

Combinatorial sentence that infers $P < NP$

L. Gordeev, FTICA, WSI f. Informatik

Tübingen/Falkensee

gordeew@informatik.uni-tuebingen.de

1 Summary

We present a plausible, purely combinatorial Ramsey-style sentence CS that infers, in Peano Arithmetic, the negative solution (abbr.: $\mathcal{P} < \mathcal{NP}$) to the familiar open problem $\mathcal{P} \stackrel{?}{=} \mathcal{NP}$. Validity of CS is briefly discussed; it will be elaborated and presented in more detail elsewhere. This work is both a simplified and extended version of [G04]. The simplification, due to A. Krebs, says that what was called the *proper normal case* in [G04] is in fact sufficient for $\mathcal{P} < \mathcal{NP}$ (see Theorem 27 in the text).

1.1 Background

1.1.1 Boolean space

Let $\mathbb{B}^n[\mathbf{2}]$ be the space of n -variable boolean polynomials. We summarize basic algebraic properties of $\mathbb{B}^n[\mathbf{2}]$ like e.g. the existence and uniqueness of minimal positive DNF, which in the sequel is referred to as the *positive base* (abbr.: PB). We describe the corresponding “school-algebra” algorithm $f \mapsto \text{BASE}(f)$ producing PB of arbitrary *basic* polynomials f , i.e. f having the same boolean values as given *positive* polynomials g , i.e. g containing only positive literals. In $\mathbb{B}^n[\mathbf{2}]$, we pose a following question:

Q: How big must be a basic polynomial f whose PB, $\text{BASE}(f)$, is isomorphic to a given “big” and “complex” PB g ?

Furthermore, we consider the familiar CoNP-complete DNF validity problem, in $\mathbb{B}^n[\mathbf{2}]$, and note that nontrivial valid DNF are not basic. Hence $\mathcal{P} \stackrel{?}{=} \mathcal{NP}$ is seemingly not related to Q.

1.1.2 Borel space

We consider a suitable real space of n^2 -variable Borel polynomials, $\mathbb{B}^{n^2}[\mathbb{R}_0]$, and elaborate basic algebraic theory along the lines of $\mathbb{B}^n[\mathbf{2}]$ (see above), except that in the Borel case, our basic proof tools are geometrical by nature. By definition the domain of $\mathbb{B}^{n^2}[\mathbb{R}_0]$ is the non-zero part, \mathbb{R}_0 , of the real continuum \mathbb{R} . Note that $\mathbb{B}^n[\mathbf{2}]$ is a discrete subspace of $\mathbb{B}^{n^2}[\mathbb{R}_0]$. We prove the existence and uniqueness of the appropriate *positive base* (abbr.: PB), in $\mathbb{B}^{n^2}[\mathbb{R}_0]$, and generalize the boolean “school-algebra” algorithm BASE , accordingly; let BASE_0 denote this Borel generalization. The corresponding Borel modification of Q reads as follows, in $\mathbb{B}^{n^2}[\mathbb{R}_0]$:

Q_0 : How big must be a basic polynomial f whose PB, $\text{BASE}_0(f)$, is isomorphic to a given “big” and “complex” PB g ?

Furthermore, we observe that the whole DNF family of \mathbb{B}^n [2] is representable in $\mathbb{B}^{n^2}[\mathbb{R}_0]$ by one “universal” positive CNF Φ_n ; such Φ_n is explicitly defined. We observe that PB $g := \text{BASE}_0(\Phi_n)$ is “big” and “complex”, relative to n . Having this we conjecture that the following condition C_0 answers the corresponding specification of Q_0 .

Definition 1 *Let C_0 abbreviate “for every $c \in \mathbb{N}$ there is a $n \in \mathbb{N}$ so large that the size of any basic polynomial f , in $\mathbb{B}^{n^2}[\mathbb{R}_0]$, satisfying $\text{BASE}_0(f) = \text{BASE}_0(\Phi_n)$ (mod isomorphism), is bigger than n^c ”.*

Next we observe that the hypothesis $\mathcal{P} = \mathcal{NP}$ is actually stronger than its “naive” discrete translation. Loosely speaking, $\mathcal{P} = \mathcal{NP}$ says that Φ_n can be characterized by an equivalent “small” (say, polynomial-size) algebraic polynomial f . The equivalence $\Phi_n \sim f$ in question usually refers to extensional equality $\Phi_n \sim_D f := (\forall x \in D) (\Phi_n(x) = f(x))$ in a given discrete domain $D \subset \mathbb{N}$ (by standard encoding we can just as well set $D := \mathbb{N}$). However, a closer look at the computing nature of $\mathcal{P} = \mathcal{NP}$ enables us to regard D as an arbitrary model of an appropriate simple algebra; in particular, we can also set $D := \mathbb{R}_0$ (see [GK] for the corresponding algebraic elaboration). Now clearly the condition $\Phi_n \sim_{\mathbb{R}_0} f$ is more restrictive than $\Phi_n \sim_{\mathbb{N}} f$, and hence passing from $\mathcal{P} = \mathcal{NP}$ to $\Phi_n \sim_{\mathbb{R}_0} f$, instead of $\Phi_n \sim_{\mathbb{N}} f$, can provide us with more insight into the structure of any hypothetical f in question. Actually we can pass from $\Phi_n \sim_{\mathbb{R}_0} f$ to $\text{BASE}_0(f) = \text{BASE}_0(\Phi_n)$ and thereby arrive at the following

Conclusion 2 *In Peano Arithmetic, C_0 infers $\mathcal{P} < \mathcal{NP}$.*

This conclusion gives us a hint how to construct the desired combinatorial sentence CS.

1.2 The results

1.2.1 Basic notations

1. Let $n > 1$ and $\mathbf{n} := \{1, \dots, n\}$. For any $i, j \in \mathbf{n}$ let $(i, j) := n(i-1) + j$
2. Let $\mathbf{n}^{2*2} := \{\{(i, j), (k, l)\} \mid i, j, k, l \in \mathbf{n} \wedge j \neq l\}$
3. For any $X \subset \mathbf{n}^{2*2}$ let $X^+ \subset \mathbf{n}^{2*2}$ be the minimal closure of X satisfying the following conditions:
 - (a) $X \subset X^+$
 - (b) if $\{\{u, v\}, \{v, w\}, \{w, z\}\} \subset X^+$ and $\{u, z\} \in \mathbf{n}^{2*2}$, then $\{u, z\} \in X^+$
 - (c) if $\{\{u, v\}, \{v, w\}, \{w, u\}\} \subset X^+$ then $X^+ := \mathbf{n}^{2*2}$
4. Let $\mathbf{n}_+^{2*2} := \{0\} \cup \mathbf{n}^{2*2}$

5. For any $X, Y \subset \mathbf{n}_+^{2*2}$ let

$$X \circledast Y := \begin{cases} X & \text{if } X \cap Y = \emptyset \\ \emptyset & \text{else} \end{cases}$$

6. Let $\Omega_n \subset \mathbf{n}^{2*2}$ be the canonical numerical encoding of $\text{BASE}_0(\Phi_n)$

7. Let $\widehat{\Omega}_n := \{X \subset \mathbf{n}^{2*2} \mid (\exists Y \in \Omega_n)(Y \subset X)\}$

8. Let \mathcal{T} be a finite rooted binary-branching tree whose gates a are supplied with labels $\partial(a) \in \{\wedge, \vee\}$. Denote by $L_{\mathcal{T}}$, $G_{\mathcal{T}}$ and $\#(\mathcal{T})$ the sources, the gates and the size (= total number of all nodes) of \mathcal{T} , respectively. For any $a \neq b \in G_{\mathcal{T}}$, denote by $a \sqcap b$ the *closest common ancestor* of a and b , in \mathcal{T} . A set of sources $X \subset L_{\mathcal{T}}$ is called *conjunctive* iff for every $a \neq b \in X$, $\partial(a \sqcap b) = \wedge$. Maximal conjunctive sets of sources are called *cuts*, in \mathcal{T} . Denote by $\mathcal{S}_{\mathcal{T}}$ the set of all cuts in \mathcal{T} ; clearly $\mathcal{S}_{\mathcal{T}} \subset \wp(L_{\mathcal{T}})$.

1.2.2 The sentence

Definition 3 Let \mathcal{T} be a tree enriched by two source-labeling functions $\varrho_1, \varrho_2 : L_{\mathcal{T}} \rightarrow \mathbf{n}_+^{2*2}$ such that for every $a \in L_{\mathcal{T}}$, $\varrho_1(a) \neq 0 \Leftrightarrow \varrho_2(a) = 0$. Let

$$\mathfrak{D}^2(\mathcal{T}) := \left\{ (\varrho_1(X) - \{0\})^+ \circledast \varrho_2(X) \mid X \in \mathcal{S}_{\mathcal{T}} \right\} - \{\emptyset\}$$

Denote by CS the following combinatorial sentence. For any enriched tree \mathcal{T} , as above, either $\Omega_n \not\subseteq \mathfrak{D}^2(\mathcal{T})$ or $\mathfrak{D}^2(\mathcal{T}) \not\subseteq \widehat{\Omega}_n$ holds true, provided that n is sufficiently large and $\#(\mathcal{T})$ merely polynomial in n .

Theorem 4 In Peano Arithmetic, CS infers C_0 .

Corollary 5 The validity of CS infers $\mathcal{P} < \mathcal{NP}$.

Proof. See Theorems 34, 39 below. ■

Remark 6 We believe that CS is valid. The desired proof runs by induction on standard Σ_k/Π_k structural tree-complexity, while analyzing complex topological structure of Ω_n . The initial cases Σ_2, Π_2 and Σ_3 are derivable in Peano Arithmetic. The desired induction step $\Sigma_k/\Pi_k \mapsto \Sigma_{k+1}/\Pi_{k+1}$ will be elaborated and formalized elsewhere; notably, the bigger the canonical proof theoretical strength of $\mathcal{P} < \mathcal{NP}$, the better a polynomial-time approximation of \mathcal{NP} (see [BDH]).

