Proof-sketch: Why NP is not P

L. Gordeev, FTICA, WSI f. Informatik
October 8, 2004, Tübingen/Falkensee
`gordeew@informatik.uni-tuebingen.de`

1 Introduction

The way is shown how to prove that **NP** is not **P**; it is not the proof proper yet, but what remains to be done is technical, though non-trivial, work along the lines of traditional combinatorics (see Attachments 6, 7 below). The underlying logic scheme is obvious – we assume that **NP** is **P** (actually in the weak form **TAU** $\subseteq$ **P/poly**, where **TAU** is the familiar co-**NP** complete propositional tautology problem[1]) and try to derive a contradiction by the appropriate chain of inferences. This chain consists of the four main inferences A, B, C, D which, loosely speaking, embed the discrete assumption **TAU** $\subseteq$ **P/poly** first into the real multi-dimensional continuum and then back into discrete combinatorics. These inferences are as follows (see also Overview 2.2 and Summary 3.3 below).

(A) The assumption is reduced to an algebraic sentence (S_A) stating that for sufficiently large n, there are "small" borel polynomials (P_n) having "regular" n^2-dim linear atoms and the same n^2-dim real zero-set (Z_n) as a fixed "large" polynomial Φ_n that characterizes the n^2-variable restriction of **TAU**.

(B) S_A is reduced to an analogous sentence (S_B) stating that the appropriate "regular-positive-consistent" $\sum_2$-form of P_n has the same zero-set Z_n.

(C) S_B is reduced to a topological sentence (S_C) stating that the corresponding $\sum_2$-decomposition of Z_n covers the canonical $\sum_2$-base of Z_n.

(D) S_C is reduced to a combinatorial sentence (S_D) about the structure of the $\sum_2$-base in question that can be refuted by straightforward combinatorial arguments - thus leading to a desired contradiction.

Note that the chain A-D is not a "natural" circuit lower bound proof according to `[RR]`. The two main diversities are as follows.

1. Our borel domains are n^2-dim real spaces, which disturbs **P/poly** constructivity and discrete counting arguments. On the other hand, adjacent n^2-dim geometry is crucial for the inference B.
2. The structure of the canonical $\sum_2$-base of Z_n characterizes the chosen polynomial Φ_n only, and hence the inference C does not apply to arbitrary "large" polynomials.

---

[1] We distinguish between validity of boolean functions f: $\{0,1\}^n \to \{0,1\}$ and the corresponding notion of tautology referring to propositional formulas $F(x_{i_1}, ..., x_{i_n})$; both are equivalent, but have different domains.

2 Overview

2.1 Basic notations

1. For any natural number $n > 0$ consider a polynomial
   $\Phi_n := \sum\limits_{f:\mathbf{n}\to\mathbf{n}} \prod\limits_{i<j\in\mathbf{n}} \left(x_{f(i),i} + x_{f(j),j}\right)^2$ over $\overrightarrow{x}_{n,n}$, where $\mathbf{n} = \{1, \cdots, n\}$ and $\overrightarrow{x}_{n,n} = (x_{i,j})_{i,j\in\mathbf{n}}$. We set $\langle i,j\rangle := n(i-1)+j$ and identify $x_{i,j}$ with $x_{\langle i,j\rangle}$ and $\mathbf{n}^2 = \{\langle i,j\rangle \mid i,j \in \mathbf{n}\}$ with $\mathbf{n^2} = \left\{1, \cdots, n^2\right\}$, which yields $\overrightarrow{x}_{n,n} = \overrightarrow{x}_{n^2} = (x_u)_{u\in\mathbf{n^2}}$. Note that Φ_n is a characteristic integer polynomial of the familiar propositional $(n \times n)$-tautology problem; graph-complexity (= circuit-complexity) of Φ_n is exponential in n (see `[GK]`).

2. Let $Z_n := \left\{\overrightarrow{x}_{n,n} \in \mathbb{R}_0^{n^2} \mid \Phi_n\left(\overrightarrow{x}_{n,n}\right) = 0\right\}$ be (closed) zero-set of Φ_n in $\mathbb{R}_0^{n^2}$, where $\mathbb{R}_0 = \mathbb{R} - \{0\}$. Obviously Z_n has boolean $\prod_2$-shape
   $\overrightarrow{x}_{n,n} \in Z_n \Leftrightarrow \bigwedge\limits_{f:\mathbf{n}\to\mathbf{n}} \bigvee\limits_{i<j\in\mathbf{n}} x_{f(i),i} + x_{f(j),j} = 0$, which yields the corresponding borel $\prod_2$-shape $Z_n = \bigcap\limits_{f:\mathbf{n}\to\mathbf{n}} \bigcup\limits_{i<j\in\mathbf{n}} \left\{\overrightarrow{x}_{n,n} \in \mathbb{R}_0^{n^2} \mid x_{f(i),i} + x_{f(j),j} = 0\right\}$ whose graph-complexity is exponential in n.

3. Let $\mathbf{n}^{2*2} := \{\{\langle i,j\rangle, \langle k,l\rangle\} \mid i,j,k,l \in \mathbf{n}\} = \left\{\{u,v\} \mid u,v \in \mathbf{n^2}\right\}$. For any $\vartheta = \{\langle i,j\rangle, \langle k,l\rangle\} \in \mathbf{n}^{2*2}$, we set $\mathfrak{D}^+(\vartheta) := x_{i,j} + x_{k,l}$, $\mathfrak{D}^-(\vartheta) := x_{i,j} - x_{k,l}$ and $\mathcal{O}^{+(-)}(\vartheta) := \left\{\overrightarrow{x}_{n,n} \in \mathbb{R}_0^{n^2} \mid \mathfrak{D}^{+(-)}(\vartheta) = 0\right\}$.

4. For any $\Gamma, \Lambda \subseteq \mathbf{n}^{2*2}$ let $(\Gamma,\Lambda)^+, (\Gamma,\Lambda)^- \subseteq \mathbf{n}^{2*2}$ be the minimal sets satisfying the five conditions:

   (a) $\Gamma \subseteq (\Gamma,\Lambda)^+$ and $\Lambda \subseteq (\Gamma,\Lambda)^-$

   (b) $\{u,v\}, \{u,w\} \in (\Gamma,\Lambda)^+ \Rightarrow \{v,w\} \in (\Gamma,\Lambda)^-$

   (c) $\{u,v\}, \{u,w\} \in (\Gamma,\Lambda)^- \Rightarrow \{v,w\} \in (\Gamma,\Lambda)^-$

   (d) $\{u,v\} \in (\Gamma,\Lambda)^+ \wedge \{v,w\} \in (\Gamma,\Lambda)^- \Rightarrow \{u,w\} \in (\Gamma,\Lambda)^+$

   (e) $(\Gamma,\Lambda)^+ \cap (\Gamma,\Lambda)^- \neq \emptyset \Rightarrow (\Gamma,\Lambda)^+, (\Gamma,\Lambda)^- := \mathbf{n}^{2*2}$

   Note that $(\Gamma,\Lambda)^+$ and $(\Gamma,\Lambda)^-$ are maximal extensions of Γ and Λ, respectively, such that $\bigcap\limits_{\vartheta\in\Gamma} \mathcal{O}^+(\vartheta) \cap \bigcap\limits_{\vartheta\in\Lambda} \mathcal{O}^-(\vartheta) = \bigcap\limits_{\vartheta\in(\Gamma,\Lambda)^+} \mathcal{O}^+(\vartheta) \cap \bigcap\limits_{\vartheta\in(\Gamma,\Lambda)^-} \mathcal{O}^-(\vartheta)$

5. A $\Delta \subset \mathbf{n}^{2*2}$ is called *perfect* (abbr.: $\Delta \Subset \mathbf{n}^{2*2}$) iff $\{\langle i,j\rangle, \langle k,l\rangle\} \in \Delta \Rightarrow j \neq l$ and $\emptyset \neq \Delta = (\Gamma,\Lambda)^+$ holds for some $\Gamma, \Lambda \subseteq \mathbf{n}^{2*2}$. In the sequel we abbreviate $(\Gamma,\emptyset)^{+(-)}$ by $\Gamma^{+(-)}$; note that $\Gamma \Subset \mathbf{n}^{2*2}$ implies $\Gamma^+ = \Gamma$.

6. Notably there exists the (uniquely determined) minimal positive borel $\sum_2$-decomposition $Z_n = \bigcup\limits_{\imath\in I} \bigcap\limits_{\vartheta\in\Delta_\imath} \mathcal{O}^+(\vartheta)$ and the underlying $\sum_2$-base $B_n =$

$\left\{\Delta_\imath \Subset \mathbf{n}^{2*2} \mid \imath \in I\right\}$ (see Comments below). In particular, for any $\sum_2$-decomposition $Z_n = \bigcup_{\jmath \in J} \left(\bigcap_{\vartheta \in \Gamma_\jmath} \mathcal{O}^+(\vartheta) \cap \bigcap_{\vartheta \in \Lambda_\jmath} \mathcal{O}^-(\vartheta) \right)$, the following two conditions hold:

(a) $(\forall \imath \in I)\,(\exists \jmath \in J)\left(\Delta_\imath = (\Gamma_\jmath, \Lambda_\jmath)^+\right)$

(b) $(\forall \jmath \in J)\,(\exists \imath \in I)\left(\Delta_\imath \subseteq (\Gamma_\jmath, \Lambda_\jmath)^+\right)$

7. Denote by $\mathbf{0}$ the n^2-dim zero-vector $\overrightarrow{0}_{n^2}$. Let $\overrightarrow{a}_{n,n} = (a_{i,j})_{i,j \in \mathbf{n}} = \left(a_{\langle i,j \rangle}\right)_{i,j \in \mathbf{n}} = (a_u)_{u \in \mathbf{n}^2} \neq \mathbf{0}$ be a n^2-dim integer vector with $\gcd\{a_u \neq 0\} = 1$ and $a_{\min\{u \mid a_u \neq 0\}} > 0$. Scalar products $\overrightarrow{a}_{n,n} \cdot \overrightarrow{x}_{n,n} = \sum_{i,j \in \mathbf{n}} a_{i,j} \cdot x_{i,j}$ and their formal negations $\neg\left(\overrightarrow{a}_{n,n} \cdot \overrightarrow{x}_{n,n}\right) = \neg\left(\sum_{i,j \in \mathbf{n}} a_{i,j} \cdot x_{i,j}\right)$ are called *linear literals*, or just *literals* (*positive* and *negative*, respectively); moreover, we call $\natural\left(\overrightarrow{a}_{n,n} \cdot \overrightarrow{x}_{n,n}\right) := \sum_{i,j \in \mathbf{n}} |a_{i,j}|$ the *weight* of both $\overrightarrow{a}_{n,n} \cdot \overrightarrow{x}_{n,n}$ and $\neg\left(\overrightarrow{a}_{n,n} \cdot \overrightarrow{x}_{n,n}\right)$. (See Comments below.)

