revising Lemma 18, as follows. Actually, it suffices to prove that the following holds for sufficiently large n. *For any* $t \in \Pi\Sigma^{(\mathrm{C})}_{3n}$ *there exists a register machine* M *whose weight is smaller than* $n^{3\mathrm{C}+2}$*, and such that for any* $\mathbf{z} = (z_1, \cdots, z_{3n}) \in \mathbb{Z}^{3n}$*, the equation* $t(\mathbf{z}) = 0$ *is decidable by* M *in less than* $\|\mathbf{z}\| \cdot n^{5\mathrm{C}+2}$ *steps.* To this end, suppose $t = t_1 \cdot \ldots \cdot t_\ell$, $\ell < (3n)^{\mathrm{C}}$, where for every $1 \leq \iota \leq \ell$, $t_\iota = \prod\limits_{\substack{Y \subseteq \mathbf{m} \\ \mathrm{Con}(Y)}} \sum\limits_{i \in Y \cup \{m+1\}} \left(\varphi_{i-1}(Y)\right)^2$, for some $m < (3n)^{\mathrm{C}}$, $\mathfrak{F}_0, \cdots, \mathfrak{F}_m$ and $\mathfrak{f}_0, \cdots, \mathfrak{f}_m$ as in Definition 35. Since $t(\mathbf{z}) = 0 \leftrightarrow t_1(\mathbf{z}) = 0 \vee \cdots \vee t_\ell(\mathbf{z}) = 0$, it will suffice to show that every $t_\iota(\mathbf{z}) = 0$ is decidable in at most $O\left(\|\mathbf{z}\| \cdot n^{4\mathrm{C}+1}\right)$ steps by a suitable register machine M_ι of the weight $O\left(n^{2\mathrm{C}+1}\right)$. The corresponding verification of $t_\iota(\mathbf{z}) = 0$ runs by recursion on $i \leq m$ (cf. Example 33):

Basis; step 0**.** Let $\varphi_0(Y_0(\mathbf{z})) := \mathfrak{f}_0(\emptyset)[x_1 := z_1, \cdots, x_{3n} := z_{3n}]$ and put $1 \in Y(\mathbf{z}) :\Leftrightarrow \varphi_0(Y_0(\mathbf{z})) = 0$

Recursion; step k**.** Let $0 < k < m$, take already computed segment $Y_k(\mathbf{z}) := Y(\mathbf{z}) \cap \mathbf{k}$, set $\varphi_k(Y_k(\mathbf{z})) := \sum\limits_{Y_k(\mathbf{z}) \supseteq X \in \mathfrak{F}_k} \mathfrak{f}_k(X)[x_1 := z_1, \cdots, x_{3n} := z_{3n}]$ and put $k+1 \in Y(\mathbf{z}) :\Leftrightarrow \varphi_k(Y_k(\mathbf{z})) = 0$

Conclusion; step m**.** Take the computed set $Y(\mathbf{z}) \subseteq \mathbf{m}$, set $\varphi_m(Y(\mathbf{z})) := \sum\limits_{Y(\mathbf{z}) \supseteq X \in \mathfrak{F}_m} \mathfrak{f}_m(X)[x_1 := z_1, \cdots, x_{3n} := z_{3n}]$ and complete the verification by setting $t_\iota(\mathbf{z}) = 0 :\Leftrightarrow \varphi_m(Y(\mathbf{z})) = 0$

By standard methods, this procedure can be implemented by a register machine $\mathcal{M}$ of the weight $O\left(3n \cdot n^{\mathrm{C}} \cdot n^{\mathrm{C}}\right) = O\left(n^{2\mathrm{C}+1}\right)$. Note that only `times` loops are required in $\mathcal{M}$. Moreover, all entirely computing steps refer to the operations $+$ and $-$ with integer inputs and outputs $\leq \|\mathbf{z}\| \cdot n^{\mathrm{C}} \cdot n^{\mathrm{C}} =$

$\|\mathbf{z}\| \cdot n^{2\,\mathrm{C}}$. Furthermore, these operations are used at most $O(3n \cdot n^{\mathrm{C}} \cdot n^{\mathrm{C}}) = O(n^{2\mathrm{C}+1})$ times. Hence total number of the $\mathcal{M}$ -steps required does not exceed $O(\|\mathbf{z}\| \cdot n^{2\mathrm{C}} \cdot n^{2\mathrm{C}+1}) = O(\|\mathbf{z}\| \cdot n^{4\mathrm{C}+1})$, Q.E.D. $\square$

Theorem 38 ***Sufficiency***. *If* **C3L** *holds, then* $\mathbf{P} \neq \mathbf{NP}$.