2 Introduction

2.1 n-dim Boolean space

2.1.1 Description

Designation: $\mathbb{B}^n[2]$

Structure:

1. Vocabulary:
 - (a) Variables $\mathbf{v}_1, \dots, \mathbf{v}_n$ (abbr.: x, y, z - possibly indexed)
 - (b) Binary operations \vee, \wedge and unary operation $\bar{}$
2. Literals: terms x and \bar{x} (abbr.: ℓ - possibly indexed)
3. Polynomials (abbr.: f, g, h - possibly indexed):
 - (a) Arbitrary polynomials: arbitrary terms of the language
 - (b) Strictly positive polynomials: $(\bar{})$ -free polynomials
 - (c) Basic polynomials: polynomials which are equivalent to strictly positive polynomials (see 5 (a) below)
 - (d) Normal forms:
 - i. PNF (*positive normal form*): polynomials built up from literals by \vee and \wedge
 - ii. DNF (*disjunctive normal form*): polynomials in Σ_2 -form $\bigvee_{i=1}^k \bigwedge_{j=1}^{s_i} \ell_{i,j}$
 - iii. CNF (*conjunctive normal form*): polynomials in dual Π_2 -form $\bigwedge_{i=1}^k \bigvee_{j=1}^{s_i} \ell_{i,j}$
 - iv. PB (*positive base*): DNF $\bigvee_{i=1}^k \bigwedge_{j=1}^{s_i} x_{i,j}$ such that for $1 \leq q < r \leq k$, the lists $X_q := [x_{q,j} \mid j = 1, \dots, s_q]$, $X_r := [x_{r,j} \mid j = 1, \dots, s_r]$ are sets which are mutually incomparable with respect to \subset , i.e. $X_q \not\subseteq X_r$ and $X_r \not\subseteq X_q$
4. Boolean evaluations $Val(f) \in \{0, 1\}$ for $Val(\mathbf{v}_i) \in \{0, 1\}$: as usual
5. Equality:
 - (a) f and g are *equivalent* (abbr.: $f \sim g$) iff they have the same boolean values $Val(f) = Val(g)$, for all boolean evaluations of the variables
 - (b) Two PB $f = \bigvee_{i=1}^k \bigwedge_{j=1}^{s_i} x_{i,j}$ and $g = \bigvee_{i=1}^l \bigwedge_{j=1}^{t_i} y_{i,j}$ are *isomorphic* (abbr.: $f \approx g$), if $k = l$ and the sets $\{\{x_{i,j} \mid j = 1, \dots, s_i\} \mid i = 1, \dots, k\}$ and $\{\{y_{i,j} \mid j = 1, \dots, t_i\} \mid i = 1, \dots, l\}$ are equal.
6. The *algebraic size* of f , $\#(f)$, is the number of all operation occurrences in f

2.1.2 Basic properties

Theorem 7 *The following hold in \mathbb{B}^n [2]:*

1. *Every polynomial has an equivalent PNF*
2. *Every polynomial has an equivalent DNF (CNF).*
3. *Every strictly positive polynomial has an equivalent PB*
4. *For any PB f and g , if $f \sim g$ then $f \approx g$*
5. *Every basic polynomial f has the unique (mod \approx) isomorphic PB, which is called the base of f .*

Proof. 1. Apply the rewrite rules $(f \vee g)^- \leftrightarrow f^- \wedge g^-$, $(f \wedge g)^- \leftrightarrow f^- \vee g^-$, $\bar{x}^- \leftrightarrow x$ to arbitrary subterms so long as possible.

2. Take a PNF (by 1) and apply the rewriting rules $(f \vee g) \wedge h \leftrightarrow f \wedge h \vee g \wedge h$ and $h \wedge (f \vee g) \leftrightarrow (h \wedge f) \vee (h \wedge g)$ for DNF (dual rules $f \vee (g \wedge h) \leftrightarrow (f \vee g) \wedge (f \vee h)$ and $(g \wedge h) \vee f \leftrightarrow (g \vee f) \wedge (h \vee f)$ for CNF) to arbitrary subterms so long as possible.

3. Take a DNF (by 2), contract conjunctions by deleting all repetitions, and afterwards delete all but minimal conjunctions, i.e. those whose sets of variables are proper extensions of other conjunctions' sets of variables.

4. Suppose $\bigvee_{i=1}^k \bigwedge_{j=1}^{s_i} x_{i,j} = f \approx g = \bigvee_{i=1}^l \bigwedge_{j=1}^{t_i} y_{i,j}$. Let

$Set_i(f) := \{x_{i,j} \mid j = 1, \dots, s_i\}$ and $Set_i(g) := \{y_{i,j} \mid j = 1, \dots, t_i\}$
and note that:

$Val(f) = 1$ iff $(\exists i = 1, \dots, k) (\forall x \in Set_i(f)) (Val(x) = 1)$,

$Val(g) = 1$ iff $(\exists i = 1, \dots, l) (\forall y \in Set_i(g)) (Val(y) = 1)$.

Hence

$$f \sim g \leftrightarrow \left(\begin{array}{l} (\forall i = 1, \dots, k) (\exists i = 1, \dots, l) (Set_i(f) \subseteq Set_i(g)) \wedge \\ (\forall i = 1, \dots, l) (\exists i = 1, \dots, k) (Set_i(g) \subseteq Set_i(f)) \end{array} \right)$$

Now by the definition of PB, we can replace above every \subseteq by $=$ and arrive at $f \sim g \leftrightarrow f \approx g$, as required.

5. It follows directly from 3 and 4. Note that the base of f is obtained by a simple algorithm **BASE** that extends a DNF conversion by first deleting all inconsistent conjunctions (i.e. those containing both x and \bar{x}) and all negative literals in the remaining consistent conjunctions, and afterwards removing all repetitions and all but minimal conjunctions as indicated in 2 (see example below). ■

Example 8 *We illustrate main algorithms involved (for brevity we first rename \vee and \wedge by $+$ and \cdot , respectively, and later omit \cdot as usual in school algebra).*

1. Consider a PNF $f = ((x + y) \cdot (z + x) + (u + x) \cdot (x + \bar{x})) \cdot (y + \bar{y})$. Clearly $f \sim g$ where $g = (x + y) \cdot (z + x) + u + x$ is strictly positive. We search for the PB of f . Our basic DNF conversion of f is given by the familiar school-algebra conversion EXPAND:

$$\text{EXPAND}(f) = xzy + xz\bar{y} + xxy + x\bar{x}\bar{y} + yzy + yz\bar{y} + xyy + xy\bar{y} + uxy + u\bar{x}\bar{y} + u\bar{x}y + u\bar{x}\bar{y} + xxy + x\bar{x}\bar{y} + x\bar{x}y + x\bar{x}\bar{y}$$

2. We upgrade EXPAND to EXPANDC by deleting all inconsistent (zero) products:

$$\text{EXPANDC}(f) = xzy + xz\bar{y} + xxy + x\bar{x}\bar{y} + yzy + xyy + uxy + u\bar{x}\bar{y} + u\bar{x}y + u\bar{x}\bar{y} + xxy + x\bar{x}\bar{y}$$

3. We further upgrade EXPANDC to EXPANDCP by deleting all negative literals:

$$\text{EXPANDCP}(f) = xzy + xz + xxy + xx + yzy + xyy + uxy + ux + uy + u + xxy + xx$$

4. Finally, we remove all repetitions and all but minimal products and arrive at the desired PB of f :

$$\text{BASE}(f) = x + yz + u$$

Lemma 9 Working in \mathbb{B}^n [2], for any basic polynomials f and g we have:

1. $\text{BASE}(f)$ is a PB
2. $f \sim \text{EXPAND}(f) \sim \text{EXPANDC}(f) \sim \text{EXPANDCP}(f) \sim \text{BASE}(f)$
3. $f \sim g$ infers $\text{BASE}(f) \approx \text{BASE}(g)$

Proof. Straightforward by the definitions used (see above Example 2). A passage from EXPANDC to EXPANDCP (Example 2 (3)) preserves \sim by induction on the number of negative literals occurring in $\text{EXPANDC}(f)$, as follows.

Let $g = (\bar{x} \wedge y_1 \wedge \cdots \wedge y_l) \vee \bigvee_{i=1}^k \bigwedge_{j=1}^{s_i} \ell_{i,j}$, $g' := (y_1 \wedge \cdots \wedge y_l) \vee \bigvee_{i=1}^k \bigwedge_{j=1}^{s_i} \ell_{i,j}$, $h =$

$\bigvee_{i=1}^r \bigwedge_{j=1}^{t_i} x_{i,j}$ such that $g \sim h$ and $x \notin \{y_1, \dots, y_l\}$, since g is consistent. Clearly

$\text{Val}(x) := 0$, $\text{Val}(y_1) = \cdots = \text{Val}(y_l) := 1$ and $\text{Val}(z) := 0$ for other variables z occurring in g, h yields $\text{Val}(g) = \text{Val}(h) = 1$. Hence there exists $a \leq r$ with $\{x_{a,1}, \dots, x_{a,t_a}\} \subseteq \{y_1, \dots, y_l\}$. Moreover, for any variable evaluation we have $\text{Val}(g') \geq \text{Val}(g) = \text{Val}(h)$. Suppose there is a one satisfying $\text{Val}(g') = 1 > 0 = \text{Val}(h)$. Since $\text{Val}(h) = \text{Val}(g)$, in that case we can just as well assume $\text{Val}(x) = 1$ and $\text{Val}(y_1) = \cdots = \text{Val}(y_l) = 1$, which infers $\text{Val}(x_{a,1} \wedge \cdots \wedge x_{a,t_a}) = 1 = \text{Val}(h)$ - a contradiction. Hence $g' \sim h$, Q.E.D. ■

Remark 10

1. For arbitrary f , the conversion to $\text{BASE}(f)$ must not necessarily preserve boolean equivalence. This is because EXPANDCP does not preserve \sim in the whole polynomial domain. For example, $\text{EXPANDCP}(x \vee \bar{x}) = x \not\sim x \vee \bar{x}$.

2. There is no natural “confluent” modification of DNF that preserves the uniqueness property in the whole polynomial domain. To grasp the point note that $x \vee \bar{x} \sim y \vee \bar{y}$ holds for all x and y .

2.1.3 Labeled trees and circuits

Working in \mathbb{B}^n [2], polynomials are naturally represented by finite rooted trees whose leaves (= sources) and other nodes (= gates) are labeled by arbitrary variables and operation names, respectively. A given strictly positive polynomial (PNF) is further specified by a rooted tree whose sources and gates are labeled by arbitrary variables (literals) and positive operation names \vee, \wedge , respectively. The corresponding labeled circuits provide more economical interpretations allowing us to identify different roots of equal subtrees. We are mostly interested in PNF, so in the sequel our definitions will be specified accordingly.

Definition 11 Let \mathcal{T} be a finite rooted binary-branching labeled tree. By $R_{\mathcal{T}}, L_{\mathcal{T}}, G_{\mathcal{T}}$ and $\#(\mathcal{T})$ we denote the root, the sources, the gates and the size (= total number of all nodes) of \mathcal{T} , respectively. \mathcal{T}_- denotes the subtree of \mathcal{T} obtained by deleting $R_{\mathcal{T}}$. We also assume that all gates $a \in G_{\mathcal{T}}$ are supplied with labels $\partial(a) \in \{\wedge, \vee\}$.

