

On P Versus NP

L. Gordeev

lew.gordeew@uni-tuebingen.de

Sep 2022

Abstract. Consider a following NP-problem DOUBLE CLIQUE (abbr.: CLIQ₂): Given a natural number $k > 2$ and a pair of two disjoint subgraphs of a fixed graph G decide whether each subgraph in question contains a k -clique. I prove that CLIQ₂ can't be solved in polynomial time by a deterministic TM, **which infers $P \neq NP$** . This proof upgrades the well-known proof of polynomial unsolvability of the partial result with respect to analogous monotone problem CLIQUE (abbr.: CLIQ). However, problem CLIQ₂ is not monotone and appears more complex than just iterated CLIQ, as the required subgraphs are mutually dependent (cf. Remark 27 in the text).

1 Introduction and survey of contents

The paper deals with the open problem **P versus NP**¹ usually abbreviated to: **P = NP** or **P \neq NP**? I argue in favor of **P \neq NP**. To this end first recall three well-known observations (cf. e.g. [1], [4], [3], [7], [8]):

- (A) The well-known graph theoretic problem CLIQUE is NP-complete. Thus in order to prove **P \neq NP** it will suffice e.g. to show that for sufficiently large natural number k there is no Boolean circuit of k -polynomial size expressing that a given graph G on k^4 vertices has a clique of k elements; this particular case of CLIQUE problem I'll designate CLIQ(G, k^4, k).
- (B) CLIQ(G, k^4, k) is monotone, i.e. $G \subset H$ implies CLIQ(G, k^4, k) \rightarrow CLIQ(H, k^4, k), while CLIQ(G, k^4, k) is not solvable by monotone, i.e. negation-free (\vee, \wedge)-circuits. More precisely, for sufficiently large k , the size of monotone circuit solutions of CLIQ(G, k^4, k) is exponential in k .
- (C) Computational complexity of Boolean circuits is linear in that of DeMorgan normal (abbr.: DMN) (\vee, \wedge)-circuits which allow negated inputs.

Summing up, in order to prove **P \neq NP** it will suffice to show that for sufficiently large natural numbers $k < m$ there are no DMN circuit solutions of CLIQ(G, m, k) whose size is polynomial in k . In fact, instead of CLIQ(G, k^4, k), it will suffice to work with an apparently stronger (but equivalent modulo NP complexity) non-monotone *double clique* problem CLIQ₂(G_1, G_2, k^{15}, k) saying that two disjoint subgraphs G_1 and G_2 of a given graph H on k^{15} vertices both contain cliques of k elements. To formalize the latter problem I upgrade monotone approach of (B) in §§2–3 using the underlying method of approximations. So aside from plain graphs I consider *double graphs* (= pairs of disjoint graphs consisting of positive and negative parts thereof) and instead of circuits and related circuit considerations I use Boolean DMN formulas (φ) and formalism of Boolean algebra, where approximations imitate disjunctive normal forms

¹See e.g. https://en.wikipedia.org/wiki/P_versus_NP_problem.

with respect to literals involved. I apply an appropriate *double Erdős-Rado* lemma to both positive and negative parts of double graphs and estimate upper bounds on deviations between total numbers of special test graphs accepted by φ and its approximation (Lemma 13). Using these upper bounds I show that the circuit size of φ that behaves correctly on all test graphs is exponential in k (Theorem 14). In the rest of §3 I use a suitable semantic approach to conclude that the assumptions of Theorem 14 are fulfilled by affirmative DMN solutions φ of $\text{CLIQ}_2(G_1, G_2, k^{15}, k)$ (Lemma 21, Corollary 22). Together with (C) this yields the result (Theorem 25, Corollary 26). The entire proof is formalizable in the exponential function arithmetic **EFA**. Below for the sake of brevity $\text{CLIQ}(G, k^4, k)$ and $\text{CLIQ}_2(G_1, G_2, k^{15}, k)$ are abbreviated by CLIQ and CLIQ_2 , respectively.

Acknowledgment I would like to thank René Thiemann who took the time to verify crucial proofs with Isabelle. His work was extremely helpful in finding flaws and errors in prior presentation of the results.

2 Preliminaries

2.1 Basic notations

- In the sequel we assume $2 < \ell, 2\ell + 1 \leq p < k \leq m^{\frac{1}{15}}$ and $L = (p - 1)^{3\ell} \ell!$.
- For any $A, B \subseteq [m]$ we let $A * B := \{\{x, y\} : x \in A \ \& \ y \in B \ \& \ x \neq y\}$ and $A^{(2)} := A * A$, where $[m] := \{1, \dots, m\}$. Thus $|[m]^{(2)}| = \frac{1}{2}m(m - 1)$, where $|S| := \text{card}(S)$.
- For any $X \subseteq [m]^{(2)}$ let:
 1. $v(X) := \{x \in [m] : (\exists y \in [m]) \{x, y\} \in X\}$,
 2. $\tilde{X} := v(X)^{(2)} \setminus X = \{\{x, y\} \in v(X)^{(2)} : \{x, y\} \notin X\}$.
- Let $\mathcal{F} := \{f : [m] \rightarrow [k]\}$ and for any $f \in \mathcal{F}$ let:

$$\text{Dom}^\circ(f) := \{x \in [m] : f(x) < k\} = \text{Dom}(f) \setminus f^{-1}\{k\},$$

$$C_f := \{\{x, y\} \in \text{Dom}^\circ(f)^{(2)} : f(x) \neq f(y)\}.$$

2.2 Plain and double graphs

- Call $\mathcal{G} := \wp[m]^{(2)}$ the set of *plain graphs* (unordered, possibly empty) with m vertices. For any $\emptyset \neq G \in \mathcal{G}$ call pairs $\{x, y\} \in G$ and $v(G)$ the *edges* and *vertices*, respectively.

- $\boxed{\text{POS} := \mathcal{K} := \{v(G)^{(2)} : |v(G)| = k\}}$ and $\boxed{\text{CLIQ} := \{G \in \mathcal{G} : (\exists K \in \mathcal{K}) K \subseteq G\}}$ are called *cliques* and *plain clique problem*, respectively.
- $\boxed{\text{NEG} := \{C_f : f \in \mathcal{F}\}}$ and $\boxed{\text{NOCLIQ} := \{G \in \mathcal{G} : (\exists H \in \text{NEG}) G \subseteq H\}}$ are called *negative tests* and *plain nocliques*, respectively.
- Pairs of disjoint plain graphs are called *double graphs*. That is, we define $\boxed{\mathcal{D} := \{\langle G, H \rangle \in \mathcal{G} \times \mathcal{G} : G \cap H = \emptyset\}}$ to be the set of double graphs. \mathcal{G} is viewed as part of \mathcal{D} via $\mathcal{G} \ni G \hookrightarrow \langle G, \emptyset \rangle \in \mathcal{D}$ and/or $\mathcal{G} \ni G \hookrightarrow \langle \emptyset, G \rangle \in \mathcal{D}$.
- For any $D = \langle G, H \rangle \in \mathcal{D}$ let $\boxed{D^+ := G \text{ and } D^- := H}$.
- For any $D, E \in \mathcal{D}$ we abbreviate $\boxed{D \subseteq^\pm E \Leftrightarrow D^+ \subseteq E^+ \ \& \ D^- \subseteq E^-}$.
- $\boxed{\text{POS}_2 := \{E \in \mathcal{K} \times \mathcal{K} : v(E^-) \cap v(E^+) = \emptyset\}}$ and $\boxed{\text{CLIQ}_2 := \{D \in \mathcal{D} : (\exists E \in \text{POS}_2) E \subseteq^\pm D\}}$ are called *double cliques* and *double clique problem*, respectively.
- $\boxed{\mathcal{F}_2 := \{\langle f, g \rangle \in \mathcal{F} \times \mathcal{F} : \text{Dom}^\circ(f) \uplus \text{Dom}^\circ(g) = [m]\}}$, where $A \uplus B = C \Leftrightarrow A \cup B = C \ \& \ A \cap B = \emptyset$.
- For any $\langle f, g \rangle \in \mathcal{F}_2$ let $\boxed{C_{\langle f, g \rangle} := \langle C_f, C_g \rangle}$.
- $\boxed{\text{NEG}_2 := \{C_{\langle f, g \rangle} : \langle f, g \rangle \in \mathcal{F}_2\} \subseteq \mathcal{D}}$ and $\boxed{\text{NOCLIQ}_2 := \{D \in \mathcal{D} : (\exists E \in \text{NEG}_2) D \subseteq^\pm E\}}$ are called *negative double tests* and *double nocliques*, respectively.