Proof. By Theorem 22, it will suffice to infer $\neg$**C3L** from $\neg$**C3** $[\mathbb{R}]$. Recall that $\Phi_n^? = 0 \underset{\mathbb{R}}{\Leftrightarrow} \Phi_n^* = 0$, and hence $\Phi_n^? \in \Sigma\Pi_{3n}^?$ (see above). Now suppose $\neg$**C3** $[\mathbb{R}]$, i.e. there are $\mathrm{C}, N \in \mathbb{N}^+$ such that for any $n > N$ there exists $t \in \mathfrak{Q}_{3n}^{(\mathrm{C})}$ with $\Phi_n^? = 0 \underset{\mathbb{R}}{\Leftrightarrow} t = 0$. Hence $t \in \mathfrak{Q}_{3n}^{(\mathrm{C})} \cap \Sigma\Pi_{3n}^?$ and by Lemma 36, $t \in \Pi\Sigma_{3n,??}^{(\mathrm{C})}$, which yields $\neg$**C3L**, Q.E.D. $\square$

Claim 39 *For any quasi-polynomial* $t = t(\overrightarrow{x})$ *there is a polynomial* $t^* \in \mathbb{Z}[\overrightarrow{x}]$ *such that* $t = 0 \underset{\mathbb{R}}{\Leftrightarrow} t^* = 0$. *Moreover, the graph-complexity of* t^* *is polynomial in the graph-complexity of* t *. The proof runs along the lines of this section (it will be presented in more detail elsewhere).*

6 Geometric approach

Suppose $D = \mathbb{C}$. (In fact, we can just as well take as D any algebraically closed field $\mathbb{F}$, e.g. $\mathbb{F} \in \left\{\overline{\mathbb{Q}}, \mathbb{C}\right\}$.) Note that contrary to our previous real case, we cannot directly convert conjunctions, since $\alpha = 0 \wedge \beta = 0 \leftrightarrow \alpha^2 + \beta^2 = 0$ fails in $\mathbb{C}$. In particular, in $\mathbb{C}$, we cannot convert $\Phi_n^? = 0$ to a single equation $t = 0$. Instead, we present zero-set of $\Phi_n^?$ via variety, as usual in algebraic geometry. To this end, for any $f \in [\mathbf{n} \to \mathbf{3}]$ and $\mathbf{x} = (x_1, \cdots, x_{3n})$ we set

$$\Phi_f^{(n)} = \Phi_f^{(n)}(\mathbf{x}) := \prod_{i,j \in \mathbf{n}} (x_{f(i),i} + x_{f(j),j})$$

where $x_{i,j} := x_{i+3(j-1)}$. Let

$$I_\Phi^{(n)} := rad \left\langle \Phi_f^{(n)} \right\rangle_{f \in [\mathbf{n} \to \mathbf{3}]}$$

be the ideal generated by the $\Phi_f^{(n)}$ in the polynomial ring. For any set of polynomials $P \subseteq D[x_1, \cdots, x_{3n}]$ define the variety

$$\mathbf{V}(P) := \{\mathbf{x} \in D^{3n} \mid (\forall \alpha \in P)\, \alpha(\mathbf{x}) = 0\}$$

and let

$$\mathbf{V}_\Phi^{(n)} := \mathbf{V}(I_\Phi^{(n)}) = \{\mathbf{x} \in D^{3n} \mid \Phi_n^?(\mathbf{x}) = 0\}$$

$\Phi_f^{(n)}$ have linear zero-sets, i..e. $\Phi_f^{(n)}(\mathbf{x}) = 0 \to (\forall c \in D)\left(\Phi_f^{(n)}(c \cdot \mathbf{x}) = 0\right)$. Thus the variety $\mathbf{V}_\Phi^{(n)} \subset D^{3n}$ is the union of some irreducible subvarieties, and the corresponding irreducible expansion is uniquely determined. Moreover, we also have the unique set of the corresponding radical ideals. It follows that