Furthermore, suppose that \mathcal{T} is enriched by a source-labeling function $\varrho : L_{\mathcal{T}} \rightarrow Y$; in the sequel we call such labeled tree enriched. In case $\varrho(a)$ are literals for all $a \in L_{\mathcal{T}}$, \mathcal{T} uniquely determines a PNF $f_{\mathcal{T}}$ that is defined by recursion on $\#(\mathcal{T})$:

1. if $\mathcal{T} = \{R_{\mathcal{T}}\}$ then $f_{\mathcal{T}} := \varrho(R_{\mathcal{T}})$
2. if $\mathcal{T}_- = \mathcal{T}' \uplus \mathcal{T}''$ and $\partial(R_{\mathcal{T}}) = \wedge$, then $f_{\mathcal{T}} := f_{\mathcal{T}'} \wedge f_{\mathcal{T}''}$
3. if $\mathcal{T}_- = \mathcal{T}' \uplus \mathcal{T}''$ and $\partial(R_{\mathcal{T}}) = \vee$, then $f_{\mathcal{T}} := f_{\mathcal{T}'} \vee f_{\mathcal{T}''}$

If $f = f_{\mathcal{T}}$ then \mathcal{T} is called a tree of a given PNF f .

Definition 12 Let \mathcal{C} be a finite directed acyclic rooted binary-branching labeled graph, also called a circuit. Thus every tree is a circuit. Let $R_{\mathcal{C}}, L_{\mathcal{C}}, G_{\mathcal{C}}, \#(\mathcal{C}), \mathcal{C}_-, \partial, \varrho$ and $f_{\mathcal{C}}$ be natural generalizations of the analogous tree-notations from previous definition. An enriched \mathcal{C} of minimal size satisfying $f = f_{\mathcal{C}}$ is called a circuit of a given PNF f .

Definition 13 Let \mathcal{T} be an enriched tree, as in Definition 11. For any $a \neq b \in G_{\mathcal{T}}$, denote by $a \sqcap b$ the closest common ancestor of a and b , in \mathcal{T} . A set of sources $X \subset L_{\mathcal{T}}$ is called conjunctive iff for every $a \neq b \in X$, $\partial(a \sqcap b) = \wedge$. Maximal conjunctive sets of sources are called cuts, in \mathcal{T} . A given cut X in \mathcal{T} is called consistent iff so is the set of labels $\varrho(X) := \{\varrho(a) \mid a \in X\}$, i.e. $\varrho(a) \neq \overline{\varrho(b)}$ holds for all $a \neq b \in X$. For any consistent cut X in \mathcal{T} , let $\varrho^p(X)$ be the set of all positive literals occurring in $\varrho(X)$. Denote by $\mathcal{S}_{\mathcal{T}}$ ($\mathcal{S}_{\mathcal{T}}^c$) the set of all (consistent) cuts in \mathcal{T} ; clearly $\mathcal{S}_{\mathcal{T}}, \mathcal{S}_{\mathcal{T}}^c \subset \wp(L_{\mathcal{T}})$.

Lemma 14 For any PNF f , a tree and a circuit of f are both uniquely determined (mod branching permutation) and in the sequel denoted by $\mathcal{T}(f)$ and $\mathcal{C}(f)$, respectively; the natural numbers $\#(\mathcal{T}(f))$ and $\#(\mathcal{C}(f))$ are also called the tree- and circuit size of f , respectively. Moreover $\#(\mathcal{C}(f)) \leq \#(\mathcal{T}(f))$ and $\#(f) \leq \#(\mathcal{T}(f)) \leq 2 \cdot \#(f)$.

Proof. Straightforward. ■

Lemma 15 There is a conversion PNF $\ni f \mapsto f^M \in \text{PNF}$ such that $f \sim f^M$ and $\#(\mathcal{T}(f^M)) \leq \#(\mathcal{C}(f))$.

Proof. Argue by induction on $\#(\mathcal{T}(f))$ using familiar conversions corresponding to basic boolean absorption and distributive laws $A \vee A = A$, $A \wedge A = A$, $A \vee (A \wedge B) = A$, $A \wedge (A \vee B) = A$, $(A \vee B) \wedge (A \vee C) = A \vee (B \wedge C)$, $(A \wedge B) \vee (A \wedge C) = A \wedge (B \vee C)$, etc. ■

Lemma 16 For any given PNF f , let $\mathcal{T} := \mathcal{T}(f)$. Then the following hold:

1. $\text{EXPAND}(f) \sim \bigvee \{ \bigwedge \{ \ell \mid \ell \in \varrho(X) \} \mid X \in \mathcal{S}_{\mathcal{T}} \}$
2. $\text{EXPANDC}(f) \sim \bigvee \{ \bigwedge \{ \ell \mid \ell \in \varrho(X) \} \mid X \in \mathcal{S}_{\mathcal{T}}^c \}$
3. $\text{EXPANDCP}(f) \sim \bigvee \{ \bigwedge \{ \mathbf{v}_i \mid \mathbf{v}_i \in \varrho^p(X) \} \mid X \in \mathcal{S}_{\mathcal{T}}^c \} \approx \text{BASE}(f)$

Proof. Straightforward. ■

2.1.4 Complexity of conversions

In the sequel we distinguish between:

1. Turing complexity: standard time-complexity
2. Size complexity: output size in relation to input size

Remark 17 By Lemmata 14, 15, the difference between algebraic-, tree- a/o circuit size complexity is irrelevant to our polynomial vs. exponential approach in general.

Theorem 18 Working in \mathbb{B}^n [2], PNF conversion has polynomial Turing size complexity, whereas DNF, CNF and PB conversions have (in worst case) exponential size complexity, and hence also exponential Turing complexity.

Proof. The former is obvious. As for the latter, it will suffice to show that PB conversion has (in worst case) exponential size complexity in strictly positive polynomial domain. So by Theorem 1, it will suffice to find an infinite sequence of strictly positive polynomials f_k such that the length of $\text{BASE}(f_k)$ is exponential in the length of f_k . Now clearly this is the case of CNF $f_k := \bigwedge_{i=1}^k (x_{2i-1} \vee x_{2i})$ for distinct x_1, \dots, x_{2k} , since $\#(f_k) = O(k)$ and $\#(\text{BASE}(f_k)) = O(2^k)$. ■

Theorem 19 Working in \mathbb{B}^n [2], let 1 abbreviate a fixed polynomial $\mathbf{v}_1 \vee \overline{\mathbf{v}_1}$. Now $\mathcal{NP} = \mathcal{P}$ iff there exists an algorithm $\text{DNF} \ni f \mapsto f^* \in \text{CNF}$ of polynomial Turing complexity, such that $f \sim 1 \leftrightarrow f^* \sim 1$.

Proof. It is well known that the validity problem $g \sim 1$ for any given CNF g is decidable in polynomial time. Hence the existence of an algorithm in question would also imply a polynomial-time decidability of the validity problem $f \sim 1$ for any given DNF f , which by Cook theorem is equivalent to $\mathcal{NP} = \mathcal{P}$. To prove the other implication, suppose that $\mathcal{NP} = \mathcal{P}$ holds and let $f^* := \begin{cases} 1 & \text{if } f \sim 1 \\ 0 & \text{else} \end{cases}$, where $0 := \mathbf{v}_1 \wedge \overline{\mathbf{v}_1}$. ■

Remark 20 Working in \mathbb{B}^n [2], by Theorem 18 and standard duality argument, no conversion $\text{DNF} \ni f \mapsto f^* \in \text{CNF}$ satisfying $f \sim f^*$ can have polynomial Turing complexity. Hence semantic equivalence $f \sim 1 \leftrightarrow f^* \sim 1$ used in Theorem 19 is essentially weaker than $f \sim f^*$, whereas the latter admits purely algebraic interpretation by familiar methods of Boolean algebra. This is to say that Theorem 18 is too weak to provide us with deep insights into the nature of \mathcal{P} vs. \mathcal{NP} problem. The crucial difference between semantic and algebraic interpretations in question is that the former is just as abstract as \mathcal{P} vs. \mathcal{NP} itself, while the latter being a classical elementary algebraic question whose solvability by elementary mathematical (actually combinatorial) means is, in principle, beyond any doubt. However, instead of dealing with size complexity of normal form conversions, we'll investigate a reverse question:

Q: How big must be a basic polynomial f whose base, $\text{BASE}(f)$, is isomorphic to a given “big” and “complex” PB g ?

It turns out that Q is closely related to the \mathcal{P} vs. \mathcal{NP} problem, provided that we extend our multidimensional Boolean space to a multidimensional regular Borel real space that is discussed below. In that Borel space, all boolean DNF are representable by one universal PB that can serve as a “big” and “complex” g in question. Moreover, basic boolean properties exposed in Section 2.1.2 (see above) can be confirmed, by geometric arguments, also in the Borel space.

2.2 n^2 -dim regular Borel space

2.2.1 Preliminaries

1. In the sequel we let $n > 1$ and $\mathbf{n} := \{1, \dots, n\}$. For any $i, j \in \mathbf{n}$ we set $(i, j) := n(i-1) + j$ and identify $\mathbf{n}^2 = \{(i, j) \mid i, j \in \mathbf{n}\}$ with $\mathbf{n}^2 = \{1, \dots, n^2\}$
2. Let $\mathbb{Z}_{|n|} := \{\pm 1, \dots, \pm n\} \subset \mathbb{Z}_0 = \mathbb{Z} - \{0\}$ and $\mathbb{Z}_{|n|}^k := (\mathbb{Z}_{|n|})^k \subset \mathbb{Z}_0^k$
3. Let $\mathbf{n}^{2 \times 2} := \{\langle (i, j), (k, l) \rangle \mid i, j, k, l \in \mathbf{n} \wedge j \neq l\}$; so $\#(\mathbf{n}^{2 \times 2}) = n^3(n-1)$

4. For any $X \subset \mathbf{n}^{2 \times 2}$ let $X^+ \subset \mathbf{n}^{2 \times 2}$ be the minimal closure of X satisfying the following four conditions:

- (a) $X \subset X^+$
- (b) if $\langle u, v \rangle \in X^+$ then $\langle v, u \rangle \in X^+$
- (c) if $\{\langle u, v \rangle, \langle v, w \rangle, \langle w, z \rangle\} \subset X^+$ and $\langle u, z \rangle \in \mathbf{n}^{2 \times 2}$, then $\langle u, z \rangle \in X^+$
- (d) if $\{\langle u, v \rangle, \langle v, w \rangle, \langle w, u \rangle\} \subset X^+$ then $X^+ := \mathbf{n}^{2 \times 2}$

$X \subset \mathbf{n}^{2 \times 2}$ is called *basic* iff $X = X^+$. A basic $X \subsetneq \mathbf{n}^{2 \times 2}$ is called *truly basic*.