Lemma 1 $\text{POS}_2 \subset \text{CLIQ}_2$, $\text{NEG}_2 \subset \text{NOCLIQ}_2$ and $\text{CLIQ}_2 \cap \text{NOCLIQ}_2 = \emptyset$. Moreover $|\text{POS}_2| = \binom{m}{k} \binom{m-k}{k}$, $|\mathcal{F}_2| = (k-1)^m (2^m - m - 1) > |\text{NEG}_2| = |\mathcal{F}_2|_{\simeq}$, where for $\langle f, g \rangle, \langle f', g' \rangle \in \mathcal{F}_2$ we let $\langle f, g \rangle \simeq \langle f', g' \rangle \Leftrightarrow C_{\langle f, g \rangle} = C_{\langle f', g' \rangle}$.

Proof. First assertion and $|\text{POS}_2| = \binom{m}{k} \binom{m-k}{k}$ are readily seen. Now $|\mathcal{F}_2| = \sum_{i=2}^m (k-1)^i (k-1)^{m-i} \binom{m}{i} = (k-1)^m \sum_{i=2}^m \binom{m}{i} = (k-1)^m (2^m - m - 1)$. The rest is obvious (a more precise estimation of $|\text{NEG}_2|$ is not important). ■

2.3 Basic operations on sets of double graphs

Except for standard set-theoretic union \cup we consider a following product \odot .

For any $\mathcal{X}, \mathcal{Y} \subseteq \mathcal{D}$ let $\boxed{\mathcal{X} \odot \mathcal{Y} := \{D \uplus E : \langle D, E \rangle \in \mathcal{X} \times \mathcal{Y}\}} \subseteq \mathcal{D}$, where

$$D \uplus E := \begin{cases} \langle D^+ \cup E^+, D^- \cup E^- \rangle, & \text{if } (D^+ \cup E^+) \cap (D^- \cup E^-) = \emptyset, \\ \langle \emptyset, \emptyset \rangle & \text{else.} \end{cases}$$

Note that $\emptyset \odot \mathcal{Y} = \mathcal{X} \odot \emptyset = \emptyset$. It is readily seen that following conditions 1–3 hold for any $\mathcal{X}, \mathcal{Y}, \mathcal{X}', \mathcal{Y}' \subseteq \mathcal{D}$.

1. $\mathcal{X} \odot \mathcal{Y} = \mathcal{Y} \odot \mathcal{X}$, $\mathcal{X} \odot (\mathcal{Y} \odot \mathcal{Z}) = (\mathcal{X} \odot \mathcal{Y}) \odot \mathcal{Z}$.
2. $\mathcal{X} \odot (\mathcal{Y} \cup \mathcal{Z}) = (\mathcal{X} \odot \mathcal{Y}) \cup (\mathcal{X} \odot \mathcal{Z})$, $\mathcal{X} \cup (\mathcal{Y} \odot \mathcal{Z}) \subseteq (\mathcal{X} \cup \mathcal{Y}) \odot (\mathcal{X} \cup \mathcal{Z})$.
3. $\mathcal{X} \subseteq \mathcal{X}' \& \mathcal{Y} \subseteq \mathcal{Y}' \Rightarrow \mathcal{X} \odot \mathcal{Y} \subseteq \mathcal{X}' \odot \mathcal{Y}'$.

3 Proof proper

3.1 Acceptability

With any given set of double graphs $\mathcal{X} \subseteq \mathcal{D}$ we correlate the *accepted* (especially positive) double tests $\text{AC}(\mathcal{X}) \subseteq \mathcal{D}$, $\text{AC}^p(\mathcal{X}) \subseteq \text{POS}_2$ and negative double colorings $\text{AC}^N(\mathcal{X}) \subseteq \text{NEG}_2$.

Definition 2 For any $\mathcal{X} \subseteq \mathcal{D}$, $D \in \mathcal{D}$ let $\mathcal{X} \Vdash^\pm D \Leftrightarrow (\exists E \in \mathcal{X}) E \subseteq^\pm D$.

Corresponding sets of accepted double tests, resp. colorings, are as follows.

1. $\text{AC}(\mathcal{X}) := \{D \in \mathcal{D} : \mathcal{X} \Vdash^\pm D\}$, $\text{AC}^p(\mathcal{X}) := \text{AC}(\mathcal{X}) \cap \text{POS}_2$.
2. $\text{AC}^N(\mathcal{X}) := \{C_{\langle f, g \rangle} \in \text{NEG}_2 : \mathcal{X} \Vdash^\pm C_{\langle f, g \rangle}\}$.

Lemma 3 Conditions 1–4 hold for any $\mathcal{X}, \mathcal{Y} \subseteq \mathcal{D}$.

1. $\text{AC}(\emptyset) = \text{AC}^p(\emptyset) = \text{AC}^N(\emptyset) = \emptyset$.
2. $\text{AC}(\mathcal{D}) = \mathcal{D}$, $\text{AC}^p(\text{POS}_2) = \text{POS}_2$, $\text{AC}^N(\text{NEG}_2) = \text{NEG}_2$.
3. (a) $\text{AC}(\mathcal{X} \cup \mathcal{Y}) = \text{AC}(\mathcal{X}) \cup \text{AC}(\mathcal{Y})$,
 (b) $\text{AC}^p(\mathcal{X} \cup \mathcal{Y}) = \text{AC}^p(\mathcal{X}) \cup \text{AC}^p(\mathcal{Y})$,
 (c) $\text{AC}^N(\mathcal{X} \cup \mathcal{Y}) = \text{AC}^N(\mathcal{X}) \cup \text{AC}^N(\mathcal{Y})$.
4. (a) $\text{AC}(\mathcal{X} \cap \mathcal{Y}) \subseteq \text{AC}(\mathcal{X} \odot \mathcal{Y}) = \text{AC}(\mathcal{X}) \cap \text{AC}(\mathcal{Y})$,
 (b) $\text{AC}^p(\mathcal{X} \cap \mathcal{Y}) \subseteq \text{AC}^p(\mathcal{X} \odot \mathcal{Y}) = \text{AC}^p(\mathcal{X}) \cap \text{AC}^p(\mathcal{Y})$,
 (c) $\text{AC}^N(\mathcal{X} \cap \mathcal{Y}) \subseteq \text{AC}^N(\mathcal{X} \odot \mathcal{Y}) = \text{AC}^N(\mathcal{X}) \cap \text{AC}^N(\mathcal{Y})$.

Proof. 1–3: trivial.

4 (a). It suffices to prove $\text{AC}(\mathcal{X} \odot \mathcal{Y}) = \text{AC}(\mathcal{X}) \cap \text{AC}(\mathcal{Y})$. So suppose $D \in \text{AC}(\mathcal{X} \odot \mathcal{Y})$, i.e. $\mathcal{X} \odot \mathcal{Y} \Vdash^\pm D$, i.e. there are $E_1 \in \mathcal{X}$ and $E_2 \in \mathcal{Y}$ such that $E_1^+ \cup E_2^+ \subseteq D^+$ and $E_1^- \cup E_2^- \subseteq D^-$, which by

$$\begin{aligned} E_1^+ \cup E_2^+ \subseteq D^+ &\& E_1^- \cup E_2^- \subseteq D^- \Leftrightarrow \\ E_1^+ \subseteq D^+ &\& E_1^- \subseteq D^- &\& E_2^+ \subseteq D^+ &\& E_2^- \subseteq D^- \end{aligned}$$

yields both $D \in \text{AC}(\mathcal{X})$ and $D \in \text{AC}(\mathcal{Y})$. Suppose $D \in \text{AC}(\mathcal{X}) \cap \text{AC}(\mathcal{Y})$, i.e. $\mathcal{X} \Vdash^\pm D$ and $\mathcal{Y} \Vdash^\pm D$, i.e. there are $E_1 \in \mathcal{X}$ and $E_2 \in \mathcal{Y}$ such that $E_1^+ \subseteq D^+$, $E_1^- \subseteq D^-$, $E_2^+ \subseteq D^+$, $E_2^- \subseteq D^-$ and hence $E_1 \uplus E_2 \in \mathcal{X} \odot \mathcal{Y}$, which by the same token yields $D \in \text{AC}(\mathcal{X} \odot \mathcal{Y})$.