$$I_\Phi^{(n)} = rad \prod_{j \in J} I_j = \bigcap_{j \in J} I_j$$

for uniquely determined ideals $I_j = \langle p_k \rangle_{k \in K_j}$, where p_k are linear polynomials. So the question to answer is about structural complexity of the resulting radical expansion, provided that $\mathbf{V}_\Phi^{(n)}$ coincides with the zero-set, in D, of a quasi-polynomial whose graph-complexity is polynomial in n. Presumably, this complexity should also be polynomial in n. On the other hand, $\Phi_n^?$ might be too complex to satisfy this hypothetical polynomial upper bound. A relevant lower bound result that can be easily proved reads that the number of irreducible subvarieties in $\mathbf{V}_\Phi^{(n)}$ is exponential in n. For the sake of brevity, we consider general DNF tautology problem by admitting, in $\Phi_n^?$, arbitrary functions $f \in [\mathbf{n} \to \mathbf{n}]$ and $\mathbf{x} = (x_1, \cdots, x_{n^2})$. The resulting modifications of $\Phi_f^{(n)}$, $I_\Phi^{(n)}$ and $\mathbf{V}_\Phi^{(n)}$ we denote by $\Phi_f^{(n,n)}$, $I_\Phi^{(n,n)}$ and $\mathbf{V}_\Phi^{(n,n)}$, respectively. (However, see Remark 42 below).

Theorem 40 *$\mathbf{V}_\Phi^{(n,n)}$ has at least n^{n-1} irreducible subvarieties.*

Proof. For any $\ell \in \{2, \cdots, n\}$ and $g : \{2, \cdots, n\} \to \{1, \cdots, n\}$ we let $\mathbf{x}_g^{(\ell)} := \ell\left(E_{\ell,1} - E_{g(\ell),\ell}\right)$, where $E_{i,j}$ denotes a $(n \times n)$-matrix having 1 at (i,j), else 0. Thus $D^{n \times n} \ni \mathbf{x}_g^{(\ell)} = \left(x_{i,j}^{(\ell)}\right)_{1 \le i,j \le n}$ for $x_{i,j}^{(\ell)} = \begin{cases} \ell & \text{if} \quad i = \ell \wedge j = 1 \\ -\ell & \text{if} \quad i = g(\ell) \wedge j = \ell \\ 0 & \text{else} \end{cases}$.

We claim that for any g as above, $\left\{\mathbf{x}_g^{(\ell)}\right\}_{\ell=2}^n$ is a basis for an irreducible subvariety of $\mathbf{V}_\Phi^{(n,n)}$. In fact, it is readily seen that $\sum\limits_{\ell=2}^n a_\ell \mathbf{x}_g^{(\ell)} \in \mathbf{V}_\Phi^{(n,n)}$ holds for any $a_1, \cdots, a_n \in D$. It remains to prove that the subspace generated by $\left\{\mathbf{x}_g^{(\ell)}\right\}_{\ell=2}^n$ is not contained in any larger subspace of $\mathbf{V}_\Phi^{(n,n)}$. To this end, it will suffice to show that $\left\{\mathbf{x}_g^{(\ell)}\right\}_{\ell=2}^n$ has no proper extension to another basis in $\mathbf{V}_\Phi^{(n,n)}$. Let $\mathbf{x} = (x_{i,j})_{1 \le i,j \le n} := \sum\limits_{\ell=2}^n \mathbf{x}_g^{(\ell)}$, $\mathbf{y} = (y_{i,j})_{1 \le i,j \le n} \in \mathbf{V}_\Phi^{(n,n)}$ and suppose that $\mathbf{x} + c \cdot \mathbf{y} \in \mathbf{V}_\Phi^{(n,n)}$ holds for every $c \in D$. Without loss of generality we can also assume $y_{i,j} = 0$ or $|y_{i,j}| > 2n$, for any $1 \le i, j \le n$. Consider two cases.

Case 1. Suppose that for some $i \in \{2, \cdots, n\}$, $y_{i,1} + y_{g(i),i} \neq 0$. Define f :

$\{1,\cdots,n\}\to\{1,\cdots,n\}$ by $f(k):=\begin{cases} i & \text{if} \quad k=1 \\ g(k) & \text{else} \end{cases}$. For any $c\in D$, consider the corresponding f-section of $\mathbf{x}+c\cdot\mathbf{y}$, i.e. a sequence

$$\begin{aligned}&\left\{x_{f(k),k}+c\cdot y_{f(k),k}\right\}_{k=1}^{n}\\ =&\left\{i+c\cdot y_{i,1},-2+c\cdot y_{g(2),2},\cdots,-i+c\cdot y_{g(i),i},\cdots,-n+c\cdot y_{g(n),n}\right\}\end{aligned}$$

By assumption, every $x_{f(k),k}+c\cdot y_{f(k),k}\neq 0$. Thus $(\forall c)\,\Phi_f^{(n,n)}(\mathbf{x}+c\cdot\mathbf{y})=0$ infers that there are $c_1\neq c_2\in D$ and $u\neq v\in\{1,\cdots,n\}$ such that

$$\begin{aligned}&x_{f(u),u}+x_{f(v),v}+c_1\cdot\left(y_{f(u),u}+y_{f(v),v}\right)=\\ &x_{f(u),u}+x_{f(v),v}+c_2\cdot\left(y_{f(u),u}+y_{f(v),v}\right)=0\end{aligned}$$

But this is only possible if $y_{f(u),u}+y_{f(v),v}=0=x_{f(u),u}+x_{f(v),v}$, and hence $u=1$, $v=i$ and $y_{f(u),u}+y_{f(v),v}=y_{i,1}+y_{g(i),i}=0$ - a contradiction.