8. Literals $\overrightarrow{a}_{n,n} \cdot \overrightarrow{x}_{n,n}$ and $\neg\left(\overrightarrow{a}_{n,n} \cdot \overrightarrow{x}_{n,n}\right)$ are called *regular* iff there exists $\Delta \Subset \mathbf{n}^{2*2}$ such that $\overrightarrow{a}_{n,n} \cdot \overrightarrow{x}_{n,n}$ is a linear combination with integer coefficients of the collection of binomials $\{\mathfrak{O}^+(\vartheta)\}_{\vartheta \in \Delta}$.

9. Let $U \otimes V := \{\{u, v\} \mid u \in U \wedge v \in V\}$ (thus $\mathbf{n}^{2*2} = \mathbf{n}^2 \otimes \mathbf{n}^2$). For any disjoint $X, Y \subset \mathbf{n}^2$ and $S \subset (X \cup Y) \otimes (X \cup Y) \subset \mathbf{n}^{2*2}$, consider the (uniquely determined) decomposition $S = S_X \cup S_Y \cup S_{X,Y}$ for $S_X \subset X \otimes X$, $S_Y \subset Y \otimes Y$ and $S_{X,Y} \subset X \otimes Y$, and let $\Gamma(S) := S_X \cup S_Y$ and $\Lambda(P) := S_{X,Y}$. Note that $\Gamma(S), \Lambda(S) \subset \mathbf{n}^{2*2}$.

10. For any (positive) regular literal $\overrightarrow{a}_{n,n} \cdot \overrightarrow{x}_{n,n}$, set $X := \left\{u \in \mathbf{n}^2 \mid a_u > 0\right\}$ and $Y := \left\{u \in \mathbf{n}^2 \mid a_u < 0\right\}$. Denote by $\left[\overrightarrow{a}_{n,n}\right]^2$ the set of all $S \subset (X \cup Y) \otimes (X \cup Y)$ such that the following two conditions hold:

    (a) $(\Gamma(S), \Lambda(S))^+ \Subset \mathbf{n}^{2*2}$

    (b) $\overrightarrow{a}_{n,n} \cdot \overrightarrow{x}_{n,n}$ is a linear combination with integer coefficients of the collection $\{\mathfrak{O}^+(\vartheta)\}_{\vartheta \in \Gamma(S)} \cup \{\mathfrak{O}^-(\vartheta)\}_{\vartheta \in \Lambda(S)}$.

    In the sequel we call $S \in \left[\overrightarrow{a}_{n,n}\right]^2$ *semipartitions* of $\overrightarrow{a}_{n,n}$. We call a borel polynomial $\bigcup_{S \in \left[\overrightarrow{a}_{n,n}\right]^2} \left(\bigcap_{\vartheta \in \Gamma(S)} \mathfrak{O}^+(\vartheta) \cap \bigcap_{\vartheta \in \Lambda(S)} \mathfrak{O}^-(\vartheta) \right)$ the *regular interpretation* of $\overrightarrow{a}_{n,n} \cdot \overrightarrow{x}_{n,n}$. (See Comments below.)

2.2 How to prove that NP = P fails

Suppose **NP** = **P**. This assumption infers:

1. For sufficiently large n, there exists a suitable *quasi-polynomial* over $\overrightarrow{x}_{n,n}$, whose zero-set in $\mathbb{R}_0^{n^2}$ is Z_n and whose graph-complexity is merely polynomial in n.[2] (This result follows by the author's interpretation of Turing computability in a suitable elementary algebraic formalism with definition-by-cases operation, see Lemma 4 and Attachment 1 below.) This in turn infers:
2. For sufficiently large n, there exists a borel term $\mathfrak{F}_n$ such that the following conditions (a)-(d) hold (see also Comments below):
    (a) The only operations occurring in $\mathfrak{F}_n$ are $\cup$ and $\cap$.
    (b) The leafs of $\mathfrak{F}_n$ are regular literals $\mathfrak{L}$ of the either form $\overrightarrow{a}_{n,n} \cdot \overrightarrow{x}_{n,n}$ or $\neg\left(\overrightarrow{a}_{n,n} \cdot \overrightarrow{x}_{n,n}\right)$.
    (c) The weight of $\mathfrak{F}_n$ is polynomial in n.
    (d) Zero-set of $\mathfrak{F}_n$ in $\mathbb{R}_0^{n^2}$ is Z_n, and hence positive $\sum_2$-expansion of $\mathfrak{F}_n$ covers the $\sum_2$-base $B_n = \left\{\Delta_\imath \Subset \mathbf{n}^{2*2} \mid \imath \in I\right\}$. To put it more exactly, the following holds.
        - Let $\mathfrak{D}_n = \bigcup_{\tau \in T} \bigcap_{\ell \in L_\tau} \mathfrak{L}_\ell$ be the canonical disjunctive normal form (DNF) of $\mathfrak{F}_n$, $\mathfrak{L}_\ell$ being the corresponding regular literals.
        - Let $\mathfrak{D}_n^{\mathrm{C}} := \bigcup_{\tau \in T^{\mathrm{C}}} \bigcap_{\ell \in L_\tau} \mathfrak{L}_\ell$ for $T^{\mathrm{C}} \subseteq T$, be the subform of $\mathfrak{D}_n$ obtained by deleting all inconsistent clauses $\bigcap_{\ell \in L_\tau} \mathfrak{L}_\ell$, $\tau \in T$.
        - Let $\mathfrak{D}_n^{\mathrm{CP}} := \bigcup_{\tau \in T^{\mathrm{CP}}} \bigcap_{\ell \in L_\tau^{\mathrm{P}}} \mathfrak{L}_\ell$ for $T^{\mathrm{CP}} \subseteq T^{\mathrm{C}}$, $L_\tau^{\mathrm{P}} \subseteq L_\tau$ be the subform of $\mathfrak{D}_n^{\mathrm{C}}$ that contains only positive literals $\mathfrak{L}_\ell$.
        - Let $\mathfrak{D}_n^{\mathrm{R}}$ be obtained by substituting regular interpretations for all (positive) literals $\mathfrak{L}_\ell$ occurring in $\mathfrak{D}_n^{\mathrm{CP}}$.
        - Let $\mathfrak{D}_n^{\mathrm{N}} = \bigcup_{\jmath \in J} \left(\bigcap_{\vartheta \in \Gamma_\jmath} \mathfrak{O}^{+}(\vartheta) \cap \bigcap_{\vartheta \in \Lambda_\jmath} \mathfrak{O}^{-}(\vartheta) \right)$ be the canonical DNF of $\mathfrak{D}_n^{\mathrm{R}}$.
        - Then the following two conditions hold:
            i. $(\forall \imath \in I)\,(\exists \jmath \in J)\left(\Delta_\imath = \left(\Gamma_\jmath, \Lambda_\jmath\right)^{+}\right)$
            ii. $(\forall \jmath \in J)\,(\exists \imath \in I)\left(\Delta_\imath \subseteq \left(\Gamma_\jmath, \Lambda_\jmath\right)^{+}\right)$
3. However, combinatorial structure of B_n is so involved that 2 (d) must fail in the presence of 2 (c). This yields a desired contradiction to the assumption **NP** = **P**. Q.E.D.

---

[2] This condition is sufficient for the conjecture **NP** $\in$ **P/poly** (see [GK: Theorem 21]).

3 Comments

3.1 Σ_2-decomposition and Σ_2-base

3.1.1 General description

For the sake of brevity denote $\overrightarrow{x}_{n,n}$ $(\overrightarrow{a}_{n,n})$ and $\mathbb{R}_0^{n^2}$ $(\mathbb{Z}^{n^2})$ by $\overrightarrow{x}$ $(\overrightarrow{a})$ and $\overrightarrow{\mathbb{R}}_0$ $(\overrightarrow{\mathbb{Z}})$, respectively. By the familiar boolean DNF approach, Z_n admits $\sum_2$-decompositions $Z_n = \bigcup\limits_{\imath \in I} \bigcap\limits_{\vartheta \in \Delta_\imath} \mathcal{O}^+(\vartheta)$ for suitable systems $\left\{\Delta_\imath \subset \mathbf{n}^{2*2} \mid \imath \in I\right\}$, and in fact $\left\{\Delta_\imath \Subset \mathbf{n}^{2*2} \mid \imath \in I\right\}$.

Definition 1 *A given* $\sum_2$*-decomposition* $Z_n = \bigcup\limits_{\imath \in I} \bigcap\limits_{\vartheta \in \Delta_\imath} \mathcal{O}^+(\vartheta)$, $\Delta_\imath \Subset \mathbf{n}^{2*2}$, *is called minimal iff for every* $\imath \in I$ *and* $\Delta_\imath \supsetneq \Delta'_\imath \Subset \mathbf{n}^{2*2}$, $\bigcap\limits_{\vartheta \in \Delta'_\imath} \mathcal{O}^+(\vartheta) \nsubseteq Z_n$ *. The corresponding minimal system* $B_n = \left\{\Delta_\imath \Subset \mathbf{n}^{2*2} \mid \imath \in I\right\}$ *is called* $\sum_2$*-base of* Z_n*.*

Theorem 2 $B_n = \left\{\Delta_\imath \Subset \mathbf{n}^{2*2} \mid \imath \in I\right\}$ *is uniquely determined by* n*. That is, for any* $n > 0$*, there is exactly one* $\sum_2$*-base of* Z_n*, and hence exactly one minimal* $\sum_2$*-decomposition of* Z_n *(modulo permutation and contraction). Moreover, if* $Z_n = \bigcup\limits_{\jmath \in J} \left(\bigcap\limits_{\vartheta \in \Gamma_\jmath} \mathcal{O}^+(\vartheta) \cap \bigcap\limits_{\vartheta \in \Lambda_\jmath} \mathcal{O}^-(\vartheta) \right)$*, then* $(\forall \imath \in I)(\exists \jmath \in J)\left(\Delta_\imath = (\Gamma_\jmath, \Lambda_\jmath)^+\right)$ *and* $(\forall \jmath \in J)(\exists \imath \in I)\left(\Delta_\imath \subseteq (\Gamma_\jmath, \Lambda_\jmath)^+\right)$.