2.2.2 Space description

Designation: $\mathbb{B}^{n^2} [\mathbb{R}_0]$

Structure:

1. Vocabulary:
 - (a) Variables $\mathbf{v}_1, \dots, \mathbf{v}_{n^2}$ (abbr.: x, y, z, w - possibly indexed)
 - (b) Binary operations \vee, \wedge and unary operation $\bar{}$
 - (c) Binary relation J
2. Literals: terms xJy and $x\bar{J}y$ (abbr.: ℓ - possibly indexed); since J is symmetric (see 5 below), we often identify these terms with yJx and $y\bar{J}x$, respectively.
3. Basic (truly basic) clauses: terms $\bigwedge_{i=1}^s \mathbf{v}_{u_i} J \mathbf{v}_{v_i}$ for basic (truly basic) sets $\{\langle u_i, v_i \rangle \mid i = 1, \dots, s\} \subset \mathbf{n}^{2 \times 2}$
4. Polynomials, also called *regular Borel polynomials* (abbr.: f, g, h - possibly indexed):
 - (a) Arbitrary polynomials: arbitrary terms of the language
 - (b) Strictly positive polynomials: $(\bar{})$ -free polynomials
 - (c) Basic polynomials: polynomials which are semi-equivalent to positive bases PB (see e (iv) and 6 (a) below)
 - (d) Truly basic polynomials: polynomials which are semi-equivalent to proper positive bases PPB (see (e) v and 6 (a) below)
 - (e) Normal forms:
 - i. PNF (*positive normal form*): polynomials built up from literals by \vee and \wedge
 - ii. DNF (*disjunctive normal form*): polynomials in Σ_2 -form $\bigvee_{i=1}^k \bigwedge_{j=1}^{s_i} \ell_{i,j}$

iii. CNF (*conjunctive normal form*): polynomials in dual Π_2 -form

$$\bigwedge_{i=1}^k \bigvee_{j=1}^{s_i} \ell_{i,j}$$

iv. PB (*positive base*): DNF $\bigvee_{i=1}^k \bigwedge_{j=1}^{s_i} x_{i,j} J y_{i,j}$ such that:

A. for every $i = 1, \dots, k$, $\bigwedge_{j=1}^{s_i} x_{i,j} J y_{i,j}$ is a basic clause

B. for any $1 \leq q < r \leq k$, the lists of unordered pairs

$$X_q := [\{x_{q,j}, y_{q,j}\} \mid j = 1, \dots, s_q]$$

$$X_r := [\{x_{r,j}, y_{r,j}\} \mid j = 1, \dots, s_r]$$

are sets which are mutually incomparable with respect to \subset ,

i.e. $X_q \not\subseteq X_r \not\subseteq X_q$

v. PPB (*proper positive base*): PB $\bigvee_{i=1}^k \bigwedge_{j=1}^{s_i} x_{i,j} J y_{i,j}$ whose every

clause $\bigwedge_{j=1}^{s_i} x_{i,j} J y_{i,j}$, $i = 1, \dots, k$, is truly basic

vi. For any PB $f = \bigvee_{i=1}^k \bigwedge_{j=1}^{s_i} x_{i,j} J y_{i,j}$ we set

$$\text{VSet}(f) = \{\{x_{i,j}, y_{i,j}\} \mid j = 1, \dots, s_i\} \mid i = 1, \dots, k\}$$

5. Evaluations $\text{Val}(f)$ in $\{0, 1\}$: as in boolean algebra via

$$\text{Val}(xJy) := \begin{cases} 1 & \text{if } \text{Val}(x) + \text{Val}(y) = 0 \\ 0 & \text{else} \end{cases}$$

for $\text{Val}(x), \text{Val}(y)$ ranging over $\mathbb{R}_0 := \mathbb{R} - \{0\}$

6. Equality:

(a) f and g are *semi-equivalent* (abbr.: $f \sim_0 g$), iff they have the same boolean values $\text{Val}(f) = \text{Val}(g)$, for all variable evaluations in \mathbb{R}_0

(b) Two PB $f = \bigvee_{i=1}^k \bigwedge_{j=1}^{s_i} x_{i,j} J y_{i,j}$ and $g = \bigvee_{i=1}^l \bigwedge_{j=1}^{t_i} x'_{i,j} J y'_{i,j}$ are *isomorphic* (abbr.: $f \approx g$) iff $k = l$ and $\text{VSet}(f) = \text{VSet}(g)$

7. The *size* of f , $\#(f)$, is the number of all operation occurrences in f

Definition 21 Working in $\mathbb{B}^{n^2}[\mathbb{R}_0]$, for any polynomial f and vector $\vec{u} \in \mathbb{R}_0^{n^2}$, we let $f(\vec{u}) := \text{Val}(f)$ for $\text{Val}(\mathbf{v}_i) := u_i$, $i = 1, \dots, n^2$. Furthermore, we call $\text{Set}(f) := \{\vec{u} \in \mathbb{R}_0^{n^2} \mid f(\vec{u}) = 1\} \subset \mathbb{R}_0^{n^2}$ a n^2 -dim regular Borel set generated by f . $\text{Set}(f)$ is called *basic* (truly basic) iff so is f .

2.2.3 Basic properties

Theorem 22 *The following hold in $\mathbb{B}^{n^2}[\mathbb{R}_0]$:*

1. *Every polynomial has a semi-equivalent PNF*
2. *Every polynomial has a semi-equivalent DNF (CNF).*
3. *Every basic (truly basic) polynomial has a semi-equivalent PB (PPB)*
4. *For any PB f and g , if $f \sim_0 g$ then $f \approx g$*
5. *Every basic (truly basic) polynomial f has the unique (mod \approx) isomorphic PB (PPB), which is called the base of f*

Proof. Argue as in Theorem 7 (see above); however, clause 4 follows by less obvious geometrical considerations (see Appendix below and [G04]). Moreover, we can just as well adopt $\mathbb{B}^n[\mathbf{2}]$ the algorithm EXPANDC (see above Example 8). However, EXPAND, EXPANDCP and BASE have to be slightly modified (this will be elaborated in the next section, see Definition 30 and Lemma 31 below). ■

Corollary 23 *Every $n^2 - \dim$ basic (truly basic) regular Borel set has the uniquely (mod index permutation) determined PB (PPB) Σ_2 -form*

$$\bigcup_{i=1}^k \bigcap_{j=1}^{s_i} \left\{ \vec{x} \in \mathbb{R}_0^{n^2} \mid x_{i,j} + x_{i,j} = 0 \right\}$$

Definition 24 *Denote by \mathbb{M}_n (in words: boolean DNF $n \times n$ -matrix) the set of all boolean DNF $\bigvee_{i=1}^n \bigwedge_{j=1}^n \ell_{i,j}$, in $\mathbb{B}^n[\mathbf{2}]$.*

Lemma 25 *In $\mathbb{B}^{n^2}[\mathbb{R}_0]$, there exists a fixed basic, strictly positive CNF Φ_n and a bijective embedding $\phi : \mathbb{M}_n \rightarrow \mathbb{Z}_{|n^2|}^{n^2}$ such that for every $f \in \mathbb{M}_n$, $f \sim 1 \leftrightarrow \Phi_n(\phi(f)) = 1$. Moreover, if $n > 2$ then Φ_n is truly basic.*

Proof. For any $f = \bigvee_{i=1}^n \bigwedge_{j=1}^n \ell_{i,j}$, let $\Phi_n := \bigwedge_{\varphi: \mathbf{n} \rightarrow \mathbf{n}} \bigvee_{i < j \in \mathbf{n}} \mathbf{v}_{(\varphi(i),i)} \cdot \mathbf{J} \mathbf{v}_{(\varphi(j),j)}$ and $\phi(f) := (z_{(i,j)})_{i,j \in \mathbf{n}} \in \mathbb{Z}_{|n^2|}^{n^2}$ for $z_{(i,j)} := \begin{cases} k & \text{if } \ell_{i,j} = \mathbf{v}_k \\ -k & \text{if } \ell_{i,j} = \overline{\mathbf{v}_k} \end{cases}$. Note that $\text{Set}(\Phi_n)$ is in the Π_2 -form $\bigcap_{\varphi: \mathbf{n} \rightarrow \mathbf{n}} \bigcup_{i < j \in \mathbf{n}} \left\{ \vec{x} \in \mathbb{R}_0^{n^2} \mid x_{\varphi(i),i} + x_{\varphi(j),j} = 0 \right\}$. Obviously Φ_n is strictly positive and basic CNF. That it is truly basic for all $n > 2$ will be shown later (see Section 3.2 below). ■

Remark 26 *The lemma shows that the whole $n - \dim$ boolean family \mathbb{M}_n is representable by one universal $n^2 - \dim$ truly basic Borel CNF Φ_n and/or the corresponding $n^2 - \dim$ truly basic regular Borel set $\text{Set}(\Phi_n)$. Moreover, the proof of the lemma shows that the validity problem for \mathbb{M}_n is reducible to the evaluation of Φ_n in $\mathbb{Z}_{|n^2|}^{n^2}$ by an algorithm whose Turing complexity is polynomial in n . Note that the circuit size of Φ_n is exponential in n .*

Theorem 27 $\mathcal{NP} \subset \mathcal{P}/poly$ holds iff there exists $c \in \mathbb{N}$ such that for infinitely many $n \in \mathbb{N}$ there exists a n^2 -dim Borel polynomial $f \sim_0 \Phi_n$, in $\mathbb{B}^{n^2}[\mathbb{R}_0]$, whose algebraic size, $\#(f)$, does not exceed n^c . Hence the right-hand side condition is necessary for the conjecture $\mathcal{P} = \mathcal{NP}$.

Proof. Sufficiency easily follows from previous remark. The necessity proof is more involved. To this end we first define a suitable mapping

$$\mathbb{R}_0^{n^2} \ni \vec{x} = (x_1, \dots, x_{n^2}) \mapsto (z_1, \dots, z_{n^2}) = \vec{z} \in \mathbb{Z}_{|n^2|}^{n^2}$$

such for any $1 \leq i \leq j \leq n^2$, $x_i + x_j = 0 \leftrightarrow z_i + z_j = 0$, and every projection $\vec{x} \mapsto z_i =: g_i(\vec{x})$ is representable in $\mathbb{B}^{n^2}[\mathbb{R}_0]$ by some g_i of polynomial circuit-size complexity. Note that by definition we have $\Phi_n(\vec{x}) = \Phi_n(\vec{z})$. Now by Remark 26, $\mathcal{NP} \subset \mathcal{P}/poly$ infers that $\Phi_n(\vec{z})$ is computable in a standard language $L \subset \{0, 1\}^*$ by a circuit \mathcal{C}_0 whose size is polynomial in n . Substituting $g_i(\vec{x})$ for each z_i we can choose a suitable constant c and extend \mathcal{C}_0 to an enriched circuit \mathcal{C} computing $\Phi_n(\vec{x})$, whose sources are labeled by the corresponding relations $x_i J x_j$ or $x_i \bar{J} z_j$ and whose circuit size does not exceed n^c . The correlated PNF $f_{\mathcal{C}}$ is a Borel polynomial in $\mathbb{B}^{n^2}[\mathbb{R}_0]$ satisfying $f_{\mathcal{C}} \sim_0 \Phi_n$, whose circuit size does not exceed n^c . By an obvious $\mathbb{B}^{n^2}[\mathbb{R}_0]$ -specification of Lemma 15, we can switch to a desired Borel polynomial $f := f_{\mathcal{C}}^M \sim_0 f$ satisfying $\#(f) \leq n^c$, Q.E.D. [This proof idea is due to A. Krebs - it simplifies our previous considerations (see [G04], [GK]) thus showing that the regular Borel space in question covers $\mathcal{NP} \subset \mathcal{P}/poly$.] ■

Remark 28 The theorem provides us with general conception of a desired mathematical proof of the conjecture $\mathcal{P} < \mathcal{NP}$. Namely, let S be a sentence stating that for every $c \in \mathbb{N}$ and a sufficiently large $n \in \mathbb{N}$, the (algebraic) size of any n^2 -dim truly basic Borel PNF that is semi-equivalent to Φ_n must be bigger than n^c . Since S is a negation of the necessary condition for $\mathcal{P} = \mathcal{NP}$ in question, it follows that S is sufficient for $\mathcal{P} < \mathcal{NP}$. S is **not** a familiar lower bound problem - rather, it says that the set of all valid n -dim boolean DNF is not measurable by n^2 -dim Borel polynomials whose size is polynomial in n .