Case 2. Suppose that for some $i,j\in\{2,\cdots,n\}$, $x_{i,j}=0\wedge y_{i,j}\neq 0$. So $1\neq j$. Define $f:\{1,\cdots,n\}\to\{1,\cdots,n\}$ by $f(k):=\begin{cases} j & \text{if} \quad k=1 \\ i & \text{if} \quad k=j \\ g(k) & \text{else} \end{cases}$, and consider the corresponding f-sections of $\mathbf{x}+c\cdot\mathbf{y}$, i.e.

$$\begin{aligned}&\left\{x_{f(k),k}+c\cdot y_{f(k),k}\right\}_{k=1}^{n}=\{j+c\cdot y_{j,1},-2+c\cdot y_{g(2),2},\cdots,-i+1\\ &+c\cdot y_{g(j-1),j-1},c\cdot y_{i,j},-j-1+c\cdot y_{g(j+1),j+1},\cdots,-n+c\cdot y_{g(n),n}\}\end{aligned}$$

Arguing as in previous case we arrive at $y_{i,j}=0$ - a contradiction.

Since the cases 1, 2 do not apply, $\mathbf{y}$ is generated by $\left\{\mathbf{x}_g^{(\ell)}\right\}_{\ell=2}^{n}$, and hence $\left\{\mathbf{x}_g^{(\ell)}\right\}_{\ell=2}^{n}$ generates an irreducible subvariety of $\mathbf{V}_\Phi^{(n,n)}$. Moreover, it is readily seen that different functions g generate different irreducible varieties. Hence there are at least n^{n-1} irreducible varieties in $\mathbf{V}_\Phi^{(n,n)}$, Q.E.D. $\square$

Remark 41 *By the same token, we can show that the number of irreducible subvarieties of* $\mathbf{V}_\Phi^{(n)}$ *is also exponential in* n. *To this end, we pass from general DNF tautology problem* **TAU** *to the required DNF3-restriction* **TAU3**. *To put it more exactly, we note that our basis* $\left\{\mathbf{x}_g^{(\ell)}\right\}_{\ell=2}^{n}$ *formalizes a tautology*

$$(\vartheta_2\wedge\vartheta_3\wedge\cdots\wedge\vartheta_n)\vee\neg\vartheta_2\wedge\neg\vartheta_3\wedge\cdots\wedge\neg\vartheta_n$$

and by standard approach rewrite this DNF to an equivalent DNF3.

7 Finite domains

Working in finite normed domains enables us to eliminate both the operation ? and norm-complexity ϱ. The latter reduces **C3** to purely algebraic condition **C3A** which, in turn, admits standard Π^0_2-interpretation **C3F** (see below).

Condition 42 *Denote by* $\mathfrak{G}^{(\mathrm{C})}_m$ *the set of* m*-ary quasi-polynomials whose graph-complexity does not exceed* m^{C}*. Let* **C3A** *arise by substituting* $\mathfrak{G}^{(\mathrm{C})}_{3n}$ *for* $\mathfrak{Q}^{(\mathrm{C})}_{3n}$ *in the condition* **C3***. That is,* **C3A** *reads (cf. Condition 18 above):*

$$(\forall \mathrm{C} \in \mathbb{N}^+)\,(\forall N \in \mathbb{N}^+)\,(\exists n > N)\left(\forall t \in \mathfrak{G}^{(\mathrm{C})}_{3n}\right)\left(\exists D \in \mathfrak{D}_{(3n)^{\mathrm{C}}}\right)\left(\Phi^{?}_n = 0 \underset{D}{\Leftrightarrow} t = 0\right)$$

In other words, **C3A** *strengthens* **C3** *by weakening algebraic complexity of* t *to its graph-complexity* $\partial(t)$*.*

Condition 43 *For any* $m > 1$*, let* $\mathbb{F}^+_m := \mathbb{Z}_p$ *for* $p = \mathrm{nextprime}(2m) = \min\{x \in \mathbb{P} \mid 2m < x\}$*. Denote by* **C3F** *a specification of* **C3A** *that is obtained by setting* $D := \mathbb{F}^+_{(3n)^{\mathrm{C}}}$ *(see Example 5 above). Obviously,* **C3F** *infers* **C3A***, while* **C3A** *infers* **C3***. Note that* **C3F** *is a* Π^0_2*-sentence.*