Proof. See Attachment 2 below. ■

3.1.2 Recursive definition of Σ_2-base B_n

Denote by $[U \curvearrowright V]$ the set of all partial functions from U to V. For any $1 \leq \ell \leq n-1$ we define a suitable set $M_n^\ell \subseteq \left[\mathbf{n}^2 \curvearrowright \{\pm 1, \cdots, \pm \ell\}\right]$ and then let $M_n := \bigcup\limits_{\ell=1}^{n-1} M_n^\ell$ and $\widetilde{M_n} := \{f \in M_n \mid (\forall y \in Dom_2(f))\, Dom_1(f, y) = \mathbf{n}\}$ where $Dom_1(f, y) := \{x \mid (\exists z)\, f(x, y) = z\}$, $Dom_2(f) := \{y \mid (\exists x \exists z)\, f(x, y) = z\}$.
Denote by $[U \curvearrowright V]$ the set of all partial functions from U to V. For any $1 \leq \ell \leq n-1$ we define a suitable set $M_n^\ell \subseteq \left[\mathbf{n}^2 \curvearrowright \{\pm 1, \cdots, \pm \ell\}\right]$ and then let $M_n := \bigcup\limits_{\ell=1}^{n-1} M_n^\ell$ and $\widetilde{M_n} := \{f \in M_n \mid (\forall y \in Dom_2(f))\, Dom_1(f, y) = \mathbf{n}\}$ where $Dom_1(f, y) := \{x \mid (\exists z)\, f(x, y) = z\}$, $Dom_2(f) := \{y \mid (\exists x \exists z)\, f(x, y) = z\}$.
The required B_n is $B_n := \left\{\{\langle i, j\rangle, \langle k, l\rangle\} \Subset \mathbf{n}^{2*2} \mid f(i, j) + f(k, l) = 0\right\}_{f \in \widetilde{M_n}}$. Now let M_n^ℓ arise by the following recursive clauses, where $\phi_{U,y,s} : U \times \{y\} \to \{s\}$ and $\phi_{U-f,y,s} : (U - Dom_1(f, y)) \times \{y\} \to \{s\}$

Basis.

$M_n^1 := \{\emptyset\} \cup \{X \times \{j\} \times \{1\} \cup Y \times \{l\} \times \{-1\} \mid j \neq l \in \mathbf{n} \wedge \emptyset \neq X, Y \subseteq \mathbf{n}\}$. That is, $M_n^1 = \{\emptyset\} \cup \left\{\phi_{X,j,1} \cup \phi_{Y,l,-1} \mid j \neq l \in \mathbf{n} \wedge \emptyset \neq X, Y \subseteq \mathbf{n}\right\}$. Note that the resulting fragment $B_n^1 \subset B_n$ is $B_n^1 := \{(\mathbf{n} \times \{j\}) \otimes (\mathbf{n} \times \{l\}) \mid j \neq l \in \mathbf{n}\}$.

Induction step. Let $1 < \ell < n$ and consider two cases ($\partial = \emptyset$ is admissible).

1. Let $\partial \cup f \in M_n^{\ell-1}$, $j \in \mathbf{n}$, and $\{X_y\}_{y\in Dom_2(f)}$ for $\emptyset \neq X_y \subseteq \mathbf{n}$ be such that:
   (a) $Dom_2(\partial) \cap Dom_2(f) = \emptyset$
   (b) $j \notin Dom_2(\partial \cup f)$
   (c) $(\forall y \in Dom_2(f))\,(Dom_1(f, y) \subsetneq X_y)$

   Then set $f' := \partial \cup f \cup \phi_{X,j,\ell} \bigcup\limits_{y\in Dom_2(f)} \phi_{X_y^{-f},y,\ell}$

2. Let $\partial\cup f, \partial\cup g \in M_n^{\ell-1}$ and $\{X_y\}_{y\in Dom_2(f)}, \{Y_z\}_{z\in Dom_2(g)}$ for $\emptyset \neq X_y \subseteq \mathbf{n}$ and $\emptyset \neq Y_z \subseteq \mathbf{n}$ be such that:
   (a) $Dom_2(f) \cap Dom_2(g) = Dom_2(\partial) \cap Dom_2(f)$
   $= Dom_2(\partial) \cap Dom_2(g) = \emptyset$
   (b) $(\forall y \in Dom_2(f))\,(Dom_1(f, y) \subsetneq X_y)$
   (c) $(\forall z \in Dom_2(g))\,(Dom_1(g, z) \subsetneq Y_z)$.

   Then set $f' := \partial \cup f \cup g \cup \bigcup\limits_{y\in Dom_2(f)} \phi_{X_y^{-f},y,\ell} \cup \bigcup\limits_{z\in Dom_2(g)} \phi_{Y_z^{-g},z,-\ell}$.

Let M_n^{ℓ} extend $M_n^{\ell-1}$ by adjoining all functions f' obtained by 1-2. This completes our recursive definition. (See also `[GMaple]`)

3.2 Borel polynomials

Definition 3 *Call* linear borel polynomials over $\overrightarrow{x}$ *(or just* borel polynomials*) arbitrary terms in the algebraic language of the two binary operations* $\cup$ *and* $\cap$*, whose* literals (positive and negative, *respectively) are of the either form* $\overrightarrow{a} \cdot \overrightarrow{x}$ *or* $\neg(\overrightarrow{a} \cdot \overrightarrow{x})$*, where* $\overrightarrow{a} = (a_{i,j})_{i,j\in\mathbf{n}} = (a_u)_{u\in\mathbf{n}^2} \in \overrightarrow{\mathbb{Z}}$, $\overrightarrow{a} \neq \mathbf{0}$ *and* $\overrightarrow{a} \cdot \overrightarrow{x} = \sum\limits_{i,j\in\mathbf{n}} a_{i,j} \cdot x_{i,j}$*. For the sake of brevity, we also assume that* $\gcd\{a_u \neq 0\} = 1$ *and* $a_{\min\{u \mid a_u \neq 0\}} > 0$*. Furthermore, we set* $\natural(\overrightarrow{a} \cdot \overrightarrow{x}) := \sum\limits_{i,j\in\mathbf{n}} |a_{i,j}| \in \mathbb{N}$ *and call it the* weight *of both* $\overrightarrow{a} \cdot \overrightarrow{x}$ *and* $\neg(\overrightarrow{a} \cdot \overrightarrow{x})$ *(cf. Overview 2.1, 8). Having this, the* weight $\natural(\mathfrak{T})$ *of a given borel polynomial* $\mathfrak{T}$ *is the summary weight of literals plus the number of operations* $\cup$, $\cap$ *occurring in it (as usual). A borel polynomial is called* positive *if so are all its literals. The literals are evaluated by* $|\overrightarrow{a} \cdot \overrightarrow{x}| := \left\{\overrightarrow{x} \in \overrightarrow{\mathbb{R}}_0 \mid \overrightarrow{a} \cdot \overrightarrow{x} = 0\right\}$ *and* $|\neg(\overrightarrow{a} \cdot \overrightarrow{x})| := \left\{\overrightarrow{x} \in \overrightarrow{\mathbb{R}}_0 \mid \overrightarrow{a} \cdot \overrightarrow{x} \neq 0\right\}$*, respectively. Together with the ordinary set-theoretical interpretations of* $\cup$ *and* $\cap$*, such evaluation of literals uniquely determines the value* $|\mathfrak{T}| \subseteq \overrightarrow{\mathbb{R}}_0$ *of any given borel polynomial* $\mathfrak{T}$ *in question;* $|\mathfrak{T}|$ *is also called the* zero-set *of* $\mathfrak{T}$ *(in* $\overrightarrow{\mathbb{R}}_0$*).*

Lemma 4 *If $\boldsymbol{NP} = \boldsymbol{P}$, then the following holds. For sufficiently large n, there exists a borel polynomial $\mathfrak{T}$ such that $|\mathfrak{T}| = Z_n$; moreover graph-complexity of $\mathfrak{T}$ is polynomial in n.*

Proof. See Attachment 1 below. ■

Remark 5 *The notion of borel polynomial is too loose, if we wish to apply Theorem 2. This is because arbitrary literal values can't be expressed as desirable compositions of "normal atomic values" $\mathcal{O}^+(\vartheta)$ and $\mathcal{O}^-(\vartheta)$ (see Overview 2.1, 3). The polynomials whose literals admit such presentations are called "regular" - these are introduced as follows.*

Definition 6 *Call* normal atoms *the binomials $x_{i,j} + x_{k,l}$ and $x_{i,j} - x_{k,l}$; normal atoms and their negations are both called* normal literals*. In the sequel we abbreviate normal literals $x_{i,j}+x_{k,l}$ and $x_{i,j}-x_{k,l}$ by $\mathfrak{O}^+(\vartheta)$ and $\mathfrak{O}^-(\vartheta)$, respectively, where $\vartheta = \{\langle i,j\rangle, \langle k,l\rangle\}$. Hence $|\mathfrak{O}^+(\vartheta)| = |x_{i,j} + x_{k,l}| = \mathcal{O}^+(\vartheta)$ and $|\mathfrak{O}^-(\vartheta)| = |x_{i,j} - x_{k,l}| = \mathcal{O}^-(\vartheta)$; these sets are called* normal atomic values *(cf. Overview 2.1, 3). Now literals $\overrightarrow{a} \cdot \overrightarrow{x}$ and $\neg(\overrightarrow{a} \cdot \overrightarrow{x})$ are called* regular *(*positive *and* negative*, respectively) iff for some $\Delta \Subset \mathbf{n}^{2*2}$, $\overrightarrow{a} \cdot \overrightarrow{x}$ is a linear combination of normal atoms $\{\mathfrak{O}^+(\vartheta)\}_{\vartheta\in\Delta}$ in $\mathbb{Z}[\overrightarrow{x}]$, i.e. $\overrightarrow{a} \cdot \overrightarrow{x} = \sum\limits_{\vartheta\in\Delta} b_\vartheta \cdot \mathfrak{O}^+(\vartheta)$ where $b_\vartheta \in \mathbb{Z}$ (cf. Overview 2.1, 8); the corresponding collection $\{\mathfrak{O}^+(\vartheta)\}_{\vartheta\in\Delta}$ we call the* normal generators *of $\overrightarrow{a} \cdot \overrightarrow{x}$. Borel polynomials whose all literals are regular (normal) are called* regular *(*normal*).*

Lemma 7 *If $\Delta \Subset \mathbf{n}^{2*2}$ and $\bigcap\limits_{\vartheta\in\Delta} \mathfrak{O}^+(\vartheta) \subseteq |\overrightarrow{a} \cdot \overrightarrow{x}|$, then $\overrightarrow{a} \cdot \overrightarrow{x}$ is a linear combination of $\{\mathfrak{O}^+(\vartheta)\}_{\vartheta\in\Delta}$ in $\mathbb{Z}[\overrightarrow{x}]$, and hence $\overrightarrow{a}$ is regular.*

Proof. See Attachment 3 below. ■

3.2.1 Consistent and positive Σ_2-expansions

Definition 8 *Let $\mathfrak{P}$ be a given regular borel polynomial. By familiar techniques we pass to its DNF $\partial(\mathfrak{P}) = \bigcup\limits_{\tau\in T} \bigcap\limits_{\ell\in L_\tau} \mathfrak{L}_\ell$, $\mathfrak{L}_\ell$ being the (regular) literals of $\mathfrak{P}$. Let $\partial^{\mathrm{C}}(\mathfrak{P}) = \bigcup\limits_{\tau\in T^{\mathrm{C}}} \bigcap\limits_{\ell\in L_\tau} \mathfrak{L}_\ell$, $T^{\mathrm{C}} \subseteq T$, arise from $\partial(\mathfrak{P})$ by deleting all inconsistent clauses, i.e. all $\bigcap\limits_{\ell\in L_\tau} \mathfrak{L}_\ell$, $\tau \in T$, such that $(\exists \ell, \ell' \in L_\tau)(\mathfrak{L}_{\ell'} = \neg\mathfrak{L}_\ell)$. Call $\partial^{\mathrm{C}}(\mathfrak{P})$ the* consistent $\sum_2$-expansion *of $\mathfrak{P}$.*