3 Elementary interpretations

3.1 Background

We wish to reduce the conjecture $\mathcal{P} < \mathcal{NP}$ to a suitable Borel modification, \mathcal{Q}_0 , of the question \mathcal{Q} posed in Remark 20 (see above). To this end, we first specify the corresponding Borel modification, BASE_0 , of the boolean algorithm BASE exposed above in Theorem 7 and Example 8.

Definition 29 Let EXPAND be the conversion exposed in Example 8 producing a DNF of any given Borel polynomial (obviously, it is not influenced by the shape of literals). In particular, for any basic (truly basic) PNF f we have

$$f \sim_0 \text{EXPAND}(f) = \bigvee_{i=1}^k \left(\bigwedge_{j=1}^{s_i} x_{i,j} J y_{i,j} \wedge \bigwedge_{j=1}^{t_i} z_{i,j} \bar{J} w_{i,j} \right)$$

In order to obtain a semi-equivalent PB (PPB) of f , we proceed as follows.

1. Consider $\text{EXPAND}(f)$, as above, where $x_{i,j} = \mathbf{v}_{u_{i,j}}$ and $y_{i,j} = \mathbf{v}_{v_{i,j}}$. For every $i = 1, \dots, k$, let $X_i := \{\langle u_{i,j}, v_{i,j} \rangle \mid j = 1, \dots, s_i\} \subset \mathbf{n}^{2 \times 2}$ and consider the closure $X_i^+ = \{\langle u'_{i,j}, v'_{i,j} \rangle \mid j = 1, \dots, s'_i\} \subset \mathbf{n}^{2 \times 2}$. Furthermore, replace each $\bigwedge_{j=1}^{s_i} x_{i,j} J y_{i,j}$ by the corresponding basic clause $\bigwedge_{j=1}^{s'_i} x'_{i,j} J y'_{i,j}$, where $x'_{i,j} := \mathbf{v}_{u'_{i,j}}$, $y'_{i,j} := \mathbf{v}_{v'_{i,j}}$. Denote by $\text{EXPANDB}(f)$ the resulting output $\bigvee_{i=1}^k \left(\bigwedge_{j=1}^{s'_i} x'_{i,j} J y'_{i,j} \wedge \bigwedge_{j=1}^{t_i} z_{i,j} \bar{J} w_{i,j} \right)$
2. Upgrade EXPANDB to EXPANDBC by deleting in $\text{EXPANDB}(f)$, as above, all inconsistent clauses $\bigwedge_{j=1}^{s'_i} x'_{i,j} J y'_{i,j} \wedge \bigwedge_{j=1}^{t_i} z_{i,j} \bar{J} w_{i,j}$, i.e. such that the corresponding sets of unordered pairs of variables $\{x'_{i,j}, y'_{i,j} \mid j = 1, \dots, s'_i\}$ and $\{z_{i,j}, w_{i,j} \mid j = 1, \dots, t_j\}$ have nonempty intersection. Let $\text{EXPANDBC}(f)$ be the output $\bigvee_{i=1}^{k'} \left(\bigwedge_{j=1}^{s'_i} x'_{i,j} J y'_{i,j} \wedge \bigwedge_{j=1}^{t_i} z_{i,j} \bar{J} w_{i,j} \right)$
3. Upgrade EXPANDBC to EXPANDBCP by deleting in $\text{EXPANDBC}(f)$, as above, all negative literals $z_{i,j} \bar{J} w_{i,j}$. Denote by $\text{EXPANDBCP}(f)$ the output $\bigvee_{i=1}^{k'} \bigwedge_{j=1}^{s'_i} x'_{i,j} J y'_{i,j}$
4. The required PB of f , $\text{BASE}_0(f)$, is obtained as in the boolean case by deleting all repetitions and all but minimal conjunctions $\bigwedge_{j=1}^{s'_i} x'_{i,j} J y'_{i,j}$ in $\text{EXPANDBCP}(f)$.
5. Now if f is truly basic, then $\text{EXPANDB}(f)$ can be further simplified by deleting from $\text{EXPAND}(f)$ all clauses $\bigwedge_{j=1}^{s_i} x_{i,j} J y_{i,j}$ for which $X_i^+ = \mathbf{n}^{2 \times 2}$. Having this done and stipulating $\text{EXPANDBCP}(f)$ and $\text{BASE}_0(f)$ as above we conclude that $\text{BASE}_0(f)$ is in fact the PPB of f .

Lemma 30 Working in $\mathbb{B}^{n^2}[\mathbb{R}_0]$, for any basic (truly basic) PNF f and g we have:

1. $\text{BASE}_0(f)$ is a PB (PPB)
2. $f \sim_0 \text{EXPAND}(f) \sim_0 \text{EXPANDB}(f) \sim_0 \text{EXPANDBCP}(f) \sim_0 \text{EXPANDCPB}(f) \sim_0 \text{BASE}_0(f)$
3. $f \sim_0 g$ infers $\text{BASE}_0(f) \approx \text{BASE}_0(g)$ and hence also $\text{VSet}(\text{BASE}_0(f)) = \text{VSet}(\text{BASE}_0(g))$

4. BASE_0 has (in worst case) exponential size complexity, and hence also exponential Turing complexity. In particular, $\#(\text{BASE}_0(\Phi_n))$ is exponential in $\#(\Phi_n)$, while $\#(\Phi_n)$ is exponential in n .

Proof. See Lemma 9, Theorem 22 above and Appendix below that summarizes geometric arguments used. ■

By Remark 29, in order to prove $\mathcal{P} < \mathcal{NP}$, it will suffice to prove

Condition 31 C : “for every $c \in \mathbb{N}$ there is a $n \in \mathbb{N}$ so large that the size of any truly basic Borel PNF, in $\mathbb{B}^{n^2}[\mathbb{R}_0]$, that is semi-equivalent to Φ_n , is bigger than n^c ”.

For the sake of brevity we also consider a weaker

Condition 32 C^p : “for every $c \in \mathbb{N}$ there is a $n \in \mathbb{N}$ so large that the size of any truly basic strictly positive Borel PNF, in $\mathbb{B}^{n^2}[\mathbb{R}_0]$, that is semi-equivalent to Φ_n , is bigger than n^c ”.

that infers the corresponding weak positive variant of $\mathcal{P} < \mathcal{NP}$. Our next goal is to present C (C^p) in a more convenient elementary-algebraic form; this can be done via conversion BASE_0 . Denote $\text{VSet}(\text{BASE}_0(\Phi_n))$ by Ω_n . The corresponding specification of our boolean question Q (see Remark 20 above) reads

Q_0 (Q_0^p) : How big must be a truly basic Borel PNF f , in $\mathbb{B}^{n^2}[\mathbb{R}_0]$, whose base, $\text{BASE}_0(f)$, is isomorphic to $\text{BASE}_0(\Phi_n)$, and hence $\text{VSet}(\text{BASE}_0(f)) = \Omega_n$?

Definition 33 Let C_0 (C_0^p) abbreviate “for every $c \in \mathbb{N}$ there is a $n \in \mathbb{N}$ so large that the size of any truly basic (strictly positive) Borel PNF f , in $\mathbb{B}^{n^2}[\mathbb{R}_0]$, satisfying $\text{BASE}_0(f) \approx \text{BASE}_0(\Phi_n)$ is bigger than n^c ”. Moreover, we can just as well replace the condition $\text{BASE}_0(f) \approx \text{BASE}_0(\Phi_n)$ by $\text{VSet}(\text{BASE}_0(f)) = \Omega_n$.

By Lemma 31, we arrive at

Theorem 34 C_0 (C_0^p) infers C (C^p). Hence C_0 infers $\mathcal{P} < \mathcal{NP}$.

3.2 Description of Ω_n

3.2.1 Recursive definition

Let $n > 1$ and $\mathbf{n}^{2*2} := \{\{u, v\} \mid \langle u, v \rangle \in \mathbf{n}^{2 \times 2}\}$. Note that $\#(\mathbf{n}^{2*2}) = \frac{1}{2}n^3(n-1)$

For any pair of sets U, V , let $U \otimes V := \{u, v \mid u \in U \wedge v \in V\}$. Moreover, denote by $[U \curvearrowright V]$ the set of all partial functions from U to V . For any $1 \leq m \leq n-1$ we define a suitable set $M_n^m \subseteq [\mathbf{n}^2 \curvearrowright \{\pm 1, \dots, \pm m\}]$ and then let

$M_n := \bigcup_{m=1}^{n-1} M_n^m$ and $\widetilde{M}_n := \{f \in M_n \mid (\forall y \in \text{Dom}_2(f)) \text{Dom}_1(f, y) = \mathbf{n}\}$ where

$\text{Dom}_1(f, y) := \{x \mid (\exists z) f(x, y) = z\}$, $\text{Dom}_2(f) := \{y \mid (\exists x \exists z) f(x, y) = z\}$.

Having this done we set $\Omega_n := \{\{\langle i, j \rangle, \langle k, l \rangle\} \in \mathbf{n}^{2*2} \mid f(i, j) + f(k, l) = 0\}_{f \in \widetilde{M}_n}$.

Back to our recursive definition, let M_n^m arise by the following recursive clauses, where $\phi_{U,y,s} : U \times \{y\} \rightarrow \{s\}$ and $\phi_{U-f,y,s} : (U - \text{Dom}_1(f, y)) \times \{y\} \rightarrow \{s\}$

Basis.

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

Induction step. Let $1 < m < n$. Consider two cases ($\partial = \emptyset$ is admissible).