4 (b), (c) follow analogously to 4 (a). ■

3.2 Approximations and deviations

In what follows we generalize conventional monotone approach, cf. e.g. [4], [8], [3], [7]. We supply operations \cup and \odot on $\wp \mathcal{D}$ with *approximators* \sqcup and \sqcap operating on arbitrary subsets $\mathcal{X} \subseteq \mathcal{D}$ such that for all D from \mathcal{X} , $\max\{|\mathbf{v}(D^+)|, |\mathbf{v}(D^-)|\} \leq \ell$; note that we approximate both (positive and negative) parts of double graphs. We define corresponding *double deviations* $\partial_{\sqcup}^p, \partial_{\sqcup}^n, \partial_{\sqcap}^p, \partial_{\sqcap}^n$ from \cup and \odot with respect to accepted double test graphs and show that these deviations make “small” fractions thereof (Lemmata 10, 11). Double deviations are analogous to “error sets” caused by approximations in conventional monotone approach that is based on the Erdős-Rado lemma [3], [8], [10]. However, dealing with double graphs we’ll use a suitable “double” version of the latter.

3.2.1 Basic notations and definitions

- Let $\mathcal{G}^\ell := \{G \in \mathcal{G} : |\mathbf{v}(G)| \leq \ell\}$ and $\mathcal{D}^\ell := \{D \in \mathcal{D} : \|\mathbf{v}(D)\| \leq \ell\}$, where $\|\mathbf{v}(D)\| := \max\{|\mathbf{v}(D^+)|, |\mathbf{v}(D^-)|\}$.²
- If $D, E \in \mathcal{D}^\ell$ and $\mathcal{X}, \mathcal{Y} \subseteq \mathcal{D}^\ell$, let $D \uplus^\ell E := \begin{cases} D \uplus E, & \text{if } D \uplus E \in \mathcal{D}^\ell, \\ \emptyset & \text{else,} \end{cases}$ and $\mathcal{X} \odot^\ell \mathcal{Y} := \{D \uplus^\ell E : D \in \mathcal{X} \ \& \ E \in \mathcal{Y}\} \setminus \{\emptyset\} \in \wp \mathcal{D}^\ell$.
- For any $\mathcal{X} \subseteq \mathcal{D}$ let $\mathcal{X}^+ = \{D^+ : D \in \mathcal{X}\}$, $\mathcal{X}^- = \{D^- : D \in \mathcal{X}\}$, $\mathbf{v}(\mathcal{X}) := \{\mathbf{v}(D) : D \in \mathcal{X}\}$ for $\mathbf{v}(D) := \langle \mathbf{v}(D^+), \mathbf{v}(D^-) \rangle$, $\wp_L \mathcal{D} := \{\mathcal{X} \subseteq \mathcal{D} : |\mathcal{X}| \leq L\}$ and $\wp_L \mathcal{D}^\ell := \{\mathcal{X} \subseteq \mathcal{D}^\ell : |\mathcal{X}| \leq L\}$.
- Parallel to double graphs \mathcal{D} we’ll consider auxiliary *double sets* $\mathcal{S} := \{\langle A, B \rangle : A, B \subseteq [m] \ \& \ A \cap B = \emptyset\}$. For any $S = \langle A, B \rangle \in \mathcal{S}$ denote A by S^+ and B by S^- and for $S, T \in \mathcal{S}$ let $S \mathbin{\frown} T := \langle S^+ \cap T^+, S^- \cap T^- \rangle \in \mathcal{S}$. Now for any $D \in \mathcal{D}$ define $\mathbf{s}(D) \in \mathcal{S}$ by $\mathbf{s}(D)^+ := \mathbf{v}(D^+) \setminus \mathbf{v}(D^-)$ and $\mathbf{s}(D)^- := \mathbf{v}(D^-) \setminus \mathbf{v}(D^+)$ and for any $\mathcal{X} \subseteq \mathcal{D}$ let $\mathbf{s}(\mathcal{X}) := \{\mathbf{s}(D) : D \in \mathcal{X}\}$.

²Note that $G \in \mathcal{G}^\ell$ implies $\sqrt{2|G|} < \frac{1}{2} (1 + \sqrt{1 + 8|G|}) \leq |\mathbf{v}(G)| \leq 2\ell$.

- Let $\mathcal{S}^\ell := \{S \in \mathcal{S} : \|S\| \leq \ell\}$ where $\|S\| := \max\{|S^+|, |S^-|\}$, $\wp_L \mathcal{S} := \{\mathcal{X} \subseteq \mathcal{S} : |\mathcal{X}| \leq L\}$ and $\wp_L \mathcal{S}^\ell := \{\mathcal{X} \subseteq \mathcal{S}^\ell : |\mathcal{X}| \leq L\}$. Thus for any $\mathcal{X} \subseteq \mathcal{D}$, $\mathcal{Y} \subseteq \mathcal{D}^\ell$ and $\mathcal{Z} \in \wp_L \mathcal{D}^\ell$ we have $s(\mathcal{X}) \subseteq \mathcal{S}$, $s(\mathcal{Y}) \subseteq \mathcal{S}^\ell$ and $s(\mathcal{Z}) \in \wp_L \mathcal{S}^\ell$.

Definition 4 A collection of double sets $\mathcal{V} = \{S_1, \dots, S_p\} \subset \mathcal{S}$ is called a sunflower with p (different) petals S_1, \dots, S_p if $S_1 \cap S_2 = S_i \cap S_j$ holds for all $i < j \in [p]$. Then $S_\odot = \bigcap_{j=1}^p S_j = S_1 \cap S_2$ is called the core of \mathcal{V} .

Lemma 5 Any $\mathcal{U} \subseteq \mathcal{S}^\ell$ such that $|\mathcal{U}| > L$ contains a sunflower $\mathcal{V} \subset \mathcal{U}$ with p petals S_1, \dots, S_p and core $S_\odot \in \mathcal{S}^\ell$.

Proof. ³ Regard $\langle A, B \rangle \in \mathcal{S}^\ell$ as disjoint sums $A \uplus B \subseteq [2\ell]$. By the original Erdős-Rado lemma [10], there is a required sunflower $\mathcal{V} \subset \mathcal{U}$, provided that $|\mathcal{U}| > L' := (p-1)^{2\ell} (2\ell)!$. But $L = (p-1)^{3\ell} \ell! > L'$ as by the assumption we have $p-1 \geq 2\ell$. ■

Definition 6 (double plucking) Double plucking algorithm $\wp \mathcal{D}^\ell \ni \mathcal{X} \mapsto \text{PL}_2(\mathcal{X}) \in \wp_L \mathcal{D}^\ell$ is defined by recursion on $|s(\mathcal{X})|$. If $|s(\mathcal{X})| \leq L$, let $\text{PL}_2(\mathcal{X}) := \mathcal{X}$. Otherwise, let $\mathcal{X}_0 := \mathcal{X}$. Hence $|s(\mathcal{X}_0)| > L$. By the double Erdős-Rado lemma we choose a sunflower of cardinality p , $\mathcal{V} = \{S_1, \dots, S_p\} \subseteq s(\mathcal{X}_0)$ with petals S_1, \dots, S_p and core $S_\odot = \bigcap_{j=1}^p S_j = \langle S_\odot^+, S_\odot^- \rangle \in \mathcal{S}^\ell$. Let $\mathcal{X}'_0 := \{D \in \mathcal{X}_0 : (\exists j \in [p]) s(D) = S_j\}$ and $D_\odot = \bigcap \{D : D \in \mathcal{X}'_0\} = \langle D_\odot^+, D_\odot^- \rangle \in \mathcal{D}^\ell$; thus $s(D_\odot)^+ \subseteq S_\odot^+$ and $s(D_\odot)^- \subseteq S_\odot^-$. Rewrite \mathcal{X}_0 to \mathcal{X}_1 that arises by replacing all $D \in \mathcal{X}'_0$ by $D_\odot := \langle D_\odot^+, D_\odot^- \rangle$. ⁴ Note that $|s(\mathcal{X}_1)| \leq |s(\mathcal{X}_0)| - p + 1$. Now if $|s(\mathcal{X}_1)| \leq L$, let $\text{PL}_2(\mathcal{X}) := \mathcal{X}_1$. Otherwise, if $|s(\mathcal{X}_1)| > L$, then we analogously pass from $\mathcal{X}_1 \subseteq \mathcal{D}^\ell$ to $\mathcal{X}_2 \subseteq \mathcal{D}^\ell$. Proceeding this way we eventually arrive at $\mathcal{X}_r \subseteq \mathcal{D}^\ell$ with $|s(\mathcal{X}_r)| \leq L$ and let $\text{PL}_2(\mathcal{X}) := \mathcal{X}_r$.

Lemma 7 For any given $\mathcal{X} \in \wp \mathcal{D}^\ell$, $\text{PL}_2(\mathcal{X}) \in \wp_L \mathcal{D}^\ell$ requires less than $|s(\mathcal{X})|$ elementary pluckings. That is, if $\text{PL}_2(\mathcal{X}) := \mathcal{X}_r$ as above, then $r < |s(\mathcal{X})|$.