Definition 9 *Let $\mathfrak{P}$ be as above; consider $\partial^{\mathrm{C}}(\mathfrak{P})$. Let $\partial^{\mathrm{CP}}(\mathfrak{P}) = \bigcup\limits_{\tau\in T^{\mathrm{CP}}} \bigcap\limits_{\ell\in L^{\mathrm{P}}_\tau} \mathfrak{L}_\ell$, $T^{\mathrm{CP}} \subseteq T^{\mathrm{C}}$, $L^{\mathrm{P}}_\tau \subseteq L_\tau$, arise from $\partial^{\mathrm{C}}(\mathfrak{P})$ by deleting all negative literals $\mathfrak{L}_\ell$ along with the empty clauses such obtained. Note that $\partial^{\mathrm{CP}}(\mathfrak{P})$ is a positive regular polynomial; call it the* positive consistent $\sum_2$-expansion *of $\mathfrak{P}$.*

Lemma 10 *For any borel polynomial $\mathfrak{T}$ with $|\mathfrak{T}| = Z_n$ there exists a regular borel polynomial $\mathfrak{P}$ such that $|\partial^{\mathrm{CP}}(\mathfrak{P})| = Z_n$; moreover $\natural(\mathfrak{P})$ is polynomial in graph-complexity of $\mathfrak{T}$.*

Proof. See Attachment 4 below; Lemma 7 is crucial for the proof. ■

3.2.2 Regular evaluations

Remark 11 *Lemmata 7, 10 allow us to reduce borel polynomials to positive regular ones. In order to make Theorem 2 work we wish to switch to the correlated normal atomic values and modify the evaluation of (positive regular) literals, accordingly. Such "regular" evaluation is introduces as follows.*

Definition 12 *Given a (positive) regular literal* $\overrightarrow{a} \cdot \overrightarrow{x}$*, we wish to characterize its normal generators. To this end, we first let* $X := \left\{u \in \mathbf{n}^2 \mid a_u > 0\right\}$ *and* $Y := \left\{u \in \mathbf{n}^2 \mid a_u < 0\right\}$ *and denote by* $\left[\overrightarrow{a}\right]^2$ *the set of semipartitions* $S \subset (X \cup Y) \otimes (X \cup Y)$ *such that* $(\Gamma(S), \Lambda(S))^+ \Subset \mathbf{n}^{2*2}$ *and* $\overrightarrow{a} \cdot \overrightarrow{x}$ *is a linear combination of* $\{\mathfrak{O}^+(\vartheta)\}_{\vartheta\in\Gamma(S)} \cup \{\mathfrak{O}^-(\vartheta)\}_{\vartheta\in\Lambda(S)}$ *in* $\mathbb{Z}[\overrightarrow{x}]$*. We call a borel polynomial* $\bigcup_{S\in[\overrightarrow{a}]^2}\left(\bigcap_{\vartheta\in\Gamma(S)}\mathfrak{O}^+(\vartheta) \cap \bigcap_{\vartheta\in\Lambda(S)}\mathfrak{O}^-(\vartheta)\right)$ *and a borel set* $\|\overrightarrow{a} \cdot \overrightarrow{x}\| := \bigcup_{S\in[\overrightarrow{a}]^2}\left(\bigcap_{\vartheta\in\Gamma(S)}\mathcal{O}^+(\vartheta) \cap \bigcap_{\vartheta\in\Lambda(S)}\mathcal{O}^-(\vartheta)\right)$ *the* regular interpretation *and* regular value *of* $\overrightarrow{a} \cdot \overrightarrow{x}$*, respectively (cf. Overview 2.1, 9, 10). Together with the ordinary set-theoretical interpretations of* $\cup$ *and* $\cap$*, regular values of literals uniquely determine the corresponding* regular value $\|\mathfrak{P}\| \subseteq \overrightarrow{\mathbb{R}}_0$ *of any given positive regular borel polynomial* $\mathfrak{P}$*;* $\|\mathfrak{P}\|$ *is also called the* regular zero-set *of* $\mathfrak{P}$ *(in* $\overrightarrow{\mathbb{R}}_0$*).*

Example 13 *Consider the following simplest cases (for the sake of brevity we extend regular evaluation to all (positive) literals by* $\|\overrightarrow{a} \cdot \overrightarrow{x}\| = \left[\overrightarrow{a}\right]^2 := \emptyset$ *if* $\overrightarrow{a} \cdot \overrightarrow{x}$ *is not regular).*

Remark 14

1. *For any* $i, j, k, l \in \mathbf{n}$*,* $j \neq l$*, we have*
   $\left[x_{i,j} \pm x_{k,l}\right]^2 = \{\{\{\langle i,j\rangle, \langle k,l\rangle\}\}\}$*, and hence*
   $\|x_{i,j} \pm x_{k,l}\| = \left\{\overrightarrow{x} \in \overrightarrow{\mathbb{R}}_0 \mid x_{i,j} \pm x_{k,l} = 0\right\} = |x_{i,j} \pm x_{k,l}|$
2. $x_{i,j} + x_{k,l} + x_{p,q}$ *and* $x_{i,j} + x_{k,l} - x_{p,q}$ *are both not regular, and hence* $\|x_{i,j} + x_{k,l} \pm x_{p,q}\| = \emptyset$
3. *If* $j \neq q \neq l \in \mathbf{n}$*, then*
   $\left[x_{i,j} + x_{k,l} + x_{p,q} + x_{r,q}\right]^2 = \{\{\{\langle i,j\rangle, \langle p,q\rangle\}, \{\langle k,l\rangle, \langle r,q\rangle\}\}\}$*, and hence*
   $\|x_{i,j} + x_{k,l} + x_{p,q} + x_{r,q}\| =$
   $\left\{\overrightarrow{x} \in \overrightarrow{\mathbb{R}}_0 \mid x_{i,j} + x_{p,q} = 0\right\} \cap \left\{\overrightarrow{x} \in \overrightarrow{\mathbb{R}}_0 \mid x_{k,l} + x_{r,q} = 0\right\} =$
   $\left\{\overrightarrow{x} \in \overrightarrow{\mathbb{R}}_0 \mid x_{i,j} + x_{p,q} = x_{k,l} + x_{r,q} = 0\right\}$
   $\subsetneqq |x_{i,j} + x_{k,l} + x_{p,q} + x_{r,q}|$
4. *If* $l \neq j \neq q \in \mathbf{n}$*, then*
   $\left[2x_{i,j} \pm x_{k,l} - x_{p,q}\right]^2 = \{\{\{\langle i,j\rangle, \langle k,l\rangle\}, \{\langle i,j\rangle, \langle p,q\rangle\}\}\}$*, and hence*

$$\|2x_{i,j} \pm x_{k,l} - x_{p,q}\| =$$

$$\left\{\overrightarrow{x} \in \overrightarrow{\mathbb{R}}_0 \mid x_{i,j} \pm x_{p,q} = 0\right\} \cap \left\{\overrightarrow{x} \in \overrightarrow{\mathbb{R}}_0 \mid x_{i,j} - x_{p,q} = 0\right\} =$$

$$\left\{\overrightarrow{x} \in \overrightarrow{\mathbb{R}}_0 \mid x_{i,j} \pm x_{p,q} = x_{i,j} - x_{p,q} = 0\right\}$$

5. *If* $j, l, q, v \in \mathbf{n}$ *are pairwise distinct, then*

$$[x_{i,j} + x_{k,l} + x_{p,q} + x_{r,s}]^2 = \left\{ \begin{array}{c} \{\{\langle i,j\rangle, \langle k,l\rangle\}, \{\langle p,q\rangle, \langle r,s\rangle\}\}, \\ \{\{\langle i,j\rangle, \langle p,q\rangle\}, \{\langle k,l\rangle, \langle r,s\rangle\}\}, \\ \{\{\langle i,j\rangle, \langle r,s\rangle\}, \{\langle k,l\rangle, \langle p,q\rangle\}\} \end{array} \right\}$$

and hence $\|x_{i,j} + x_{k,l} + x_{p,q} + x_{r,s}\| =$

$$\left\{ \overrightarrow{x} \in \overrightarrow{\mathbb{R}}_0 \mid \left(\begin{array}{r} x_{i,j} + x_{k,l} = x_{p,q} + x_{r,s} = 0 \\ \vee\ x_{i,j} + x_{p,q} = x_{k,l} + x_{r,s} = 0 \\ \vee\ x_{i,j} + x_{r,s} = x_{k,l} + x_{p,q} = 0 \end{array} \right) \right\}$$

$$\subsetneqq |x_{i,j} + x_{k,l} + x_{p,q} + x_{r,s}|$$

6. *For* j, l, q, v *as above, we have*

$$[x_{i,j} + x_{k,l} - x_{p,q} - x_{r,s}]^2 = \left\{ \begin{array}{c} \{\{\langle i,j\rangle, \langle k,l\rangle\}, \{\langle p,q\rangle, \langle r,s\rangle\}\}, \\ \{\{\langle i,j\rangle, \langle p,q\rangle\}, \{\langle k,l\rangle, \langle r,s\rangle\}\}, \\ \{\{\langle i,j\rangle, \langle r,s\rangle\}, \{\langle k,l\rangle, \langle p,q\rangle\}\} \end{array} \right\}$$

and hence $\|x_{i,j} + x_{k,l} - x_{p,q} - x_{r,s}\| =$

$$\left\{ \overrightarrow{x} \in \overrightarrow{\mathbb{R}}_0 \mid \left(\begin{array}{r} x_{i,j} + x_{k,l} = x_{p,q} + x_{r,s} = 0 \\ \vee\ x_{i,j} - x_{p,q} = x_{k,l} - x_{r,s} = 0 \\ \vee\ x_{i,j} - x_{r,s} = x_{k,l} - x_{p,q} = 0 \end{array} \right) \right\}$$

$$\subsetneqq |x_{i,j} + x_{k,l} - x_{p,q} - x_{r,s}|$$

Lemma 15 *For any regular* $\overrightarrow{a} \cdot \overrightarrow{x}$, $\|\overrightarrow{a} \cdot \overrightarrow{x}\| \subseteq |\overrightarrow{a} \cdot \overrightarrow{x}|$. *Moreover, if* $\Delta \Subset \mathbf{n}^{2*2}$ *and* $\bigcap_{\vartheta \in \Delta} \mathfrak{D}^{+}(\vartheta) \subseteq |\overrightarrow{a} \cdot \overrightarrow{x}|$, *then* $\bigcap_{\vartheta \in \Delta} \mathfrak{D}^{+}(\vartheta) \subseteq \|\overrightarrow{a} \cdot \overrightarrow{x}\|$.