1. Let $\partial \cup f \in M_n^{m-1}$, $j \in \mathbf{n}$, and $\{X_y\}_{y \in \text{Dom}_2(f)}$ for $\emptyset \neq X_y \subset \mathbf{n}$ be such that:

- (a) $\text{Dom}_2(\partial) \cap \text{Dom}_2(f) = \emptyset$
- (b) $j \notin \text{Dom}_2(\partial \cup f)$
- (c) $(\forall y \in \text{Dom}_2(f)) (\text{Dom}_1(f, y) \subsetneq X_y)$

Then set $f' := \partial \cup f \cup \bigcup_{y \in \text{Dom}_2(f)} \phi_{X_y^{-f}, y, m}$

2. Let $\partial \cup f, \partial \cup g \in M_n^{m-1}$ and $\{X_y\}_{y \in \text{Dom}_2(f)}, \{Y_z\}_{z \in \text{Dom}_2(g)}$ for $\emptyset \neq X_y \subset \mathbf{n}$ and $\emptyset \neq Y_z \subset \mathbf{n}$ be such that:

- (a) $\text{Dom}_2(f) \cap \text{Dom}_2(g) = \text{Dom}_2(\partial) \cap \text{Dom}_2(f)$
 $= \text{Dom}_2(\partial) \cap \text{Dom}_2(g) = \emptyset$
- (b) $(\forall y \in \text{Dom}_2(f)) (\text{Dom}_1(f, y) \subsetneq X_y)$
- (c) $(\forall z \in \text{Dom}_2(g)) (\text{Dom}_1(g, z) \subsetneq Y_z)$.

Then set $f' := \partial \cup f \cup g \cup \bigcup_{y \in \text{Dom}_2(f)} \phi_{X_y^{-f}, y, m} \cup \bigcup_{z \in \text{Dom}_2(g)} \phi_{Y_z^{-g}, z, -m}$.

Let M_n^m extend M_n^{m-1} by adjoining all functions f' obtained by 1-2. This completes our recursive definition of Ω_3 . (The corresponding correctness proof will be presented elsewhere.) Below we briefly illustrate the simplest

3.2.2 Cases Ω_2 and Ω_3

- Ω_2 : Clearly M_2 contains two mutually isomorphic (2×2) -matrices:

$$\begin{pmatrix} 1 & -1 \\ 1 & -1 \end{pmatrix} \text{ and } \begin{pmatrix} -1 & 1 \\ -1 & 1 \end{pmatrix}$$

and hence

$$\Omega_2 = \{\langle 1, 1 \rangle, \langle 1, 2 \rangle\}, \{\langle 1, 1 \rangle, \langle 2, 2 \rangle\}, \{\langle 2, 1 \rangle, \langle 1, 2 \rangle\}, \{\langle 2, 1 \rangle, \langle 2, 2 \rangle\} = \mathbf{2}^{2 \times 2}$$

- Ω_3 : M_3 contains all matrices of the following types (mod row/column permutation):

$$\begin{bmatrix} 1 & -1 \end{bmatrix}, \begin{bmatrix} 1 & 2 & -1 \\ & & -2 \end{bmatrix}, \begin{bmatrix} 1 & -1 & -1 \\ & 2 & -2 \end{bmatrix}$$

That is, every (3×3) -matrix from M_3 is obtained from a chosen type from the above list by completing every column using the labels exposed and, if necessary, adding the empty column (this applies to the first type only). For example,

$$\begin{pmatrix} 1 & \emptyset & -1 \\ 1 & \emptyset & -1 \\ 1 & \emptyset & -1 \end{pmatrix} \text{ and } \begin{pmatrix} -1 & 1 & -2 \\ -1 & 1 & -1 \\ 2 & 1 & -2 \end{pmatrix}$$

are matrices of the first and third type, respectively, which yield the following two elements of Ω_3 :

$$\begin{aligned} & \{\langle 1, 1 \rangle, \langle 1, 3 \rangle\}, \{\langle 1, 1 \rangle, \langle 2, 3 \rangle\}, \{\langle 1, 1 \rangle, \langle 3, 3 \rangle\}, \\ & \quad \{\langle 2, 1 \rangle, \langle 1, 3 \rangle\}, \{\langle 2, 1 \rangle, \langle 2, 3 \rangle\}, \{\langle 2, 1 \rangle, \langle 3, 3 \rangle\}, \\ & \quad \{\langle 3, 1 \rangle, \langle 1, 3 \rangle\}, \{\langle 3, 1 \rangle, \langle 2, 3 \rangle\}, \{\langle 3, 1 \rangle, \langle 3, 3 \rangle\} \\ & \{\langle 1, 1 \rangle, \langle 1, 2 \rangle\}, \{\langle 1, 1 \rangle, \langle 2, 2 \rangle\}, \{\langle 1, 1 \rangle, \langle 3, 2 \rangle\}, \\ & \quad \{\langle 2, 1 \rangle, \langle 1, 2 \rangle\}, \{\langle 2, 1 \rangle, \langle 2, 2 \rangle\}, \{\langle 2, 1 \rangle, \langle 3, 2 \rangle\}, \\ & \quad \{\langle 3, 1 \rangle, \langle 1, 3 \rangle\}, \{\langle 3, 1 \rangle, \langle 3, 3 \rangle\} \\ & \quad \{\langle 1, 2 \rangle, \langle 2, 3 \rangle\}, \{\langle 2, 2 \rangle, \langle 2, 3 \rangle\}, \{\langle 3, 2 \rangle, \langle 2, 3 \rangle\} \end{aligned}$$

All in all M_3 contains 129 distinct (mod row/column permutation) matrices, and hence Ω_3 has 129 elements all of which are distinct from $\mathbf{3}^{2*2}$ (see also [GMaple]). Hence Φ_3 is truly basic. By the same token, it is readily seen that Φ_n is truly basic for every $n > 2$.

3.3 Combinatorial interpretation of \mathbf{C}_0^p and \mathbf{C}_0

3.3.1 Basic notations

1. For any $X \subset \mathbf{n}^{2*2}$ let $X^+ \subset \mathbf{n}^{2*2}$ be the minimal closure of X satisfying the following conditions:
 - (a) $X \subset X^+$
 - (b) if $\{\{u, v\}, \{v, w\}, \{w, z\}\} \subset X^+$ and $\{u, z\} \in \mathbf{n}^{2*2}$, then $\{u, z\} \in X^+$
 - (c) if $\{\{u, v\}, \{v, w\}, \{w, u\}\} \subset X^+$ then $X^+ := \mathbf{n}^{2*2}$
2. Let $\mathbf{n}_+^{2*2} := \{0\} \cup \mathbf{n}^{2*2}$
3. For any $X, Y \subset \mathbf{n}_+^{2*2}$ let
$$X \circledast Y := \begin{cases} X & \text{if } X \cap Y = \emptyset \\ \emptyset & \text{else} \end{cases}$$
4. Let $\widehat{\Omega}_n := \{X \subset \mathbf{n}^{2*2} \mid (\exists Y \in \Omega_n)(Y \subset X)\}$

3.3.2 Borel trees

Working in Borel space $\mathbb{B}^{n^2}[\mathbb{R}_0]$ we adopt our previous tree interpretation of polynomials in boolean space $\mathbb{B}^n[\mathbf{2}]$ (see above Section 2.1.3). To this end, we label the sources by Borel literals $\mathbf{v}_u J \mathbf{v}_v$ ($\mathbf{v}_u \bar{J} \mathbf{v}_v$) instead of boolean literals \mathbf{v}_i ($\bar{\mathbf{v}}_i$). In fact, we can just as well replace literals $\mathbf{v}_u J \mathbf{v}_v$ ($\mathbf{v}_u \bar{J} \mathbf{v}_v$) by their numerical codes $\{u, v\} \in \mathbf{n}^{2*2}$. In order to separate numerical codes of positive and negative literals, we replace the ordinary literal labeling ϱ by the two source-labeling functions $\varrho_1, \varrho_2 : L_{\mathcal{T}} \rightarrow \mathbf{n}_+^{2*2}$ with the intended meaning

$$\begin{aligned} \varrho_1(\sigma) &:= \begin{cases} \{u, v\} & \text{if } \varrho(\sigma) = \mathbf{v}_u J \mathbf{v}_v \\ 0 & \text{else} \end{cases} \quad \text{and} \\ \varrho_2(\sigma) &:= \begin{cases} \{u, v\} & \text{if } \varrho(\sigma) = \mathbf{v}_u \bar{J} \mathbf{v}_v \\ 0 & \text{else} \end{cases}. \end{aligned}$$

Thus for every $a \in L_{\mathcal{T}}$, $\varrho_1(a) \neq 0 \Leftrightarrow \varrho_2(a) = 0$. Moreover, for any given cut X , we have $\varrho(X) = (\varrho_1(X) - \{0\}) \cup (\varrho_2(X) - \{0\})$. Furthermore, we set $\varrho^p(X) := (\varrho_1(X) - \{0\})^+$ and call X *consistent* iff $\varrho^p(X) \cap \varrho_2(X) = \emptyset$. Keeping these specifications in mind we adopt previous notations $\mathcal{S}_{\mathcal{T}}, \mathcal{S}_{\mathcal{T}}^c \subset \wp(L_{\mathcal{T}})$.

Having this done, it is obvious that Lemmata 14, 15 are also true of $\mathbb{B}^{n^2}[\mathbb{R}_0]$. Furthermore, analyzing Borel conversions of Definition 20 (see above) we can specify Lemma 16, as follows.

Lemma 35 *For any basic PNF f , in $\mathbb{B}^{n^2}[\mathbb{R}_0]$, let $\mathcal{T} := \mathcal{T}(f)$. Then the following hold:*

1. $\text{EXPANDB}(f) \sim_0 \bigvee \{ \bigwedge \{ \ell \mid \ell \in \varrho(X) \} \mid X \in \mathcal{S}_{\mathcal{T}} \}$
2. $\text{EXPANDBC}(f) \sim_0 \bigvee \{ \bigwedge \{ \ell \mid \ell \in \varrho(X) \} \mid X \in \mathcal{S}_{\mathcal{T}}^c \}$
3. $\text{EXPANDBCP}(f) \sim_0 \bigvee \{ \bigwedge \{ \mathbf{v}_u J \mathbf{v}_v \mid \mathbf{v}_u J \mathbf{v}_v \in \varrho^p(X) \} \mid X \in \mathcal{S}_{\mathcal{T}}^c \}$
4. $\text{VSet}(\text{EXPANDBCP}(f)) = \left\{ \{ \{u, v\} \mid \{u, v\} \in \varrho^p(X) \}^+ \mid X \in \mathcal{S}_{\mathcal{T}}^c \right\}$
5. *If $\text{VSet}(\text{BASE}_0(f)) = \Omega_n$ and $\text{VSet}(\text{EXPANDCPB}(f)) = B$, then*

$$\Omega_n \subset B \subset \widehat{\Omega}_n$$

Proof. Straightforward via Lemma 30. ■

3.3.3 Results

Definition 36 *For any tree \mathcal{T} enriched by a source-labeling function $\varrho : L_{\mathcal{T}} \rightarrow \mathbf{n}^{2*2}$, let*

$$\mathfrak{D}^1(\mathcal{T}) := \left\{ \varrho(X)^+ \mid X \in \mathcal{S}_{\mathcal{T}} \right\}$$