Proof. Each elementary plucking reduces the number of sets at least by $p-1$. Hence $r < |s(\mathcal{X})| (p-1)^{-1} < |s(\mathcal{X})|$. ■

Definition 8 For any $\mathcal{X}, \mathcal{Y} \in \wp \mathcal{D}^\ell$ we call following operations \sqcup , \sqcap and sets $\mathcal{X} \sqcup \mathcal{Y}$, $\mathcal{X} \sqcap \mathcal{Y}$ the approximators of $\wp \mathcal{D}$ -operations \cup , \odot and corresponding approximations, respectively, which determine corresponding double deviations $\partial_\sqcup^p, \partial_\sqcup^N, \partial_\sqcap^p, \partial_\sqcap^N$ with respect to accepted tests. ⁵

1. $\mathcal{X} \sqcup \mathcal{Y} := \text{PL}_2(\mathcal{X} \cup \mathcal{Y}) \in \wp_L \mathcal{D}^\ell$.

³This proof is due to R. Thiemann.

⁴This operation will be referred to as elementary plucking.

⁵We write ∂ instead of δ used in [4]–[6].

2. $\mathcal{X} \sqcap \mathcal{Y} := \text{PL}_2(\mathcal{X} \odot^\ell \mathcal{Y}) \in \wp_L \mathcal{D}^\ell$.
3. $\partial_\sqcup^{\text{P}}(\mathcal{X}, \mathcal{Y}) := \text{AC}^{\text{P}}(\mathcal{X} \cup \mathcal{Y}) \setminus \text{AC}^{\text{P}}(\mathcal{X} \sqcup \mathcal{Y}) \subseteq \text{POS}_2$.
4. $\partial_\sqcap^{\text{P}}(\mathcal{X}, \mathcal{Y}) := \text{AC}^{\text{P}}(\mathcal{X} \odot \mathcal{Y}) \setminus \text{AC}^{\text{P}}(\mathcal{X} \sqcap \mathcal{Y}) \subseteq \text{POS}_2$
5. $\partial_\sqcup^{\text{N}}(\mathcal{X}, \mathcal{Y}) := \text{AC}^{\text{N}}(\mathcal{X} \sqcup \mathcal{Y}) \setminus \text{AC}^{\text{N}}(\mathcal{X} \cup \mathcal{Y}) \subseteq \text{NEG}_2$.
6. $\partial_\sqcap^{\text{N}}(\mathcal{X}, \mathcal{Y}) := \text{AC}^{\text{N}}(\mathcal{X} \sqcap \mathcal{Y}) \setminus \text{AC}^{\text{N}}(\mathcal{X} \odot \mathcal{Y}) \subseteq \text{NEG}_2$.

For any $\mathcal{U} \subseteq \text{NEG}_2$ we let $|\mathcal{U}|^* := \{ \langle f, g \rangle \in \mathcal{F}_2 : C_{\langle f, g \rangle} \in \mathcal{U} \}$ (\because functional cardinality of \mathcal{U}). In particular $|\text{NEG}_2|^* = \mathcal{F}_2$. In the sequel we use functional cardinality as our basic measure of the number of negative double tests involved.

Upper bounds Below we assume that m is sufficiently large and $k = \ell^2$.

Lemma 9 For any $D \in \mathcal{D}^\ell$ Let $\mathcal{R}_\subseteq(D) := \{ \langle f, g \rangle \in \mathcal{F}_2 : D \subseteq^\pm C_{\langle f, g \rangle} \}$ and $\mathcal{R}_{\not\subseteq}(D) := \{ \langle f, g \rangle \in \mathcal{F}_2 : D \not\subseteq^\pm C_{\langle f, g \rangle} \} = \mathcal{F}_2 \setminus \mathcal{R}_\subseteq(D)$. Then $|\mathcal{R}_\subseteq(D)| \geq \frac{1}{4} |\mathcal{F}_2|$ and $|\mathcal{R}_{\not\subseteq}(D)| \leq \frac{3}{4} |\mathcal{F}_2|$.⁶

Proof. For any $A \subseteq [m], |A| \geq 2$ and $G \in \mathcal{G}^\ell$ let

$$\mathcal{R}_\subseteq(A, G) := \{ f \in \mathcal{F} : \text{Dom}^\circ(f) = A \& G \subseteq C_f \}.$$

This yields by standard monotone arguments

$$|\mathcal{R}_\subseteq(A, G)| \geq \frac{1}{2} (k-1)^{|A|} \quad (\text{cf. e.g. Appendix A}).$$

Now for any $A \subseteq [m], |A| \geq 2$ and $D \in \mathcal{D}^\ell$ let

$$\mathcal{R}_\subseteq(A, D) := \{ \langle f, g \rangle \in \mathcal{F}_2 : \text{Dom}^\circ(f) = A \& \text{Dom}^\circ(g) = [m] \setminus A \& D \subseteq^\pm C_{\langle f, g \rangle} \}.$$

We have

$$\mathcal{R}_\subseteq(D) = \bigcup_{A \subseteq [m], |A| \geq 2} \mathcal{R}_\subseteq(A, D) = \bigcup_{A \subseteq [m], |A| \geq 2} \mathcal{R}_\subseteq(A, D^+) \times \mathcal{R}_\subseteq([m] \setminus A, D^-)$$

which yields

$$\begin{aligned} |\mathcal{R}_\subseteq(D)| &\geq \sum_{A \subseteq [m], |A| \geq 2} \frac{1}{2} |\mathcal{R}_\subseteq(A, G)| \times \frac{1}{2} |\mathcal{R}_\subseteq([m] \setminus A, G)|_{\simeq} \\ &\geq \frac{1}{4} \sum_{A \subseteq [m], |A| \geq 2} (k-1)^{|A|} \times (k-1)^{m-|A|} \\ &= \frac{1}{4} (k-1)^m \sum_{i=2}^m \binom{m}{i} = \frac{1}{4} (k-1)^m (2^m - m - 1) \\ &= \frac{1}{4} |\mathcal{F}_2| \end{aligned}$$

and hence

$$|\mathcal{R}_{\not\subseteq}(D)| \leq |\mathcal{F}_2| - |\mathcal{R}_\subseteq(D)| \leq |\mathcal{F}_2| - \frac{1}{4} |\mathcal{F}_2| = \frac{3}{4} |\mathcal{F}_2|.$$

■

⁶Constants $\frac{3}{4}$ and $\frac{1}{4}$ involved can be slightly improved to 0.63212056 and 0.36787944, respectively, for sufficiently large m .

Lemma 10 *Let $\mathcal{Z} = \text{PL}_2(\mathcal{X} \cup \mathcal{Y}) \in \wp_L \mathcal{D}^\ell$ for $\mathcal{X}, \mathcal{Y} \in \wp_L \mathcal{D}^\ell$ and $\mathcal{X} \cup \mathcal{Y} \in \wp \mathcal{D}^\ell$. So $|\mathcal{S}(\mathcal{Z})| \leq L$ and $|\mathcal{S}(\mathcal{X} \cup \mathcal{Y})| \leq 2L$. Then \mathcal{Z} requires $< 2L$ elementary pluckings. Moreover $\partial_\square^p(\mathcal{X}, \mathcal{Y}) = 0$ while $|\partial_\square^N(\mathcal{X}, \mathcal{Y})|^* < 2 \left(\frac{3}{4}\right)^p |\mathcal{F}_2| L$.*