Proof. See Attachment 3 below. ■

Lemma 16 *Let* $\mathfrak{P}$ *be any positive regular borel polynomial with* $|\mathfrak{P}| = Z_n$. *Then* $\|\mathfrak{P}\| = Z_n$.

Proof. See Attachment 5 below; Lemma 15 is crucial for the proof. ■

Corollary 17 *Let* $\mathfrak{P}$ *be any regular borel polynomial such that* $|\partial^{\text{CP}}(\mathfrak{P})| = Z_n$. *Let* $\partial^{\text{R}}(\mathfrak{P})$ *arise from* $\partial^{\text{CP}}(\mathfrak{P})$ *by replacing all literals occurring in it by their regular interpretations. Let* $\partial^{\text{N}}(\mathfrak{P}) := \partial(\partial^{\text{R}}(\mathfrak{P}))$ *be the DNF of* $\partial^{\text{R}}(\mathfrak{P})$*; call it the normal* $\sum_2$*-expansion of* $\mathfrak{P}$. *Then* $|\partial^{\text{N}}(\mathfrak{P})| = Z_n$.

Proof. Clearly $|\partial^{\text{N}}(\mathfrak{P})| = |\partial^{\text{R}}(\mathfrak{P})| = \|\partial^{\text{CP}}(\mathfrak{P})\|$. ■

3.3 Summary

Suppose **NP** $=$ **P**. By Lemma 4, we obtain a borel polynomial $\mathfrak{T}_n$ whose zero-set is Z_n and whose graph-complexity is polynomial in n. By Lemma 10, we pass to a regular borel polynomial $\mathfrak{P}_n$ satisfying $|\partial^{\mathrm{CP}}(\mathfrak{P}_n)| = Z_n$, whose weight is polynomial in n. By Corollary 17, we take its normal $\sum_2$-expansion $\partial^{\mathrm{N}}(\mathfrak{P}_n)$ and arrive at $|\partial^{\mathrm{N}}(\mathfrak{P})| = Z_n$. (In Overview 2.2 such $\mathfrak{P}_n$, $\partial^{\mathrm{CP}}(\mathfrak{P}_n)$ and $\partial^{\mathrm{N}}(\mathfrak{P}_n)$ are referred to as $\mathfrak{F}_n$, $\mathfrak{D}_n^{\mathrm{CP}}$ and $\mathfrak{D}_n^{\mathrm{N}}$, respectively). Note that $\partial^{\mathrm{N}}(\mathfrak{P}_n)$ has the desired $\sum_2$-form $\bigcup\limits_{\jmath\in J}\left(\bigcap\limits_{\vartheta\in\Gamma_\jmath}\mathfrak{O}^+(\vartheta)\cap\bigcap\limits_{\vartheta\in\Lambda_\jmath}\mathfrak{O}^-(\vartheta)\right)$, and hence $Z_n = \bigcup\limits_{\jmath\in J}\left(\bigcap\limits_{\vartheta\in\Gamma_\jmath}\mathcal{O}^+(\vartheta)\cap\bigcap\limits_{\vartheta\in\Lambda_\jmath}\mathcal{O}^-(\vartheta)\right)$. By Theorem 2, this $\sum_2$-decomposition of Z_n yields $(\forall\imath\in I)(\exists\jmath\in J)\left(\Delta_\imath = (\Gamma_\jmath,\Lambda_\jmath)^+\right)$ and $(\forall\jmath\in J)(\exists\imath\in I)\left(\Delta_\imath\subseteq(\Gamma_\jmath,\Lambda_\jmath)^+\right)$ where $B_n = \left\{\Delta_\imath\Subset\mathbf{n}^{2*2}\mid\imath\in I\right\}$ is the $\sum_2$-base. However, our recursive definition of the $\sum_2$-basis (3.1.2) drops a hint that combinatorial-topological structure of B_n is so involved that it actually requires exponential weight of $\mathfrak{P}_n$ (see also purely combinatorial connections in Attachments 6, 7 below). The resulting contradiction refutes the assumption **NP** $=$ **P**. Hence **NP** $\neq$ **P**.

4 Attachment 1: Background

In `[GK]` we established the following inference.

Claim 18 *If* ***NP*** $=$ ***P****, then for every* $n>0$ *there exists a (quasi-)polynomial* π_n *in the algebraic language* $\mathcal{L}_n$ *of variables* $\overrightarrow{x} = \overrightarrow{x}_{n,n}$*, constant* 1 *and three binary operations* $+,-,?$ *such that the graph-complexity of* π_n *is polynomial in* n *and* $Z_n = \left\{\overrightarrow{x}\in\overrightarrow{\mathbb{R}}_0\mid\pi_n(\overrightarrow{x}) = 0\right\}$ *holds under the canonical interpretation of* $1,+,-$*, while* $?$ *being the definition-by-cases* $u?v := \begin{cases} 0 & \text{if } u=0 \\ v & \text{otherwise}\end{cases}$.

We prove the Lemma 4. Denote by α, β, γ arbitrary $\mathcal{L}_n$-polynomials and consider a polynomial rewriting ?-elimination algorithm:

$\alpha^* := \alpha$, if ? does not occur in α

$(\alpha?\beta)^* := \alpha^*\vee\beta^*$ and $(\alpha?\beta\pm\gamma)^* := (\alpha^*\wedge\gamma^*)\vee\left(\neg(\alpha^*)\wedge(\beta\pm\gamma)^*\right)$, otherwise

Having arrived at ?-free expression α^*, we further eliminate all nonatomic negations by boolean duality laws (which do not increase graph complexity). Call the resulting expression $\alpha^{\#}$. Furthermore, we replace in $\alpha^{\#}$ every occurrence of $\vee$ and $\wedge$ by $\cup$ and $\cap$, respectively, and call the resulting expression $\alpha^\star$. Note that $\alpha^\star$ is a borel polynomial whose graph-complexity is polynomial in the one of α. Moreover, it is readily seen that $\left\{\overrightarrow{x}\in\overrightarrow{\mathbb{R}}_0\mid\alpha(\overrightarrow{x}) = 0\right\} = |\alpha^\star|$. In particular $Z_n = \left\{\overrightarrow{x}\in\overrightarrow{\mathbb{R}}_0\mid\pi_n(\overrightarrow{x}) = 0\right\} = |\pi_n^\star|$, where π_n is as in the claim. Q.E.D.

5 Attachment 2: Theorem 2 and beyond

5.1 Basic tools

Definition 19 *For an arbitrary positive literal* $\overrightarrow{a} \cdot \overrightarrow{x} = \sum\limits_{i,j \in \mathbf{n}} a_{i,j} \cdot x_{i,j}$, $|\overrightarrow{a} \cdot \overrightarrow{x}|$ *and* $|\neg(\overrightarrow{a} \cdot \overrightarrow{x})|$ *are called planes and coplanes (in* $\overrightarrow{\mathbb{R}}_0$ *) respectively; they both are also called linear sections. Finite nonempty intersections of planes and linear sections are called* $\prod_1$*-sets and* $\prod_1$*-expansions, respectively. For any* $\prod_1$*-expansion* $E = \bigcap\limits_{\imath \in I} |\overrightarrow{a}_\imath \cdot \overrightarrow{x}| \cap \bigcap\limits_{\jmath \in J} |\neg(\overrightarrow{a}_\jmath \cdot \overrightarrow{x})|$, $I \cap J = \emptyset$, *denote by* E^+ *the corresponding* $\prod_1$*-set* $\bigcap\limits_{\imath \in I} |\overrightarrow{a}_\imath \cdot \overrightarrow{x}|$*; clearly* $E \subseteq E^+$*. For any* $\Delta \subseteq \mathbf{n}^{2*2}$*, a* $\prod_1$*-set* $\bigcap\limits_{\vartheta \in \Delta} \mathcal{O}^+(\vartheta)$ *is called proper.*

Claim 20 *Disjunction property. For any* $\prod_1$*-sets* U*,* V *and* W*, if* $U \subseteq V \cup W$ *then either* $U \subseteq V$ *or* $U \subseteq W$*.*

Proof. Because $\prod_1$-sets are convex. (Geometrically obvious.) ■

Claim 21 *Absorption property. For any* $\prod_1$*-expansion* E *and* $\prod_1$*-set* U*, if* $E \subseteq U$ *then* $E^+ \subseteq U$*.*

Proof. Because $\prod_1$-sets are convex and closed (see also `[GK: Lemma 34]`.) ■

Claim 22 *Linearity. For any positive literal* $\overrightarrow{a}$ *and* $\prod_1$*-set* $U = \bigcap\limits_{\imath \in I} |\overrightarrow{a}_\imath \cdot \overrightarrow{x}|$*, if* $U \subseteq |\overrightarrow{a} \cdot \overrightarrow{x}|$ *then* $\overrightarrow{a} \cdot \overrightarrow{x}$ *is a linear combination of* $\{\overrightarrow{a}_\imath \cdot \overrightarrow{x}\}_{\imath \in I}$ *in* $\mathbb{Q}[\overrightarrow{x}]$*.*

Proof. Basic linear algebra. ■

Claim 23 *Monotonicity. For any* $\Gamma, \Lambda, \Gamma', \Lambda' \subseteq \mathbf{n}^{2*2}$ *and the corresponding proper* $\prod_1$*-sets* $U = \bigcap\limits_{\vartheta \in \Gamma} \mathcal{O}^+(\vartheta) \cap \bigcap\limits_{\vartheta \in \Lambda} \mathcal{O}^-(\vartheta)$ *and* $U' = \bigcap\limits_{\vartheta \in \Gamma'} \mathcal{O}^+(\vartheta) \cap \bigcap\limits_{\vartheta \in \Lambda'} \mathcal{O}^-(\vartheta)$*, if* $U' \subseteq U$ *then* $(\Gamma, \Lambda)^+ \subseteq (\Gamma', \Lambda')^+$*.*

Proof. A consequence of previous claim a/o the completeness of equational calculus. ■

5.2 Proof of Theorem 2

Step 1. We show that the recursive definition 3.1.2 provides us with (at least one) minimal $\sum_2$-decomposition of Z_n. To this end, we interpret elements of Z_n as boolean tautologies of dimension $n \times n$ (see `[GK]` for details). A tautology in question is called minimal iff its every proper subformula is not a tautology. Clearly every tautology extends or coincides with a minimal tautology. With every minimal tautology $\mathcal{F}$ we associate a minimal natural number $\ell > 0$ such that the literals occurring in $\mathcal{F}$ can be homomorphically collapsed onto segment $\{\upsilon_x, \neg\upsilon_x \mid 0 < x \leq \ell\}$. The resulting renamed minimal tautology is called properly minimal. Note that all properly minimal tautologies admit a natural hierarchy which is described in 3.1.2.