Theorem 37 *Condition C_0^p is derivable from the following combinatorial sentence (call it CS^p). For any enriched tree \mathcal{T} , as above, either $\Omega_n \not\subseteq \mathfrak{D}^1(\mathcal{T})$ or $\mathfrak{D}^1(\mathcal{T}) \not\subseteq \widehat{\Omega}_n$ holds true, provided that n is sufficiently large and $\#(\mathcal{T})$ merely polynomial in n .*

Proof. Straightforward via Lemma 35. ■

Definition 38 Let \mathcal{T} be a tree enriched by two source-labeling functions $\varrho_1, \varrho_2 : L_{\mathcal{T}} \rightarrow \mathbf{n}_+^{2*2}$ such that for every $a \in L_{\mathcal{T}}$, $\varrho_1(a) \neq 0 \Leftrightarrow \varrho_2(a) = 0$. Let

$$\varrho^2(\mathcal{T}) := \left\{ (\varrho_1(X) - \{0\})^+ \circ \varrho_2(X) \mid X \in \mathcal{S}_{\mathcal{T}} \right\} - \{\emptyset\}$$

Theorem 39 Condition C_0 , and hence also $\mathcal{P} < \mathcal{NP}$, is derivable from the following strengthening of \mathcal{CS}^p , which we call \mathcal{CS} . For any enriched tree \mathcal{T} , as above, either $\Omega_n \not\subseteq \varrho^2(\mathcal{T})$ or $\varrho^2(\mathcal{T}) \not\subseteq \widehat{\Omega}_n$ holds true, provided that n is sufficiently large and $\#(\mathcal{T})$ merely polynomial in n .

Proof. Straightforward via Theorem 34, Lemma 35 and the intended interpretation

$$\varrho_1(\sigma) := \begin{cases} \{u, v\} & \text{if } \varrho(\sigma) = \mathbf{v}_u J \mathbf{v}_v \text{ and} \\ 0 & \text{else} \end{cases}$$

$$\varrho_2(\sigma) := \begin{cases} \{u, v\} & \text{if } \varrho(\sigma) = \mathbf{v}_u \bar{J} \mathbf{v}_v \\ 0 & \text{else} \end{cases}$$

where $\varrho(\sigma)$ denotes the ordinary literal of a source $\sigma \in L_{\mathcal{T}}$. ■

Conclusion 40 According to the last theorem, the problem of proving $\mathcal{P} < \mathcal{NP}$ reduces to topological-combinatorial analysis of the sets Ω_n . Section 3.2 shows (see above) that Ω_n is exponentially large in size and structurally complex, in relation to n , provided that n is sufficiently large. It remains to separate and precisely formalize the topological-combinatorial properties of Ω_n which would infer the desired combinatorial requirement $\Omega_n \not\subseteq \varrho^2(\mathcal{T}) \vee \varrho^2(\mathcal{T}) \not\subseteq \widehat{\Omega}_n$ of \mathcal{CS} , for any n and \mathcal{T} in question (see above Theorem 39). Obviously, a weaker requirement $\Omega_n \not\subseteq \varrho^1(\mathcal{T})$ or $\varrho^1(\mathcal{T}) \not\subseteq \widehat{\Omega}_n$ of \mathcal{CS}^p (see Theorem 37) is technically easier; in the next section we indicate crucial arguments in its favor (the proof proper will be exposed elsewhere). The treatment of \mathcal{CS} is analogous, but technically more involved.

Summary 41 It is very likely that \mathcal{CS}^p and \mathcal{CS} are both provable by standard combinatorial arguments.

Corollary 42 It is verly likely that $\mathcal{P} = \mathcal{NP}$ is refutable by standard combinatorial arguments.

4 Basic combinatorics

For the sake of brevity we discuss more thoroughly the weaker positive condition C_0^p and the corresponding combinatorial sentence \mathcal{CS}^p . By the familiar logic pattern, we adopt standard classification $\{\Pi_1 \not\subseteq \Pi_2 \not\subseteq \dots \not\subseteq \Pi_k \not\subseteq \dots\}$ of trees whose roots are labeled by \wedge , and dual hierarchy $\{\Sigma_1 \not\subseteq \Sigma_2 \not\subseteq \dots \not\subseteq \Sigma_k \not\subseteq \dots\}$ of trees whose roots are labeled by \vee . Moreover, we regard arbitrary iterations

$x_1 \wedge \cdots \wedge x_k$ ($x_1 \vee \cdots \vee x_k$) as legitimate multi-dimensional variants of the canonical binary operations \wedge (\vee). Furthermore, we can just as well assume that all multi-dimensional occurrences of \wedge (\vee) in a given Π_k (Σ_k)-tree \mathcal{T} have the same dimension (= arity) $\sqrt[k]{\#(\mathcal{T})}$. Thus in particular, we assume that PNF $f_{\mathcal{T}}$ of Σ_2 -, Π_2 -, Σ_3 - and Π_3 -trees \mathcal{T} have the shape $\bigvee_{i=1}^m \bigwedge_{j=1}^m x_{i,j} J y_{i,j}$, $\bigwedge_{i=1}^m \bigvee_{j=1}^m x_{i,j} J y_{i,j}$, $\bigvee_{i=1}^m \bigwedge_{j=1}^m \bigvee_{k=1}^m x_{i,j,k} J y_{i,j,k}$ and $\bigwedge_{i=1}^m \bigvee_{j=1}^m \bigwedge_{k=1}^m x_{i,j,k} J y_{i,j,k}$, respectively. Hence the corresponding PNF $f_{\mathcal{T}}$ of Σ_2 -, Π_2 -, Σ_3 - and Π_3 -trees \mathcal{T} from Theorem 37 are in the corresponding forms $\bigvee_{i=1}^m \bigwedge_{j=1}^m \{u_{i,j}, v_{i,j}\}$, $\bigwedge_{i=1}^m \bigvee_{j=1}^m \{u_{i,j}, v_{i,j}\}$, $\bigvee_{i=1}^m \bigwedge_{j=1}^m \bigvee_{k=1}^m \{u_{i,j,k}, v_{i,j,k}\}$ and $\bigwedge_{i=1}^m \bigvee_{j=1}^m \bigwedge_{k=1}^m \{u_{i,j,k}, v_{i,j,k}\}$. Consider the corresponding Σ_2 -, Π_2 -, Σ_3 -, Π_3 - ... restrictions of the condition $\Omega_n \not\subseteq \mathfrak{D}^1(\mathcal{T}) \vee \mathfrak{D}^1(\mathcal{T}) \not\subseteq \widehat{\Omega}_n$ of CS^p .

4.1 CS^p -cases Σ_2 , Π_2

4.1.1 Case Σ_2

We have $f_{\mathcal{T}} = \bigvee_{i=1}^m \bigwedge_{j=1}^m \{u_{i,j}, v_{i,j}\}$, $\#(\mathcal{T}) = m^2$ being polynomial in n . Obviously, $\varrho_1(X)$ for $X \in \mathcal{S}_{\mathcal{T}}$ are the clauses $\{\{u_{i,j}, v_{i,j}\} \mid j = 1, \dots, m\}$, $i = 1, \dots, m$. Hence $\#(\mathfrak{D}^1(\mathcal{T})) \leq m < \#(\mathcal{T})$. Since $\#(\Omega_n)$ is exponential in n (see above Section 3.2.1), we arrive at $\Omega_n \not\subseteq \mathfrak{D}^1(\mathcal{T})$, provided that n is sufficiently large. Hence the corresponding condition of CS^p is fulfilled, Q.E.D.

4.1.2 Case Π_2

We have $f_{\mathcal{T}} = \bigwedge_{i=1}^m \bigvee_{j=1}^m \{u_{i,j}, v_{i,j}\}$, $n \gg 1$. Suppose $\Omega_n \subset \mathfrak{D}^1(\mathcal{T}) \subset \widehat{\Omega}_n$. We show that m is superpolynomial in n . Consider the corresponding $(m \times m)$ -matrix

$$\left(\begin{array}{ccccc} \vartheta_{1,1} & \vartheta_{2,1} & \cdots & \vartheta_{m-1,1} & \vartheta_{m,1} \\ \vartheta_{1,2} & \vartheta_{2,2} & \cdots & \vartheta_{m-1,2} & \vartheta_{m,2} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \vartheta_{1,m-1} & \vartheta_{2,m-1} & \cdots & \vartheta_{m-1,m-1} & \vartheta_{m,m-1} \\ \vartheta_{1,m} & \vartheta_{2,m} & \cdots & \vartheta_{m-1,m} & \vartheta_{m,m} \end{array} \right) \text{ where } \vartheta_{i,j} = \{u_{i,j}, v_{i,j}\}$$

Hence $\varrho_1(X)$ for $X \in \mathcal{S}_{\mathcal{T}}$ are elements $\tilde{\varphi} := \{\vartheta_{i,\varphi(i)} \mid i = 1, \dots, m\}$, where $\varphi : \mathbf{m} \rightarrow \mathbf{m}$, of Cartesian set-product $\bigotimes_{i=1}^m \{\vartheta_{i,j} \mid j = 1, \dots, m\}$. Thus $\mathfrak{D}^1(\mathcal{T}) = \{\tilde{\varphi}^+ \mid \varphi : \mathbf{m} \rightarrow \mathbf{m}\}$. Let $\Psi := \{\varphi : \mathbf{m} \rightarrow \mathbf{m} \mid \tilde{\varphi}^+ \in \Omega_n\}$ and $\tilde{\Psi} := \{\tilde{\varphi}^+ \mid \varphi \in \Psi\}$. Hence $\tilde{\Psi} = \Omega_n$, since $\Omega_n \subset \mathfrak{D}^1(\mathcal{T})$. Consider the subset $\Omega_n^1 \subset \Omega_n$ dealing with two-column matrices from M_n^1 (see above Section 3.2.1), i.e. $\Omega_n^1 = \{R_{k,l} \mid k < l \in \mathbf{n}\}$ for $R_{k,l} := (\mathbf{n} \times \{k\}) \otimes (\mathbf{n} \times \{l\})$. Since $\Omega_n^1 \subset \Omega_n = \tilde{\Psi}$, for every $k < l \in \mathbf{n}$ there is a $\varphi \in \Psi$ such that $\tilde{\varphi}^+ = R_{k,l}$. Note that for any $U \subset \mathbf{n}^{2 \times 2}$,