Proof. We argue as in the analogous monotone case using Lemmata 7, 9. Let $\mathcal{V} = \{S_1, \dots, S_p\} \subseteq \mathcal{S}((\mathcal{X} \cup \mathcal{Y})_i)$ be the sunflower with petals S_1, \dots, S_p and core $S_\odot = \bigcap_{j=1}^p S_j$ that arises at i^{th} elementary plucking ($i > 0$) and let $D_\odot^+, D_\odot^- \in \mathcal{G}^\ell$ be the corresponding plain graphs (cf. Definition 6). $\partial_\square^p(\mathcal{X}, \mathcal{Y}) = \emptyset$ is clear as elementary pluckings replace some plain graphs by subgraphs and hence preserve the accepted positive double tests. Consider $\partial_\square^N(\mathcal{X}, \mathcal{Y})$. Let us estimate the total number of fake negative double tests that arise after executing rewriting $\mathcal{X}_{i-1} \hookrightarrow \mathcal{X}_i$ involved. Suppose that \mathcal{X}_i is obtained by substituting $D_\odot = \langle D_\odot^+, D_\odot^- \rangle = \bigcap \{D : D \in \mathcal{X}'_{i-1}\}$ for every $D \in \mathcal{X}'_{i-1}$, where $\mathcal{X}'_{i-1} = \{D \in \mathcal{X}_{i-1} : (\exists j \in [p]) \mathcal{S}(D) = S_j\}$ (cf. Definition 6). Let $|\mathcal{X}'_{i-1}| = p' \geq p$ and $\mathcal{X}'_{i-1} = \{D_1, \dots, D_{p'}\}$. Now let $C_{\langle f, g \rangle} = \langle C_f, C_g \rangle \in \text{NEG}_2$ be any fake negative double test created by this substitution. That is, $D_\odot \subseteq^\pm C_{\langle f, g \rangle}$ and hence $D_\odot^+ \subseteq C_f$ and $D_\odot^- \subseteq C_g$, although for every $t \in [p']$, we have $D_t \not\subseteq^\pm C_{\langle f, g \rangle}$. Let $D'_t := \langle D_t^+ \setminus D_\odot^+, D_t^- \setminus D_\odot^- \rangle \in \mathcal{D}^\ell$ and note that for any $s \neq t \in [p']$ we have $D'_s \cap D'_t = \emptyset \neq D_t$. This shows that the corresponding sets $\mathcal{R}_{\not\subseteq}(D_s)$ and $\mathcal{R}_{\not\subseteq}(D_t)$ are independent events in the space \mathcal{F}_2 . By Lemma 9 we conclude that $\mathbb{P}[\mathcal{R}_{\not\subseteq}(D_t)] \leq \frac{3}{4}$ holds for every $t \in [p']$, where for any $\mathcal{X} \subseteq \mathcal{F}_2$ we abbreviate $\mathbb{P}[\mathcal{X}] := |\mathcal{X}|_\simeq |\mathcal{F}_2|^{-1}$ (the probability). Hence

$$\mathbb{P}\left[\bigcap_{t=1}^{p'} \mathcal{R}_{\not\subseteq}(D_t)\right] = \prod_{t=1}^{p'} \mathbb{P}[\mathcal{R}_{\not\subseteq}(D_t)] \leq \prod_{t=1}^p \frac{3}{4} = \left(\frac{3}{4}\right)^p.$$

Consequently, with regard to functional cardinality there are less than

$$\mathbb{P}\left[\bigcap_{t=1}^{p'} \mathcal{R}_{\not\subseteq}(D_t)\right] |\mathcal{F}_2| \leq \left(\frac{3}{4}\right)^p |\mathcal{F}_2|$$

fake negative double tests $C_{\langle f, g \rangle}$ created by the replacement $\mathcal{X}_{i-1} \hookrightarrow \mathcal{X}_i$. Recall that by Lemma 7 there are $r < 2L$ elementary pluckings involved. This yields

$$\partial_\square^N(\mathcal{X}, \mathcal{Y}) \subseteq \bigcup_{i=0}^{r-1} \partial_\square^N(\mathcal{X}, \mathcal{Y})_i \text{ for } \partial_\square^N(\mathcal{X}, \mathcal{Y})_i := \text{AC}^N(\mathcal{X} \cup \mathcal{Y})_{i+1} \setminus \text{AC}^N(\mathcal{X} \cup \mathcal{Y})_i.$$

Hence $|\partial_\square^N(\mathcal{X}, \mathcal{Y})|^* \leq \sum_{i=0}^{r-1} |\partial_\square^N(\mathcal{X}, \mathcal{Y})_i|^* < r \left(\frac{3}{4}\right)^p |\mathcal{F}_2| < 2 \left(\frac{3}{4}\right)^p |\mathcal{F}_2| L$. ■

Lemma 11 Let $\mathcal{X}, \mathcal{Y} \in \wp_L \mathcal{D}^\ell$, $\mathcal{X} \odot^\ell \mathcal{Y} \in \wp \mathcal{D}^\ell$ and $\mathcal{Z} = \text{PL}_2(\mathcal{X} \odot^\ell \mathcal{Y}) \in \wp_L \mathcal{D}^\ell$.

So $|\mathcal{S}(\mathcal{Z})| \leq L$ and $|\mathcal{S}(\mathcal{X} \odot \mathcal{Y})| \leq L^2$. Then $|\partial_\sqcap^p(\mathcal{X}, \mathcal{Y})| < \binom{m-\ell-1}{k-\ell-1} \binom{m-k}{k} L^2$
and $|\partial_\sqcap^N(\mathcal{X}, \mathcal{Y})|^* < (\frac{3}{4})^p |\mathcal{F}_2| L^2$.

Proof. $|\partial_\sqcap^N(\mathcal{X}, \mathcal{Y})|^* < (\frac{3}{4})^p |\mathcal{F}_2| L^2$ is analogous to the inequality for $\partial_\sqcup^N(\mathcal{X}, \mathcal{Y})$. Consider $\partial_\sqcap^p(\mathcal{X}, \mathcal{Y})$. We adapt standard arguments used in familiar “monotone” proofs (cf. e.g. [3], [8]). It is readily seen that deviations can only arise by deleting a $D \uplus E \notin \mathcal{D}^\ell$ for some $D, E \in \mathcal{D}^\ell$ when passing from $\mathcal{X} \odot \mathcal{Y}$ to $\mathcal{X} \odot^\ell \mathcal{Y}$ (note that $\mathcal{X} \odot \mathcal{Y}$ can completely disappear, in which case $\text{PL}_2(\mathcal{X} \odot^\ell \mathcal{Y}) = \mathcal{X} \odot^\ell \mathcal{Y} = \emptyset$). So suppose $H \in (\mathcal{X} \odot \mathcal{Y}) \setminus \mathcal{D}^\ell$ and hence $H^b \in (\mathcal{X} \odot \mathcal{Y})^b \setminus \mathcal{G}^\ell$ for some $b \in \{+, -\}$. Thus $\ell < |\mathbf{v}(H^b)| \leq 2\ell$, while $|\mathbf{v}(H^\natural)| \leq 2\ell$ for $b \neq \natural \in \{+, -\}$. Moreover $\mathbf{v}(H^b) \cap \mathbf{v}(H^\natural) = \emptyset$. Let us estimate $|\mathcal{K}_H|$ for $\mathcal{K}_H := \{\langle K^b, K^\natural \rangle \in \text{POS}_2 : H^b \subseteq K^b \& H^\natural \subseteq K^\natural\}$. Note that $\ell < |\mathbf{v}(H^b)|$ and $K^b \cap K^\natural = \emptyset$ implies that \mathcal{K}_H contains at most $\binom{m-\ell-1}{k-\ell-1}$ cliques K^b and $\binom{m-k}{k}$ cliques K^\natural , respectively. Thus $|\mathcal{K}_H| \leq \binom{m-\ell-1}{k-\ell-1} \binom{m-k}{k}$. Now

$$\partial_\sqcap^p(\mathcal{X}, \mathcal{Y}) \subseteq \bigcup \{\mathcal{K}_H : H \in (\mathcal{X} \odot \mathcal{Y}) \setminus \mathcal{G}^\ell\} \subseteq \bigcup \{\mathcal{K}_H : H \in \mathcal{X} \odot \mathcal{Y}\}$$

which by $|\mathcal{S}(\mathcal{X} \odot \mathcal{Y})| \leq L^2$ and Lemma 7 yields the result. ■

3.3 Formalism

To formalize previous considerations we use basic DeMorgan logic with atomic negation (also called *DMN logic*) over $\binom{m}{2}$ distinct variables. For any DMN formula φ we define its double graph set representation $\mathcal{S}(\varphi)$ together with approximation $\text{AP}(\varphi)$ augmented with corresponding *total deviations* $\partial^p(\varphi) \subseteq \text{POS}_2$ and $\partial^N(\varphi) \subseteq \text{NEG}_2$. Using previous estimates on $\partial_\sqcup^p, \partial_\sqcup^N, \partial_\sqcap^p, \partial_\sqcap^N$ we show that the assumptions $\text{POS}_2 = \text{AC}^p(\mathcal{S}(\varphi))$ and $\text{AC}^N(\mathcal{S}(\varphi)) = \emptyset$ infer exponential circuit size of φ (cf. Theorem 14 below).