Step 2. Consider any $\sum_2$-decompositions $Z_n = \bigcup\limits_{\imath \in I} \bigcap\limits_{\vartheta \in \Delta_\imath} \mathcal{O}^+ (\vartheta)$ and $Z_n = \bigcup\limits_{\jmath \in J} \left(\bigcap\limits_{\vartheta \in \Gamma_\jmath} \mathcal{O}^+ (\vartheta) \cap \bigcap\limits_{\vartheta \in \Lambda_\jmath} \mathcal{O}^- (\vartheta) \right)$ for $\Delta_\imath \Subset \mathbf{n}^{2*2}$ and $\Gamma_\jmath, \Lambda_\jmath \subseteq \mathbf{n}^{2*2}$. It holds $\bigcup\limits_{\imath \in I} \bigcap\limits_{\vartheta \in \Delta_\imath} \mathcal{O}^+ (\vartheta) = \bigcup\limits_{\jmath \in J} \left(\bigcap\limits_{\vartheta \in \Gamma_\jmath} \mathcal{O}^+ (\vartheta) \cap \bigcap\limits_{\vartheta \in \Lambda_\jmath} \mathcal{O}^- (\vartheta) \right)$. Hence by the disjunction property (Claim 20) we have

$(\forall \imath \in I) (\exists \jmath \in J) \left(\bigcap\limits_{\vartheta \in \Delta_\imath} \mathcal{O}^+ (\vartheta) \subseteq \bigcap\limits_{\vartheta \in \Gamma_\jmath} \mathcal{O}^+ (\vartheta) \cap \bigcap\limits_{\vartheta \in \Lambda_\jmath} \mathcal{O}^- (\vartheta) \right)$ and

$(\forall \jmath \in J) (\exists \imath \in I) \left(\bigcap\limits_{\vartheta \in \Gamma_\jmath} \mathcal{O}^+ (\vartheta) \cap \bigcap\limits_{\vartheta \in \Lambda_\jmath} \mathcal{O}^- (\vartheta) \subseteq \bigcap\limits_{\vartheta \in \Delta_\imath} \mathcal{O}^+ (\vartheta) \right)$, which by the monotonicity (Claim 23) yields

$(\forall \imath \in I) (\exists \jmath \in J) \left((\Gamma_\jmath, \Lambda_\jmath)^+ \subseteq \Delta_\imath^+ = \Delta_\imath \right)$ and

$(\forall \jmath \in J) (\exists \imath \in I) \left(\Delta_\imath = \Delta_\imath{}^+ \subseteq (\Gamma_\jmath, \Lambda_\jmath)^+ \right)$. Furthermore, if the decomposition $Z_n = \bigcup\limits_{\imath \in I} \bigcap\limits_{\vartheta \in \Delta_\imath} \mathcal{O}^+ (\vartheta)$ is minimal, then $(\forall \imath \in I) (\exists \jmath \in J) \left((\Gamma_\jmath, \Lambda_\jmath)^+ \subseteq \Delta_\imath \right)$ implies $(\forall \imath \in I) (\exists \jmath \in J) \left(\Delta_\imath = (\Gamma_\jmath, \Lambda_\jmath)^+ \right)$, since $\bigcap\limits_{\vartheta \in (\Gamma_\jmath, \Lambda_\jmath)^+} \mathcal{O}^+ (\vartheta) \subseteq Z_n$.

Step 3. If $Z_n = \bigcup\limits_{\imath \in I} \bigcap\limits_{\vartheta \in \Delta_\imath} \mathcal{O}^+ (\vartheta)$ and $Z_n = \bigcup\limits_{\imath \in I'} \bigcap\limits_{\vartheta \in \Delta'_\imath} \mathcal{O}^+ (\vartheta)$ for $\Delta_\imath, \Delta'_\imath \Subset \mathbf{n}^{2*2}$ are both minimal, then previous step yields $(\forall \imath \in I) (\exists \jmath \in I') \left(\Delta_\imath = \Delta'_\jmath \right)$ and $(\forall \imath \in I') (\exists \jmath \in I) (\Delta'_\imath = \Delta_\jmath)$, i.e. both $\sum_2$-decompositions are equal (modulo permutation and contraction). Q.E.D.

6 Attachment 3: Proof of Lemmata 7, 15

Lemma 7. By the linearity (Claim 22), $\bigcap\limits_{\vartheta \in \Delta} \mathcal{O}^+ (\vartheta) \subseteq |\overrightarrow{a} \cdot \overrightarrow{x}|$ infers that $\overrightarrow{a} \cdot \overrightarrow{x}$ is a linear combination of $\{\mathcal{O}^+ (\vartheta)\}_{\vartheta \in \Delta}$ in $\mathbb{Q} [\overrightarrow{x}]$; this implication holds true for any $\Delta \subset \mathbf{n}^{2*2}$. Now suppose $\Delta \Subset \mathbf{n}^{2*2}$. In order to strengthen $\mathbb{Q} [\overrightarrow{x}]$ to $\mathbb{Z} [\overrightarrow{x}]$ in the conclusion, let $F := \left\{ u \in \mathbf{n}^2 \mid \left(\exists v \in \mathbf{n}^2 \right) (u, v \in \Delta) \right\}$ be the field of Δ and observe that from $\Delta \Subset \mathbf{n}^{2*2}$ we can extract three disjoint sets $U, V, W \subset \mathbf{n}^2$ and two embeddings $\varphi : V \to U$, $\psi : W \to U$ such that the following three conditions hold for $\Gamma := \{\{v, \varphi (v)\} \mid v \in V\} \subset \mathbf{n}^{2*2}$ and $\Lambda := \{\{w, \varphi (w)\} \mid w \in W\} \subset \mathbf{n}^{2*2}$.

1. $F = U \cup V \cup W$
2. $U = Rng (\varphi) \cup Rng (\varphi)$
3. $\bigcap\limits_{\vartheta \in \Delta} \mathcal{O}^+ (\vartheta) = \bigcap\limits_{\vartheta \in \Gamma} \mathcal{O}^+ (\vartheta) \cap \bigcap\limits_{\vartheta \in \Lambda} \mathcal{O}^- (\vartheta)$

Furthermore, set $\overrightarrow{y} = (y_z)_{z\in\mathbf{n}^2}$ for $y_z := \begin{cases} -x_{\varphi(z)} & \text{if} \quad z\in V \\ x_{\psi(z)} & \text{if} \quad z\in W \\ x_z & \text{else} \end{cases}$. Then $\bigcap\limits_{\vartheta\in\Delta}\mathcal{O}^{+}(\vartheta) = \bigcap\limits_{\vartheta\in\Gamma}\mathcal{O}^{+}(\vartheta)\cap\bigcap\limits_{\vartheta\in\Lambda}\mathcal{O}^{-}(\vartheta) \subseteq |\overrightarrow{a}\cdot\overrightarrow{x}|$ infers $|\overrightarrow{a}\cdot\overrightarrow{y}| = \overrightarrow{\mathbb{R}}_0$. Since $\overrightarrow{a}\cdot\overrightarrow{y}$ admits the unique $\mathbb{Z}[\overrightarrow{x}]$-conversion $\overrightarrow{a}\cdot\overrightarrow{y} = \sum\limits_{z\in\mathbf{n}^2} a_z\cdot y_z = \sum\limits_{u\in U} b_u\cdot x_u$, the last conclusion yields $b_u = 0$, for all $u\in U$. This, in turn, shows that $\overrightarrow{a}\cdot\overrightarrow{x}$ admits the required $\mathbb{Z}[\overrightarrow{x}]$-expansion $\sum\limits_{\imath\in I} c_\imath (x_{u_\imath}+x_{v_\imath})$ for $\{u_\imath, v_\imath\}\in\Delta$, which completes the proof. To illustrate the point, consider two simple cases:

1. $\overrightarrow{a}\cdot\overrightarrow{x} = x_u + 3x_w + 4x_v$ where $u = \varphi(v) = \psi(w)\in U$, $v\in V$, $w\in W$
2. $\overrightarrow{a}\cdot\overrightarrow{x} = x_u + 3x_w - 4x_{w'}$ where $u = \varphi(w) = \varphi(w')\in U$, $w, w'\in W$

Case 1. We have $\overrightarrow{a}\cdot\overrightarrow{y} = x_u + 3x_u - 4x_u = 0\cdot x_u$ and $\overrightarrow{a}\cdot\overrightarrow{x} = (x_u + x_v) + 3(x_w + x_v)$, because $\{v, w\}\in\Gamma$ and $\{u, v\}\in\Lambda$, and hence $\{u, v\}, \{v, w\}\in\Delta$, since Δ is perfect.

Case 2. We still have $\overrightarrow{a}\cdot\overrightarrow{y} = x_u + 3x_u - 4x_u = 0\cdot x_u$, but this time instead of $\{w, w'\}\in\Gamma$ we have only $\{u, w\}, \{u, w'\}\in\Lambda$ from which, however, we can infer $\{u, u'\}, \{u', w\}, \{u', w'\}\in\Delta$, since Δ is perfect. This conclusion yields $\overrightarrow{a}\cdot\overrightarrow{x} = (x_u + x_{u'}) - (x_{u'} + x_{w'}) + 3(x_w + x_{u'}) - 3(x_{u'} + x_{w'})$, as required.

Note. An imperfect $\Delta = \{u, v\}, \{u, w\}, \{v, w\}$, say, fails to produce the disjoint U, V, W in question. As a result, the assumption $\bigcap\limits_{\vartheta\in\Delta}\mathcal{O}^{+}(\vartheta)\subseteq |x_u + 2x_v|$, say, does not infer the conclusion of the lemma.)

Lemma 15. $\|\overrightarrow{a}\cdot\overrightarrow{x}\|\subseteq|\overrightarrow{a}\cdot\overrightarrow{x}|$ is obvious. In the rest of the proof we argue as above and arrive at $\mathbb{Z}[\overrightarrow{x}]$-expansion $\overrightarrow{a}\cdot\overrightarrow{x} = \sum\limits_{\imath\in I} c_\imath (x_{u_\imath} + x_{v_\imath})$, $\{u_\imath, v_\imath\}\in\Delta$. We can just as well assume that for all $\imath, \jmath\in I$, $c_\imath\neq 0$, $u_\imath\neq v_\imath$ and $\{u_\imath, v_\imath\}\neq\{u_\jmath, v_\jmath\}$. On the other hand $\overrightarrow{a}\cdot\overrightarrow{x} = \sum\limits_{u\in X\cup Y} a_u x_u$ holds in $\mathbb{Z}[\overrightarrow{x}]$, where $X = \left\{u\in\mathbf{n}^2 \mid a_u > 0\right\}$ and $Y = \left\{u\in\mathbf{n}^2 \mid a_u < 0\right\}$. Hence $\sum\limits_{\imath\in I} c_\imath (x_{u_\imath} + x_{v_\imath})$ can be further converted, in $\mathbb{Z}[\overrightarrow{x}]$, to the required expression $\sum\limits_{\jmath\in J} d_\jmath \left(x_{u_\jmath} + x_{v_\imath}\right) + \sum\limits_{\kappa\in K} d_\kappa (x_{u_\kappa} - x_{v_\kappa})$ such that for all $\jmath\in I$, $\kappa\in K$, $u_\jmath\neq v_\jmath\in X$, $u_\kappa\neq v_\kappa\in Y$, $\{u_\jmath, v_\jmath\}\in\Delta^{+} = \Delta$ and $\{u_\kappa, v_\kappa\}\in\Delta^{-}$. Since $\bigcap\limits_{\vartheta\in\Delta}\mathcal{O}^{+}(\vartheta) = \bigcap\limits_{\vartheta\in\Delta}\mathcal{O}^{+}(\vartheta)\cap\bigcap\limits_{\vartheta\in\Delta^{-}}\mathcal{O}^{-}(\vartheta)$ (cf. Overview, 4), we arrive at $\bigcap\limits_{\vartheta\in\Delta}\mathcal{O}^{+}(\vartheta)\subseteq\bigcap\limits_{\jmath\in J}\mathcal{O}^{+}(\{u_\jmath, v_\jmath\})\cap\bigcap\limits_{\kappa\in K}\mathcal{O}^{-}(\{u_\kappa, v_\kappa\})\subseteq\|\overrightarrow{a}\cdot\overrightarrow{x}\|$, Q.E.D.