$R_{k,l} \subset U^+$ implies $\#(U) \geq 2n - 1$. Set $\Psi_{k,l} := \{\varphi : \mathbf{m} \rightarrow \mathbf{m} \mid \tilde{\varphi}^+ = R_{k,l}\}$. For any $r \in \mathbf{n}$, let $S_{k,l,r} := \{(r,k), (l,j)\} \mid j \in \mathbf{n}\}$; thus $R_{k,l} = \bigsqcup_{r=1}^n S_{k,l,r}$ and $R_{k,l} \not\supseteq (U - S_{k,l,r})^+$, provided that $R_{k,l} = U^+$. Now let $\varphi \in \Psi_{1,2}$; thus $m \geq \#(\tilde{\varphi}) \geq 2n - 1$. Consider any $\vartheta \in \tilde{\varphi}$ and the uniquely determined $r \in \mathbf{n}$ such that $\vartheta \in S_{1,2,r}$. Since $\tilde{\varphi} \subset R_{k,l}$, we have $(\tilde{\varphi} - S_{1,2,r})^+ \subset (R_{k,l} - S_{k,l,r})^+ \neq R_{1,2}$. Now take any $\psi \in \Psi_{3,4}$; thus $\tilde{\varphi}^+ = R_{1,2}$ and $\tilde{\psi}^+ = R_{3,4}$. Define $\phi : \mathbf{m} \rightarrow \mathbf{m}$ by $\phi(x) := \begin{cases} \psi(x) & \text{if } \varphi(x) \in S_{1,2,r} \\ \varphi(x) & \text{else} \end{cases}$ and consider $\tilde{\phi}^+ \in \mathcal{D}^1(\mathcal{T})$. Since $\mathcal{D}^1(\mathcal{T}) \subset \hat{\Omega}_n$, there is a $\xi \in \Psi$ satisfying $\tilde{\xi} \subset \tilde{\xi}^+ \subset \tilde{\phi}^+$. We observe that it is only possible if either $R_{1,2} \subset \tilde{\phi}^+$ or $R_{3,4} \subset \tilde{\phi}^+$, since $R_{1,2}$ and $R_{3,4}$ are minimal and disjoint. However, by definition we have $R_{1,2} \not\subset \tilde{\phi}^+$, and hence $R_{3,4} \subset \tilde{\phi}^+$, i.e. $R_{3,4} = \tilde{\phi}^+ \cap R_{3,4} = (\tilde{\phi} \cap R_{3,4})^+$. By previous general observation, this yields $\#(U) = \#(\tilde{\phi}^+ \cap R_{3,4}) \geq 2n - 1$, where $U := \{x \in \mathbf{m} \mid \varphi(x) \in S_{1,2,r}\}$. Since $\vartheta \in \tilde{\varphi}$ was arbitrary chosen and $\bigsqcup_{r=1}^n S_{k,l,r}$ is a disjoint partition of $R_{k,l}$ where for each $r \in \mathbf{n}$, $\#(S_{1,2,r}) = n$, we can argue analogously for all $\vartheta \in \tilde{\varphi}$, which yields $m \geq \frac{2n-1}{n} \cdot \#(\tilde{\varphi})$. Furthermore, we take any $\vartheta' \in S' = \tilde{\phi} \cap S_{3,4,r'}$, $R_{3,4} \not\supseteq (\tilde{\phi} \cap R_{3,4} - S')$, and consider any $\psi' \in \Psi_{5,6}$. Arguing as above we arrive at $m \geq \frac{(2n-1)^2}{n} \cdot \#(\tilde{\varphi})$, and so on. By iteration this yields $m \geq \left(\frac{2n-1}{n}\right)^{\frac{n}{2}} \cdot \#(\tilde{\varphi}) \geq \left(\frac{2n-1}{n}\right)^{\frac{n}{2}} (2n - 1)$. Hence m is superpolynomial in n , Q.E.D.

To put it more exactly, we easily arrive at the following

Criterion 43 *For any natural numbers $n > 1$, $c > 0$ and any Π_2 -tree \mathcal{T} satisfying $\#(\mathcal{T}) \leq n^c$, either $\Omega_n \not\subset \mathcal{D}^1(\mathcal{T})$ or $\mathcal{D}^1(\mathcal{T}) \not\subset \hat{\Omega}_n$ holds true, provided that $c < n \log_n(2 - \frac{1}{n}) + 2 \log_n(2n - 1)$. In particular, $\Omega_n \not\subset \mathcal{D}^1(\mathcal{T})$ or $\mathcal{D}^1(\mathcal{T}) \not\subset \hat{\Omega}_n$ holds whenever $n \log_n(1.5) > c$.*

4.2 CS^p -cases Σ_3 , Π_3 and beyond

In the Π_2 case (see above) we did not require the whole Ω_n to be in $\mathcal{D}^1(\mathcal{T})$ and actually used a weaker assumption $\Omega_n^1 \subset \mathcal{D}^1(\mathcal{T}) \subset \hat{\Omega}_n$ instead (in fact $\#(\Omega_n^1) = \frac{1}{2}n(n-1)$ is polynomial in n). But it is not difficult to modify our Π_2 proof under another weak assumption that requires $\mathcal{D}^1(\mathcal{T}) \subset \hat{\Omega}_n$ to contain any subset of Ω_n whose cardinality is merely a polynomial divisor of $\#(\Omega_n)$ (see also 4.1.1 above). Note that the latter modification is sufficient for the proof of CS^p in the Σ_3 case $f_{\mathcal{T}} = \bigvee_{i=1}^m \bigwedge_{j=1}^m \bigvee_{k=1}^m \{u_{i,j,k}, v_{i,j,k}\}$. The Π_3 case $f_{\mathcal{T}} = \bigwedge_{i=1}^m \bigvee_{j=1}^m \bigwedge_{k=1}^m \{u_{i,j,k}, v_{i,j,k}\}$ is proved by the modified iteration along the lines of the Π_2 -proof. This generalizes previous Π_2 -case by strengthening

$\vartheta_{i,\varphi(i)} \in \mathbf{n}^{2*2}$ to $\vartheta_{i,\varphi(i)} \in \mathbf{n}^{2*2}$, i.e. regarding matrix elements as arbitrary multisubsets of \mathbf{n}^{2*2} . For $k > 3$, the corresponding Σ_k, Π_k cases should follow by analogous, though more sophisticated induction on k .

4.3 General CS case

To grasp the deviation from CS^p , consider basic cases Σ_2, Π_2 . Without loss of generality let $f_{\mathcal{T}} = \bigvee_{i=1}^m \left(\bigwedge_{j=1}^m \vartheta_{i,j}^+ \wedge \bigwedge_{j=1}^m \vartheta_{i,j}^- \right)$ and $f_{\mathcal{T}} = \bigwedge_{i=1}^m \left(\bigvee_{j=1}^m \vartheta_{i,j}^+ \vee \bigvee_{j=1}^m \vartheta_{i,j}^- \right)$ in Σ_2 and Π_2 case, respectively, where $\vartheta_{i,j}^+ = \{u_{i,j}^+, v_{i,j}^+\} = \varrho_1(a_{i,j}) \in \mathbf{n}^{2*2}$ and $\vartheta_{i,j}^- = \{u_{i,j}^-, v_{i,j}^-\} = \varrho_2(a_{i,j}) \in \mathbf{n}^{2*2}$ are the correlated source labels, $\#(\mathcal{T}) = m^2$ being polynomial in n . Case Σ_2 does not really differ from previous CS^p consideration, since clearly $\#(\mathcal{D}^2(\mathcal{T})) \leq m < \#(\mathcal{T})$. Case Π_2 is more involved because we cannot guarantee that composite choice sequences like $\phi : \mathbf{m} \rightarrow \mathbf{m}$ (see 4.1.2 above) are consistent. That is, if two different choice sequences $\varphi, \psi : \mathbf{m} \rightarrow \mathbf{m}$ are consistent, then substituting (say) $\psi(x)$ for $\varphi(x)$ can lead to inconsistency, provided that $\vartheta_{x,\psi(x)}^- \in \widetilde{\varphi}^- := \{\vartheta_{i,\varphi(i)}^- \mid i = 1, \dots, m\}$. A desired conclusion that m is superpolynomial in n requires more advanced combinatorial arguments, which will be presented elsewhere.

5 Appendix (cf. [G04])

Definition 44 If $\{u, v\} \in \mathbf{n}^{2*2}$, Borel sets $\mathcal{O}_{\{u,v\}} := \{\vec{x} \in \mathbb{R}_0^n \mid x_u + x_v = 0\}$ and their complements $\overline{\mathcal{O}}_{\{u,v\}} := \{\vec{x} \in \mathbb{R}_0^n \mid x_u + x_v \neq 0\}$ are called regular planes and coplanes (in \mathbb{R}_0^n), respectively; they both are also called regular elements. A set of regular elements $\{\mathcal{O}_i, \overline{\mathcal{O}}_j \mid i \in I, j \in J\}$, $I \cap J = \emptyset$, is called consistent if no $\bigcap_{i \in I} \mathcal{O}_i \cap \bigcap_{j \in J} \overline{\mathcal{O}}_j = \{\mathbf{0}\}$. Intersections of sets of regular planes and consistent sets of regular elements are called regular Π_1 -sets and regular Π_1 -expansions, respectively. For any regular Π_1 -expansion $E = \bigcap_{i \in I} \mathcal{O}_i \cap \bigcap_{j \in J} \overline{\mathcal{O}}_j$, $I \cap J = \emptyset$, denote by E^p the corresponding regular Π_1 -set $\bigcap_{i \in I} \mathcal{O}_i$; clearly $E \subset E^p$.

Claim 45 Disjunction property. For any regular Π_1 -sets U, V and W , if $U \subset V \cup W$ then either $U \subset V$ or $U \subset W$.

Proof. Because regular Π_1 -sets are convex. (Geometrically obvious.) ■

Claim 46 Absorption property. For any regular Π_1 -expansion E and regular Π_1 -set U , if $E \subset U$ then $E^p \subset U$.

Proof. Because regular Π_1 -sets are convex and closed (see also [GK: Lemma 34]). ■

Claim 47 Monotonicity. For any $X, Y \subset \mathbf{n}^{2*2}$ and the corresponding regular Π_1 -sets $U = \bigcap_{i \in X} \mathcal{O}_i$ and $V = \bigcap_{i \in Y} \mathcal{O}_i$, if $V \subset U$ then $X^+ \subset Y^+$.

Proof. Easy linear algebra a/o the completeness of equational calculus. ■

6 References

[BDH]: S. Ben-David, S. Halevi, *On the Independence of P versus NP* (revised version), Tech. Report #699, Technion, 1991

[GK]: L. Gordeev, A. Krebs, *Elementary Interpretations of NP vs. P*, Second St. Petersburg Logic Days, 2003

<http://www-ls.informatik.uni-tuebingen.de/gordeew/publikationen/e4.pdf>

[GMaple]: L. Gordeev, *Base B3 (Maple program/Text)*, 2004

<http://www-ls.informatik.uni-tuebingen.de/gordeew/publikationen/B3Test.pdf>

[G04]: L. Gordeev, *Proof-sketch: Why NP is not P*, 2004

<http://www-ls.informatik.uni-tuebingen.de/gordeew/publikationen/ProofSketch.pdf>