3.3.1 Syntax

- Let $n := \binom{m}{2} = \frac{1}{2}m(m-1)$ and $\pi : [n] \xrightarrow{1-1} [m]^{(2)}$.
- Let \mathcal{A} denote boolean algebra with constants \top, \perp , operations \vee, \wedge , atomic negation \neg and variables v_1, \dots, v_n . Formulas of \mathcal{A} (abbr.: φ, σ, τ) are built up from literals $\top, \perp, v_i, \neg v_i$ ($i = 1, \dots, n$) by positive operations \vee and \wedge . For brevity we also stipulate $\top \vee \varphi = \varphi \vee \top := \top$, $\perp \wedge \varphi = \varphi \wedge \perp := \perp$ and $\top \wedge \varphi = \varphi \wedge \top = \perp \vee \varphi = \perp \vee \varphi = \varphi \vee \perp := \varphi$. Let $\text{cs}(\varphi)$ denote structural complexity (= circuit size) of φ .⁷ De Morgan rules for negation

⁷More precisely $\text{cs}(\varphi)$ is the total number of pairwise distinct subterms of φ (including φ).

provide length-preserving interpretation in \mathcal{A} of corresponding full boolean algebra.

- We define by recursion on $\text{cs}(\varphi)$ two assignments

$$\mathcal{A} \ni \varphi \mapsto \text{DN}(\varphi) \in \{\top\} \cup \wp \mathcal{D} \text{ and } \mathcal{A} \ni \varphi \mapsto \text{AP}(\varphi) \in \{\top\} \cup \wp_L \mathcal{D}^\ell$$

that represent DNFs and corresponding approximations of τ , respectively.

1. $\text{DN}(\top) = \text{AP}(\top) := \top$, $\text{DN}(\perp) = \text{AP}(\perp) := \emptyset$.
 2. $\text{DN}(v_i) = \text{AP}(v_i) := \{\{\pi(i)\}, \emptyset\}$,
 $\text{DN}(\neg v_i) = \text{AP}(\neg v_i) := \{\{\emptyset, \{\pi(i)\}\}\}$.
 3. $\text{DN}(\sigma \vee \tau) := \text{DN}(\sigma) \cup \text{DN}(\tau)$, $\text{AP}(\sigma \vee \tau) := \text{AP}(\sigma) \sqcup \text{AP}(\tau)$.
 4. $\text{DN}(\sigma \wedge \tau) := \text{DN}(\sigma) \odot \text{DN}(\tau)$, $\text{AP}(\sigma \wedge \tau) := \text{AP}(\sigma) \sqcap \text{AP}(\tau)$.
- For any $\varphi \in \mathcal{A}$, total deviations $\partial^P(\varphi)$ and $\partial^N(\varphi)$ are defined as follows, where we let $\text{AC}^P(\top) := \text{POS}_2$ and $\text{AC}^N(\top) := \text{NEG}_2$ and abbreviate $\text{AC}^P(\text{DN}(\varphi))$ and $\text{AC}^N(\text{DN}(\varphi))$ by $\text{AC}^P(\varphi)$ and $\text{AC}^N(\varphi)$, respectively.
 1. $\partial^P(\varphi) := \text{AC}^P(\varphi) \setminus \text{AC}^P(\text{AP}(\varphi))$.
 2. $\partial^N(\varphi) := \text{AC}^N(\text{AP}(\varphi)) \setminus \text{AC}^N(\varphi)$.

Lemma 12 *For any $\sigma, \tau \in \mathcal{A}$ the following holds.*

1. $\partial^P(\sigma \vee \tau) \subseteq \partial^P(\sigma) \cup \partial^P(\tau) \cup \partial_{\sqcup}^P(\text{AP}(\sigma), \text{AP}(\tau))$.
2. $\partial^P(\sigma \wedge \tau) \subseteq \partial^P(\sigma) \cup \partial^P(\tau) \cup \partial_{\sqcap}^P(\text{AP}(\sigma), \text{AP}(\tau))$.
3. $\partial^N(\sigma \vee \tau) \subseteq \partial^N(\sigma) \cup \partial^N(\tau) \cup \partial_{\sqcup}^N(\text{AP}(\sigma), \text{AP}(\tau))$.
4. $\partial^N(\sigma \wedge \tau) \subseteq \partial^N(\sigma) \cup \partial^N(\tau) \cup \partial_{\sqcap}^N(\text{AP}(\sigma), \text{AP}(\tau))$.

Proof. Straightforward via boolean inclusion $A \setminus B \subseteq (A \setminus C) \cup (C \setminus B)$ (cf. Appendix C). ■

Lemma 13 *For any $\varphi \in \mathcal{A}$ the following holds.*

1. $|\partial^P(\varphi)| < \text{cs}(\varphi) \cdot \binom{m-\ell-1}{k-\ell-1} \binom{m-k}{k} L^2$.
2. $|\partial^N(\varphi)|^* \leq \text{cs}(\varphi) \cdot 2 \left(\frac{3}{4}\right)^p |\mathcal{F}_2| L^2$.
3. If $\text{AC}^P(\text{AP}(\varphi)) \neq \emptyset$ then $|\text{AC}^N(\text{AP}(\varphi))|^* \geq \frac{1}{4} |\mathcal{F}_2|$.

Proof. 1–2 follows from Lemmata 10, 11 by induction on $\text{cs}(\varphi)$.

3: $\text{AC}^P(\text{AP}(\varphi)) \neq \emptyset$ implies $\text{AP}(\varphi) \neq \emptyset$, so there is at least one $D \in \text{AP}(\varphi)$, $\|\vee(D)\| \leq \ell$. Now by Lemma 9, $|\text{AC}^N(\text{AP}(\varphi))|^* \geq |\mathcal{R}_{\subseteq}(D)| \geq \frac{1}{4} |\mathcal{F}_2|$, as $\text{AC}^N(\text{AP}(\varphi)) \supseteq \mathcal{R}_{\subseteq}(D)$. ■

- **Final assumptions.** Let

$$k = 2\ell^2 = m^{\frac{1}{15}}, \quad p = \ell \log_{\frac{4}{3}} m, \quad L = (p-1)^{3\ell} \ell!, \quad m \gg 0.$$

Theorem 14 *Suppose that $\text{POS}_2 = \text{AC}^P(\varphi)$ and $\text{AC}^N(\varphi) = \emptyset$ both hold for a given $\varphi \in \mathcal{A}$. Then for sufficiently large m , $\text{cs}(\varphi) > m^{\frac{1}{5}m^{\frac{1}{30}}} = m^{\frac{1}{5}\sqrt{k}}$.*

Proof. Consider two cases (cf. Appendix B).

1: Assume $\text{AC}^P(\text{AP}(\varphi)) = \emptyset$. By $\text{POS}_2 = \text{AC}^P(\varphi)$ we have

$$\partial^P(\varphi) = \text{AC}^P(\varphi) \setminus \text{AC}^P(\text{AP}(\varphi)) = \text{POS}_2. \text{ Hence by Lemma 13 (1),}$$

$$\text{cs}(\varphi) \cdot \binom{m-\ell-1}{k-\ell-1} \binom{m-k}{k} L^2 \geq |\partial^P(\varphi)| = |\text{POS}_2| = \binom{m}{k} \binom{m-k}{k}.$$

$$\text{Hence } \text{cs}(\varphi) \geq \binom{m}{k} \binom{m-\ell-1}{k-\ell-1}^{-1} L^{-2} > \left(\frac{m-\ell}{k}\right)^\ell L^{-2} > m^{\frac{1}{5}m^{\frac{1}{30}}}.$$

2: Otherwise, assume $\text{AC}^P(\text{AP}(\varphi)) \neq \emptyset$. So $\text{AC}^N(\varphi) = \emptyset$ implies

$$\partial^N(\varphi) = \text{AC}^N(\text{AP}(\varphi)) \setminus \text{AC}^N(\varphi) = \text{AC}^N(\text{AP}(\varphi)). \text{ Hence}$$

$$\text{cs}(\varphi) \cdot 2 \left(\frac{3}{4}\right)^p |\mathcal{F}_2| L^2 \geq |\partial^N(\varphi)|^* \geq \frac{1}{4} |\mathcal{F}_2| \text{ by Lemma 13 (2, 3). So}$$

$$\text{cs}(\varphi) \geq \frac{1}{8} \left(\frac{4}{3}\right)^p L^{-2} > m^{\frac{1}{5}m^{\frac{1}{30}}}. \quad \blacksquare$$

In the sequel we show that the assumptions of Theorem 14 are fulfilled by any formula $\varphi \in \mathcal{A}$ that provides a solution of CLIQ_2 . To this end we supply \mathcal{G} and \mathcal{D} with natural semantic, as follows.