7 Attachment 4: Proof of Lemma 10

Step 1. We observe that $\mathfrak{T}$ can be converted to an equivalent borel polynomial $\mathfrak{S}$ such that $\natural\left(\mathfrak{S}\right)$ is polynomial in the graph-complexity of $\mathfrak{T}$. Here we use familiar conversions corresponding to basic borel (boolean) absorption laws $U\cup U=U$, $U\cap U=U$, $U\cup\left(U\cap V\right)=U\cap V$, $U\cap\left(U\cup V\right)=U$, etc. Clearly $\left|\mathfrak{T}\right|=Z_n$ infers $\left|\mathfrak{S}\right|=Z_n$.

Step 2. Let $\mathfrak{P}$ arise from $\mathfrak{S}$ by substituting regular borel polynomial $\emptyset:=\left(x_{1,1}+x_{1,2}\right)\cap\neg\left(x_{1,1}+x_{1,2}\right)$ for every non-regular literal occurring in $\mathfrak{S}$. Let $\mathfrak{D}:=\partial\left(\mathfrak{P}\right)$, $\mathfrak{D}^{\mathrm{C}}:=\partial^{\mathrm{C}}\left(\mathfrak{P}\right)$ and $\mathfrak{D}^{\mathrm{CP}}:=\partial^{\mathrm{CP}}\left(\mathfrak{P}\right)=\bigcup\limits_{\jmath\in J}\bigcap\limits_{\ell\in L_\jmath}\overrightarrow{a}_{\jmath,\ell}\cdot\overrightarrow{x}$ (see Definitions 8, 9). We show that $\left|\mathfrak{S}\right|=Z_n$ infers $\left|\mathfrak{D}^{\mathrm{CP}}\right|=Z_n$. Clearly $\left|\mathfrak{D}^{\mathrm{C}}\right|=\left|\mathfrak{D}\right|\subseteq\left|\mathfrak{S}\right|=Z_n$, which by the absorption property (Claim 21) yields $\left|\mathfrak{D}^{\mathrm{CP}}\right|\subseteq Z_n$. Now consider the minimal $\sum_2$-decomposition $Z_n=\bigcup\limits_{\imath\in I}\bigcap\limits_{\vartheta\in\Delta_\imath}\mathcal{O}^+\left(\vartheta\right)$, $\Delta_\imath\Subset\mathbf{n}^{2*2}$. We have $Z_n\subseteq\left|\mathfrak{S}\right|=\left|\partial\left(\mathfrak{S}\right)\right|=\left|\partial^{\mathrm{C}}\left(\mathfrak{S}\right)\right|\subseteq\left|\mathfrak{S}^{\mathrm{CP}}\right|$, which by the disjunction property (Claim 20) infers $\left(\forall\imath\in I\right)\left(\exists\jmath\in J\right)\left(\bigcap\limits_{\vartheta\in\Delta_\imath}\mathcal{O}^+\left(\vartheta\right)^+\subseteq\bigcap\limits_{\ell\in L_\jmath}\left|\overrightarrow{a}_{\jmath,\ell}\cdot\overrightarrow{x}\right|\right)$, since by Lemma 7 all clauses containing non-regular positive literals can be removed from $\mathfrak{S}^{\mathrm{CP}}$. Hence $Z_n\subseteq\left|\mathfrak{D}^{\mathrm{CP}}\right|$, Q.E.D.

8 Attachment 5: Proof of Lemma 16

By the assumption, $\left|\mathfrak{P}\right|=Z_n$, while all literals occurring in $\mathfrak{P}$ are positive and regular. Let $\mathfrak{D}:=\partial\left(\mathfrak{P}\right)=\bigcup\limits_{\jmath\in J}\bigcap\limits_{\ell\in L_\jmath}\overrightarrow{a}_{\jmath,\ell}\cdot\overrightarrow{x}$; note that $\mathfrak{D}=\partial^{\mathrm{P}}\left(\mathfrak{P}\right)$, since $\mathfrak{P}$ is positive (see Definitions 8, 9). We show that $\left\|\mathfrak{P}\right\|=Z_n$. Since $\left\|\overrightarrow{a}_{\jmath,\ell}\cdot\overrightarrow{x}\right\|\subseteq\left|\overrightarrow{a}_{\jmath,\ell}\cdot\overrightarrow{x}\right|$, we have $\left\|\mathfrak{P}\right\|=\left\|\mathfrak{D}\right\|\subseteq\left|\mathfrak{D}\right|=\left|\mathfrak{P}\right|=Z_n$. Consider the minimal $\sum_2$-decomposition $Z_n=\bigcup\limits_{\imath\in I}\bigcap\limits_{\vartheta\in\Delta_\imath}\mathcal{O}^+\left(\vartheta\right)$. Since $Z_n\subseteq\left|\mathfrak{P}\right|=\left|\mathfrak{D}\right|$, by the disjunction property (Claim 20) we get $\left(\forall\imath\in I\right)\left(\exists\jmath\in J\right)\left(\bigcap\limits_{\vartheta\in\Delta_\imath}\mathcal{O}^+\left(\vartheta\right)\subseteq\bigcap\limits_{\ell\in L_\jmath}\left|\overrightarrow{a}_{\jmath,\ell}\cdot\overrightarrow{x}\right|\right)$, $\Delta_\imath\Subset\mathbf{n}^{2*2}$. Now by Lemma 15, $\bigcap\limits_{\vartheta\in\Delta_\imath}\mathcal{O}^+\left(\vartheta\right)\subseteq\left|\overrightarrow{a}_{\jmath,\ell}\cdot\overrightarrow{x}\right|$ infers $\bigcap\limits_{\vartheta\in\Delta_\imath}\mathcal{O}^+\left(\vartheta\right)\subseteq\left\|\overrightarrow{a}_{\jmath,\ell}\cdot\overrightarrow{x}\right\|$, and hence $\left(\forall\imath\in I\right)\left(\exists\jmath\in J\right)\left(\bigcap\limits_{\vartheta\in\Delta_\imath}\mathcal{O}^+\left(\vartheta\right)\subseteq\bigcap\limits_{\ell\in L_\jmath}\left\|\overrightarrow{a}_{\jmath,\ell}\cdot\overrightarrow{x}\right\|\right)$, from which we arrive at $Z_n\subseteq\left\|\mathfrak{D}\right\|=\left\|\mathfrak{P}\right\|$, Q.E.D.

9 Attachment 6: Basic combinatorics

To illuminate the underlying combinatorial argument, first suppose that our regular borel polynomial $\mathfrak{P}_n$ is normal, and hence $\left\|\mathfrak{P}_n\right\|=\left|\mathfrak{P}_n\right|$. Furthermore, suppose that $\mathfrak{P}_n$ is positive and every leaf of $\mathfrak{P}_n$ is some $x_{i,j}+x_{k,l}$, i.e. $\mathfrak{O}^+\left(\vartheta\right)$;

call it *proper positive normal case*. Consider the structure of $\mathfrak{P}_n$. The two simplest subcases are $\sum_2$ and $\prod_2$, as follows.

Subcase Σ_2: We have $|\mathfrak{P}_n| = |\partial^{\mathrm{N}}(\mathfrak{P}_n)| = \bigcup\limits_{\sigma\in S}\bigcap\limits_{\vartheta\in\Omega_\sigma}\mathcal{O}^{+}(\vartheta)$, $\Omega_\sigma \subseteq \mathbf{n}^{2*2}$, where $\#(S)$ is polynomial in n. Moreover, by Theorem 2 (first condition) we have $B_n \subseteq \{\Omega_\sigma^{+} \mid \sigma \in S\}$. Hence the number of distinct $\Delta_\imath$ from B_n is also polynomial in n. However, it is readily seen by the definition 3.1.2 that $\#(B_n)$ is in fact exponential in n - a contradiction.

Subcase Π_2: We have $\mathfrak{P}_n = \bigcap\limits_{k=1}^{m}\bigcup\limits_{\vartheta\in\Gamma_k}\mathfrak{O}^{+}(\vartheta)$, $\partial^{\mathrm{N}}(\mathfrak{P}_n) = \bigcup\limits_{\sigma\in S}\bigcap\limits_{\vartheta\in\Omega_\sigma}\mathfrak{O}^{+}(\vartheta)$, where $\Gamma_k, \Omega_\sigma \subseteq \mathbf{n}^{2*2}$ and $\{\mathfrak{O}(\vartheta) \mid \vartheta \in \Omega_\sigma\}_{\sigma\in S}$ is the set of choice sequences over $\{\mathfrak{O}(\vartheta) \mid \vartheta \in \Gamma_k\}_{k\in\mathbf{m}}$. For a moment consider the most transparent

Subsubcase: $\Gamma_k = \{\{\langle f_k(i), i\rangle, \langle f_k(j), j\rangle\} \mid i < j \in \mathbf{m}\}$ for $f_k : \mathbf{n} \to \mathbf{n}$. By the shape of Φ_n, this obviously yields $Z_n \subseteq |\mathfrak{P}_n|$. The required contradiction to $|\mathfrak{P}_n| \subseteq Z_n$ follows from the assumption that m is polynomial in n, which infers that for large n, the collection $\{f_k\}_{k\in\mathbf{m}}$ occurring in $\mathfrak{P}_n$ is not representative for all functions $f : \mathbf{n} \to \mathbf{n}$ occurring in Φ_n. To put it formal terms, the contradiction follows directly from combinatorial observation stating that

$$\begin{gathered}(\forall f_1, \cdots, f_m : \mathbf{n} \to \mathbf{n})\,(\exists f : \mathbf{n} \to \mathbf{n})\,(\exists i_1 < j_1, \cdots, i_m < j_m \in \mathbf{n})\\ \left(\begin{gathered}\{\{\langle f_k(i_k), i_k\rangle, \langle f_k(j_k), j_k\rangle\}\}^{+}_{k\in\mathbf{m}} \Subset \mathbf{n}^{2*2} \wedge (\forall \ell \in \mathbf{m})\\ \left(\{\langle f(i_\ell), i_\ell\rangle, \langle f(j_\ell), j_\ell\rangle\} \notin \{\{\langle f_k(i_k), i_k\rangle, \langle f_k(j_k), j_k\rangle\}\}^{+}_{k\in\mathbf{m}}\right)\end{gathered}\right)\end{gathered}$$

holds for sufficiently large n, provided that m is merely polynomial in n.[3]

Subcase Π_2 proper: $\Gamma_k \subseteq \mathbf{n}^{2*2}$. We let:

$$\bigotimes_{k=1}^{m}\Gamma_k := \left\{(Rng(f))^{+} \mid f : \mathbf{m} \ni k \mapsto f(k) \in \Gamma_k\right\}$$

$$B_n \subset \widehat{B}_n := \left\{\Theta \subseteq \mathbf{n}^{2*2} \mid (\exists \Delta \in B_n)\,(\Delta \subseteq \Theta)\right\}$$

and arrive at combinatorial lemma stating that

$$\left(\forall \Gamma_1, \cdots, \Gamma_m \subseteq \mathbf{n}^{2*2}\right)\left(B_n \nsubseteq \bigotimes_{k=1}^{m}\Gamma_k \vee \bigotimes_{k=1}^{m}\Gamma_k \nsubseteq \widehat{B}_n\right)$$

holds for sufficiently large n, provided that m is merely polynomial in n.