Theorem 44 *If* **C3F** *fails, then* $\mathbf{TAU3} \in \mathbf{P/poly}$*.*

Proof. The proof runs along the lines of Theorem 21 (see above). Suppose $\neg$**C3F**, i.e. there are $\mathrm{C}, N \in \mathbb{N}^+$ such that for every $n > N$ there exists a quasi-polynomial $t_0 \in \mathfrak{G}^{(\mathrm{C})}_{3n}$ such that $\Phi^{?}_n = 0 \Leftrightarrow t_0 = 0$ holds in $\mathbb{F}^+_{(3n)^{\mathrm{C}}} = \mathbb{Z}_p$. Without loss of generality we assume $\mathrm{C} \geq 3$. Then by Lemma 23 with $D = \mathbb{Z}$, it will suffice to show that for any $t \in \mathfrak{G}^{(\mathrm{C})}_{3n}$ and $p \in \mathbb{P}$, there exists a `register machine` $\mathcal{M}$ weight-polynomial in $\max(p, n)$ and computing the value $t(\mathbf{v}) \in \mathbb{Z}^{3n}_p$, for any input $\mathbf{v} = (\upsilon_1, \cdots \upsilon_{3n}) \in \mathbb{Z}^{3n}_p = (\mathbb{Z}_p)^{3n}$; moreover, the number of $\mathcal{M}$-steps required for the computation of $t(\mathbf{v})$ is also polynomial in $\max(p, n)$. But this is readily seen, since $+$ and $-$ from t are reduced modulo p. Q.E.D. $\square$

Corollary 45 *If either* **C3A** *or* **C3F** *fails, then* $\mathbf{TAU3} \in \mathbf{P/poly}$*. If either* **C3A** *or* **C3F** *holds, then so is* **C3***, and hence* $\mathbf{NP} \neq \mathbf{P}$*.*

Remark 46 ***?-elimination.*** *By (small) Fermat theorem, if* $p \in \mathbb{P}$ *and* $p \nmid a$ *then* $a^{p-1} \equiv 1 \mod p$*. Thus* $x^{p-1} = \left\{ \begin{array}{lll} 0 & \mathit{if} & x = 0 \\ 1 & \mathit{else} & \end{array} \right\} = sgn(x)$ *and hence* $x?y = x^{p-1} \cdot y$ *both hold in* $\mathbb{Z}_p$*. Now for any* m*-ary quasi-polynomial*

t, let $t_p^\star \in \mathbb{Z}[x_1, \cdots, x_m]$ be a polynomial that arises from t by successively replacing every occurrence $x?y$ by $x^{p-1} \cdot y$. By the above, $t = t_p^\star$ holds in $\mathbb{Z}_p$. Moreover, $\partial(t_p^\star) \leq \partial(t)(\lceil \log_2 p \rceil + 1)$, provided that x^{p-1} is formalized via fast exponentiation as $(\cdots(((x \cdot x) \cdot (x \cdot x)) \cdot ((x \cdot x) \cdot (x \cdot x)))\cdots)$. This enables us to replace in **C3F** *quasi-polynomials $t \in \mathfrak{G}_{3n}^{(\mathrm{C})}$ by polynomials $t_p^\star \in \mathbb{Z}[x_1, \cdots, x_{3n}]$ whose graph-complexity is still polynomial in n.*

Acknowledgements

We also thank Christoph Behle, Robert Kremser, Klaus-Jörn Lange and the anonymous referee for valuable inputs and hints how to improve the paper.

References

[C] : S. Cook, *The P versus NP Problem*, URL:http://www.claymath.org/Millennium_Prize_Problems/P_vs_NP/_objects/Official_Problem_Description.pdf

[Co] : David A. Cox and John B. Little and Don O'Shea, *Using Algebraic Geometry*, Springer-Verlag, NY 1998

[G] : L. Gordeev, *Proof theory and Post-Turing analysis*, Proc. Proof Theory in Computer Science, Dagstuhl 2001, LN in Comp. Sci. **2183** (2001), 130-152

[Ka] : R. M. Karp and R. J. Lipton. *Turing machines that take advice*, Enseign. Math. **28**:191-201, 1982.

[P] : E. Post, *Finite combinatory processes - formulation I*, Journ. Symb. Logic **1** (1936), 103-105

[Tu] : A. Turing, *On computable numbers, with an application to the Entscheidungsproblem*, Proc. London Math. Soc. **42** (1937), 230-265