3.3.2 Semantic

Definition 15 *Consider variable assignments $\text{VA} = \{\vartheta : [n] \longrightarrow \{0, 1, \square\}\}$ ⁸ where we set*

$$\begin{aligned} 0 \wedge 1 &= 1 \wedge 0 = 0, & 0 \wedge 0 &= 0, & 1 \wedge 1 &= 1, \\ 0 \vee 1 &= 1 \vee 0 = 1, & 0 \vee 0 &= 0, & 1 \vee 1 &= 1, \\ \square \wedge 0 &= 0 \wedge \square = 0, & \square \wedge 1 &= 1 \wedge \square = \square, & \square \wedge \square &= \square, \\ \square \vee 0 &= 0 \vee \square = 0, & \square \vee 1 &= 1 \vee \square = 1, & \square \vee \square &= \square. \end{aligned}$$

For any $v_i, \varphi_1, \dots, \varphi_s \in \mathcal{A}$, $G \in \mathcal{G}$, $D \in \mathcal{D}$, $\mathcal{X} \subseteq \mathcal{D}$, $\mathcal{Y} \subseteq \mathcal{G}$, $\vartheta \in \text{VA}$, formulas $F(G)$, $F(D)$, $F(\mathcal{X})$, $F(\mathcal{Y})$ and values $\|\sigma\|_\vartheta$, $\|\tau\|_\vartheta$, $\|G\|_\vartheta$, $\|D\|_\vartheta$, $\|\mathcal{X}\|_\vartheta$, $\|\mathcal{Y}\|_\vartheta$ are defined recursively as follows.

1. $F(G) := \bigwedge_{\pi(i) \in G} v_i$, $F(D) := \bigwedge_{\pi(i) \in D^+} v_i \wedge \bigwedge_{\pi(j) \in D^-} \neg v_j$.
2. $F(\mathcal{X}) := \bigvee_{D \in \mathcal{X}} F(D)$, $F(\mathcal{Y}) := \bigvee_{G \in \mathcal{Y}} F(G)$.
3. $\|\top\|_\vartheta := 1$, $\|\perp\|_\vartheta = \|\emptyset\|_\vartheta := 0$.
4. $\|v_i\|_\vartheta := \begin{cases} \square, & \text{if } \vartheta(i) = \square \\ \vartheta(i), & \text{else.} \end{cases}$

⁸ \square reads “undefined”

5. $\| \neg v_i \|_{\vartheta} := \begin{cases} \square, & \text{if } \vartheta(i) = \square \\ 1 - \vartheta(i), & \text{else.} \end{cases}$
6. $\| \varphi_1 \vee \dots \vee \varphi_s \|_{\vartheta} := \| \varphi_1 \|_{\vartheta} \vee \dots \vee \| \varphi_s \|_{\vartheta}.$
7. $\| \varphi_1 \wedge \dots \wedge \varphi_s \|_{\vartheta} := \| \varphi_1 \|_{\vartheta} \wedge \dots \wedge \| \varphi_s \|_{\vartheta},$ if $(\nexists i, j \in [s]) \varphi_i = \neg \varphi_j,$
otherwise $\| \varphi_1 \wedge \dots \wedge \varphi_s \|_{\vartheta} := 0.$
8. $\| D \|_{\vartheta} := \| F(D) \|_{\vartheta}, \| G \|_{\vartheta} := \| F(G) \|_{\vartheta}.$
9. $\| \mathcal{X} \|_{\vartheta} := \| F(\mathcal{X}) \|_{\vartheta}, \| \mathcal{Y} \|_{\vartheta} := \| F(\mathcal{Y}) \|_{\vartheta}.$

Lemma 16 $\| \varphi \|_{\vartheta} = \| \text{DN}(\varphi) \|_{\vartheta}$ holds for any $\varphi \in \mathcal{A}$ and $\vartheta \in \text{VA}.$

Proof. Consider induction step $\varphi = \sigma \wedge \tau$ where $\text{DN}(\sigma), \text{DN}(\tau) \neq \emptyset.$ So $\text{DN}(\varphi) = \text{DN}(\sigma) \odot \text{DN}(\tau) = \{ D \uplus E : \langle D, E \rangle \in \text{DN}(\sigma) \times \text{DN}(\tau) \},$ which yields
 $\| \text{DN}(\varphi) \|_{\vartheta} = \bigvee \{ \| D \uplus E \|_{\vartheta} : \langle D, E \rangle \in \text{DN}(\sigma) \times \text{DN}(\tau) \}$
 $= \bigvee \{ \| D^+ \cup E^+ \|_{\vartheta} \wedge \| D^- \cup E^- \|_{\vartheta} : D \in \text{DN}(\sigma) \ \& \ E \in \text{DN}(\tau) \}.$
(We omit possible occurrences of $D \uplus E = \emptyset$ for $(D^+ \cup E^+) \cap (D^- \cup E^-) \neq \emptyset,$ as in this case $\| D^+ \cup E^+ \|_{\vartheta} \wedge \| D^- \cup E^- \|_{\vartheta} = 0.$)

Below for the sake of brevity we assume $\| \varphi \|_{\vartheta} = 1$ (values 0, \square are treated analogously). So by the induction hypothesis we get

$$\begin{aligned}
& \| \text{DN}(\varphi) \|_{\vartheta} = 1 \Leftrightarrow (\exists D \in \text{DN}(\sigma)) (\exists E \in \text{DN}(\tau)) \\
& \quad \left[(D^+ \cup E^+) \cap (D^- \cup E^-) = \emptyset \ \& \right. \\
& \quad \left. (\forall v_i \in D^+ \cup E^+) \| v_i \|_{\vartheta} = 1 \ \& \ (\forall v_j \in D^- \cup E^-) \| v_j \|_{\vartheta} = 0 \right] \\
& \Leftrightarrow (\exists D \in \text{DN}(\sigma)) (\exists E \in \text{DN}(\tau)) \\
& \quad [(\forall v_i \in D^+ \cup E^+) \| v_i \|_{\vartheta} = 1 \ \& \ (\forall v_j \in D^- \cup E^-) \| v_j \|_{\vartheta} = 0] \\
& \Leftrightarrow (\exists D \in \text{DN}(\sigma)) [(\forall v_i \in D^+) \| v_i \|_{\vartheta} = 1 \ \& \ (\forall v_j \in E^-) \| v_j \|_{\vartheta} = 0] \ \& \\
& \quad (\exists E \in \text{DN}(\tau)) [(\forall v_i \in E^+) \| v_i \|_{\vartheta} = 1 \ \& \ (\forall v_j \in E^-) \| v_j \|_{\vartheta} = 0] \\
& \Leftrightarrow \| \text{DN}(\sigma) \|_{\vartheta} = 1 = \| \text{DN}(\tau) \|_{\vartheta} \\
& \Leftrightarrow \| \sigma \|_{\vartheta} = 1 = \| \tau \|_{\vartheta} \\
& \Leftrightarrow \| \tau \|_{\vartheta} = 1,
\end{aligned}$$

which yields $\| \sigma \wedge \tau \|_{\vartheta} = \| \text{DN}(\varphi) \|_{\vartheta}.$

Basis of induction and case $\varphi = \sigma \vee \tau$ are trivial. ■

Definition 17 For any $\varphi \in \mathcal{A}$ and $\mathcal{X}, \mathcal{Y} \subseteq \mathcal{D}$ let

$\mathcal{X} \sim \mathcal{Y} \Leftrightarrow (\forall \vartheta \in \text{VA}) \ \mathcal{X} \ _{\vartheta} = \ \mathcal{Y} \ _{\vartheta}$ $\mathcal{X} \approx \mathcal{Y} \Leftrightarrow (\forall \vartheta \in \text{VA}) (\ \mathcal{X} \ _{\vartheta} = 1 \Leftrightarrow \ \mathcal{Y} \ _{\vartheta} = 1)$ $\varphi \sim \mathcal{X} \Leftrightarrow \text{DN}(\varphi) \sim \mathcal{X}, \ \varphi \approx \mathcal{X} \Leftrightarrow \text{DN}(\varphi) \approx \mathcal{X}$

Obviously \sim and \approx are equivalences, \sim being stronger than $\approx.$ Moreover $\varphi \sim F(\text{DN}(\varphi))$ and $\mathcal{X} \sim \text{DN}(F(\mathcal{X})),$ and hence $\varphi \approx F(\text{DN}(\varphi))$ and $\mathcal{X} \approx \text{DN}(F(\mathcal{X})).$

3.4 Conclusion

Definition 18 $\boxed{B(\mathcal{X}) := \bigcap \{\mathcal{Y} \subseteq \mathcal{X} : (\forall X \in \mathcal{X}) (\exists Y \in \mathcal{Y}) Y \subseteq X\}}$ is called the base of a given $\mathcal{X} \subseteq \mathcal{D}$. Obviously $\mathcal{Y} \subseteq \mathcal{X}$ implies $B(\mathcal{Y}) \subseteq B(\mathcal{X}) \subseteq \mathcal{X}$ while $\mathcal{X} \subseteq B(\mathcal{X})$ implies $\mathcal{X} = B(\mathcal{X})$. A following lemma is easily verified.