Proper positive normal case just generalizes these simplest subcases. Arbitrary regular borel polynomials $\mathfrak{P}_n$ are more involved (see Attachment 7 below).

---

[3] In fact, this subsubcase follows from the known result stating that standard sequent calculus approach to boolean validity problem is exponential in the input length, see [T] (one can also use [H]).

10 Attachment 7: Combinatorial translations

10.1 Basic notions (cf. Overview 2.1 and Attachment 6)

$$\mathbf{n}_{+}^{2*2} := \{0\} \cup \mathbf{n}^{2*2}$$

$$U \oslash V := \begin{cases} U - \{0\} & \text{if} \quad U \cap V = \{0\} \\ \emptyset & \text{else} \end{cases}$$

$$\mathbb{A}_m := \left\{ \begin{array}{c} \overrightarrow{a} = (a_u) \in \mathbb{Z}_{\mathbf{0}}^{n^2} \mid \gcd\{a_u \neq 0\} = 1 \wedge a_{\min\{u \mid a_u \neq 0\}} > 0 \wedge [\overrightarrow{a}]^2 \neq \emptyset \\ \wedge \natural(\overrightarrow{a}) \leq m \end{array} \right\}$$

$$\mathbb{A}_m^{+} := \{0\} \cup \mathbb{A}_m$$

$$U_1 \oplus \cdots \oplus U_k := \{u_1 \cup \cdots \cup u_k \mid u_1 \in U_1, \cdots, u_k \in U_k\}$$

$$[\overrightarrow{a}]_1^2 := \left\{\Gamma(S) \mid S \in [\overrightarrow{a}]^2\right\}, \ [\overrightarrow{a}]_2^2 := \left\{\Lambda(S) \mid S \in [\overrightarrow{a}]^2\right\}$$

$$A = \{\overrightarrow{a}_1, \cdots, \overrightarrow{a}_k\} \subset \mathbb{A}_m \hookrightarrow \begin{cases} \Gamma(A) := [\overrightarrow{a}_1]_1^2 \oplus \cdots \oplus [\overrightarrow{a}_k]_1^2 \\ \Lambda(A) := [\overrightarrow{a}_1]_2^2 \oplus \cdots \oplus [\overrightarrow{a}_k]_2^2 \end{cases}$$

Definition 24 *Let $\mathcal{T}$ be a finite rooted tree. By ρ, $\mathcal{T}_0$ and $\mathcal{T}_1$ we denote the root of $\mathcal{T}$, the leaves of $\mathcal{T}$ and the subtree of $\mathcal{T}$ obtained by deleting all leaves, respectively. Moreover, we assume that every node $\nu \in \mathcal{T}_1$ is labelled by $\ell(\nu) \in \{\cap, \cup\}$. For any pair of leaves $\sigma, \varsigma \in \mathcal{T}_0$, we denote by $\sigma \sqcap \varsigma$ the closest common ancestor of σ and ς, in $\mathcal{T}$. $\mathcal{T}$ is called a $\prod$-tree iff $\rho \in \mathcal{T}_1$ and $\ell(\rho) = \cap$. A set of leaves $X \subseteq \mathcal{T}_0$ is called a cut iff for every pair $\sigma \neq \varsigma \in X$, $\ell(\sigma \sqcap \varsigma) = \cap$. A maximal cut is called a clause (in $\mathcal{T}$). Denote by $\mathfrak{C}(\mathcal{T})$ the set of all clauses (in $\mathcal{T}$); thus $\mathfrak{C}(\mathcal{T}) \subseteq \wp(\mathcal{T}_0)$.*

10.2 Proper positive normal case

10.2.1 Subcase Π_2 revisited

Notation 25 *For any $m > 0$, consider arbitrary functions $F : \mathbf{m}^2 \to \mathbf{n}^{2*2}$ and $f : \mathbf{m} \to \mathbf{m}$. Define $F_f : \mathbf{m} \to \mathbf{n}^{2*2}$ and $\otimes F \subseteq \wp\left(\mathbf{n}^{2*2}\right)$ by:*

$$F_f(x) := F(x, f(x))$$

$$\begin{aligned} \otimes F &:= \left\{Rng(F_f)^{+} \mid f : \mathbf{m} \to \mathbf{m}\right\} = \left\{\{F(x, f(x))\}_{x \in \mathbf{m}}^{+}\right\}_{f : \mathbf{m} \to \mathbf{m}} \\ &= \left\{\{F(1, x_1), \cdots, F(m, x_m)\}^{+}\right\}_{x_1, \cdots, x_m \in \mathbf{m}} \end{aligned}$$

Claim 26 *Proper positive normal $\prod_2$-subcase of $\boldsymbol{NP} \neq \boldsymbol{P}$ is derivable from the following combinatorial principle. Suppose n is sufficiently large and m merely polynomial in n. Then for any F as above, either $B_n \nsubseteq \otimes F$ or $\otimes F \nsubseteq \widehat{B}_n$.*

10.2.2 General case

Notation 27 *Let* $\mathcal{T}$ *be a* $\prod$*-tree with leaf-labeling* $F : \mathcal{T}_0 \rightarrow \mathbf{n}^{2*2}$*. For any* $X \in \mathfrak{C}(\mathcal{T})$ *set:*

$$F[X] := \{F(\sigma) \mid \sigma \in X\} \subseteq \mathbf{n}^{2*2}$$

$$\mathcal{T} \boxdot F := \left\{ F[X]^{+} \mid X \in \mathfrak{C}(\mathcal{T}) \right\} \subseteq \wp\left(\mathbf{n}^{2*2}\right)$$

Claim 28 *Proper positive normal case of* $\boldsymbol{NP} \neq \boldsymbol{P}$ *is derivable from the following combinatorial principle. Suppose* n *is sufficiently large and* $\#(\mathcal{T})$ *merely polynomial in* n*. Then for any* F *as above, either* $B_n \nsubseteq \mathcal{T} \boxdot F$ *or* $\mathcal{T} \boxdot F \nsubseteq \widehat{B}_n$*.*

10.3 Proper normal case

Notation 29 *Let* $\mathcal{T}$ *be a* $\prod$*-tree with two leaf-labelings* $F, G : \mathcal{T}_0 \rightarrow \mathbf{n}_{+}^{2*2}$ *such that for every* $\sigma \in \mathcal{T}_0$*,* $F(\sigma) = 0 \Leftrightarrow G(\sigma) \neq 0$*. For any* $X \in \mathfrak{C}(\mathcal{T})$ *set:*

$$F[X] := \{F(\sigma) \mid \sigma \in X\}, \ G[X] := \{G(\sigma) \mid \sigma \in X\} \subseteq \mathbf{n}_{+}^{2*2}$$

$$\mathcal{T} \boxdot (F \oslash G) := \left\{ (F[X] \oslash G[X])^{+} \mid X \in \mathfrak{C}(\mathcal{T}) \right\} \subseteq \wp\left(\mathbf{n}^{2*2}\right)$$

Claim 30 *Proper normal case of* $\boldsymbol{NP} \neq \boldsymbol{P}$ *that is obtained from previous case by dropping the positive restriction is derivable from the following combinatorial principle. Suppose* n *is sufficiently large and* $\#(\mathcal{T})$ *merely polynomial in* n*. Then for any* F *and* G *as above, either* $B_n \nsubseteq \mathcal{T} \boxdot (F \oslash G)$ *or* $\mathcal{T} \boxdot (F \oslash G) \nsubseteq \widehat{B}_n$*.*

10.4 General case

Notation 31 *Let* $\mathcal{T}$ *be a* $\prod$*-tree with two leaf-labelings* $F, G : \mathcal{T}_0 \rightarrow \mathbb{A}_m^{+}$ *such that for every* $\sigma \in \mathcal{T}_0$*,* $F(\sigma) = 0 \Leftrightarrow G(\sigma) \neq 0$*. For any* $X \in \mathfrak{C}(\mathcal{T})$ *set:*

$$F[X] := \{F(\sigma) \mid \sigma \in X\}, \ G[X] := \{G(\sigma) \mid \sigma \in X\} \subseteq \mathbb{A}_m^{+}$$

$$\mathcal{T} \boxtimes (F \oslash G) := \left\{ \begin{array}{c} (\Gamma(F[X] \oslash G[X]), \Lambda(F[X] \oslash G[X]))^{+} \\ \mid X \in \mathfrak{C}(\mathcal{T}) \end{array} \right\} \subseteq \wp\left(\mathbf{n}^{2*2}\right)$$

Claim 32 $\boldsymbol{NP} \neq \boldsymbol{P}$ *is derivable from the following combinatorial principle. Suppose* n *is sufficiently large and* $\#(\mathcal{T})$ *merely polynomial in* n*. Then for any* F *and* G *as above, either* $B_n \nsubseteq \mathcal{T} \boxtimes (F \oslash G)$ *or* $\mathcal{T} \boxtimes (F \oslash G) \nsubseteq \widehat{B}_n$*.*

11 References

`[GK]`: L. Gordeev, A. Krebs, *Elementary interpretations of P vs. NP*, Second St. Petersburg Logic Days, 2003 (to appear in APAL).

`[GMaple]`: L. Gordeev, *Base* B_3, Preprint (Maple text), 2004

`[H]`: A. Haken, *The intractability of resolution*, Theor. Comp. Sci. **39** (1985),

297-308

`[RR]`: A. Razborov, S. Rudich, *Natural proofs*, J. Comp. Sys. Sci. **55** (1997), 24-35

`[T]`: G. Takeuti, *Computational complexity and proof theory*, Sugaku **39** (2),

1987, 110-123 (Transl. in **AMS** Sugaku expositions **0** (1), 1988, 1-14