Lemma 19 $\text{POS}_2 = B(\text{CLIQ}_2)$.

Lemma 20 For any $\mathcal{X}, \mathcal{Y} \subseteq \mathcal{D}$ the following conditions hold.

1. $\mathcal{X} \sim B(\mathcal{X})$, and hence $\mathcal{X} \approx B(\mathcal{X})$.
2. $\mathcal{X} \approx \mathcal{Y}$ implies $B(\mathcal{X}) = B(\mathcal{Y})$.

Proof. 1 is readily seen.

2. Suppose $\mathcal{X} \approx \mathcal{Y}$. By Definition 17, $\mathcal{X} \approx \mathcal{Y} \Leftrightarrow F(\mathcal{X}) \approx F(\mathcal{Y}) \Leftrightarrow$

$$\bigvee_{D \in \mathcal{X}} \left(\bigwedge_{\pi(i) \in D^+} v_i \wedge \bigwedge_{\pi(j) \in D^-} \neg v_j \right) \approx \bigvee_{E \in \mathcal{Y}} \left(\bigwedge_{\pi(i) \in E^+} v_i \wedge \bigwedge_{\pi(j) \in E^-} \neg v_j \right)$$

and $B(\mathcal{X}) \approx B(\mathcal{Y}) \Leftrightarrow F(B(\mathcal{X})) \approx F(B(\mathcal{Y})) \Leftrightarrow$

$$\bigvee_{D \in B(\mathcal{X})} \left(\bigwedge_{\pi(i) \in D^+} v_i \wedge \bigwedge_{\pi(j) \in D^-} \neg v_j \right) \approx \bigvee_{E \in B(\mathcal{Y})} \left(\bigwedge_{\pi(i) \in E^+} v_i \wedge \bigwedge_{\pi(j) \in E^-} \neg v_j \right)$$

Thus by 1, we have $F(B(\mathcal{X})) \approx F(B(\mathcal{Y}))$. So let $B(\mathcal{X}) = \{D_1, \dots, D_s\} \subseteq \mathcal{X}$ and $B(\mathcal{Y}) = \{E_1, \dots, E_t\} \subseteq \mathcal{Y}$ with $\bigvee_{r=1}^s F(D_r) \approx \bigvee_{r=1}^t F(E_r)$, which implies

$$(\forall x \in [s])(\exists y \in [t]) \text{DN}(E_y) \subseteq \text{DN}(D_x) \ \& \ (\forall y \in [t])(\exists x \in [s]) \text{DN}(D_x) \subseteq \text{DN}(E_y). \quad (*)$$

Indeed, for any $x \in [s]$, let $\vartheta \in \text{VA}$ be defined by $(\forall \pi(i) \in D_x^+) \vartheta(i) = 1$, $(\forall \pi(j) \in D_x^-) \vartheta(j) = 0$ and $(\forall \pi(i) \notin D_x^+ \cup D_x^-) \vartheta(i) = \square$. Then $1 = \|F(D_x)\|_{\vartheta} = \left\| \bigvee_{r=1}^s F(D_r) \right\|_{\vartheta}$. But then $\left\| \bigvee_{r=1}^t F(E_r) \right\|_{\vartheta} = 1$, i.e. there is $y \in [t]$ such that $\|F(E_y)\|_{\vartheta} = 1$, which yields $(\forall \pi(i) \in E_y^+) \vartheta(i) = 1$, $(\forall \pi(j) \in E_y^-) \vartheta(j) = 0$ and hence $\text{DN}(E_y) \subseteq \text{DN}(D_x)$. The inversion $(\forall y \in [t])(\exists x \in [s]) \text{DN}(D_x) \subseteq \text{DN}(E_y)$ is analogous. By the \subseteq -minimality of $B(\mathcal{X})$ and $B(\mathcal{Y})$, the conjunction $(*)$ yields $B(\mathcal{X}) = B(\mathcal{Y})$. ■

Lemma 21 Suppose that $\varphi \in \mathcal{A}$ satisfies $\varphi \approx \text{CLIQ}_2$. Then $\text{POS}_2 = \text{AC}^p(\varphi)$ and $\text{AC}^n(\varphi) = \emptyset$. Hence by Theorem 14, $\text{cs}(\varphi) > m^{\frac{1}{5}m^{\frac{1}{30}}}$ holds for sufficiently large m .

Proof. By Lemmata 16, 19, 20, $\varphi \approx \text{CLIQ}_2$ successively implies $\text{DN}(\varphi) \approx \text{CLIQ}_2$ and $\text{POS}_2 = \text{B}(\text{DN}(\varphi)) \subseteq \text{DN}(\varphi)$. By Lemma 3 (2) this yields $\text{POS}_2 = \text{AC}^P(\text{POS}_2) \subseteq \text{AC}^P(\varphi) \subseteq \text{POS}_2$ and hence $\text{POS}_2 = \text{AC}^P(\varphi)$. Now suppose there is a $C_{(f,g)} \in \text{AC}^N(\varphi)$, i.e. there exists $D \in \text{DN}(\varphi)$ such that $D^+ \subseteq C_f$ and $D^- \subseteq C_g$. But then there exists $E \in \text{B}(\text{DN}(\varphi)) = \text{POS}_2$ such that $\mathcal{K} \ni E^+ \subseteq C_f$ and $\mathcal{K} \ni E^- \subseteq C_g$, which contradicts Lemma 1. Thus $\text{AC}^N(\varphi) = \emptyset$, as required. ■

Corollary 22 *Suppose that $\varphi \in \mathcal{A}$ provides a solution of CLIQ_2 in the DMN logic. Then for sufficiently large $m \geq k^{15}$, $\text{cs}(\varphi) > m^{\frac{1}{5}m^{\frac{1}{30}}} = k^{\frac{1}{5}\sqrt{k}}$.*

3.5 General Boolean case

- Let \mathcal{B} denote full Boolean (also called DeMorgan) algebra with constants \top, \perp , operations \vee, \wedge, \neg and variables $\text{VAR} = \{v_1, \dots, v_n\}$.

Recall that arbitrary Boolean formulas $\varphi \in \mathcal{B}$ are convertible to equivalent DMN $\varphi^* \in \mathcal{A}$ obtained by applying standard DeMorgan rules 1–4.

1. $\neg\top \leftrightarrow \perp, \neg\perp \leftrightarrow \top$.
2. $\neg(\sigma \vee \tau) \leftrightarrow \neg\sigma \wedge \neg\tau$.
3. $\neg(\sigma \wedge \tau) \leftrightarrow \neg\sigma \vee \neg\tau$.
4. $\neg\neg\varphi \leftrightarrow \varphi$.

Every φ^* obviously preserves conventional tree-like structure and standard (linear) length of φ . Consider dag-like structures and corresponding circuit sizes. It is a folklore that circuit size of φ^* at most doubles that of φ , i.e.

Lemma 23 $\text{cs}(\varphi^*) \leq 2\text{cs}(\varphi)$ holds for any $\varphi \in \mathcal{B}$.

Proof. See e.g. Appendix D. ■

Theorem 24 *Suppose that $\varphi \in \mathcal{B}$ provides a solution of CLIQ_2 in full Boolean logic. Then for sufficiently large $m \geq k^{15}$, $\text{cs}(\varphi) > m^{\frac{1}{5}m^{\frac{1}{30}}} = k^{\frac{1}{5}\sqrt{k}}$.*

Proof. This follows directly from Corollary 21 and Lemma 22 via $\varphi^* \approx \text{CLIQ}_2$ as in Theorem 14 (cf. also Appendix C). ■

Theorem 25 CLIQ_2 is not solvable by polynomial-size Boolean circuits. In fact, algorithmic solutions of CLIQ_2 require exponential-size boolean circuits.

Proof. Consider two disjoint sets of variables $\{x_1, \dots, x_n\}$ and $\{y_1, \dots, y_n\}$ (as positive and negative variables, respectively). Boolean circuits C with gates \vee, \wedge, \neg are supplied with standard semantic determined by (consistent) Boolean assignments $\beta : \{x_1, \dots, x_n, y_1, \dots, y_n\} \rightarrow \{0, 1\}$, $\{i \in [n] : \beta(x_i) = \beta(y_i) = 1\} = \emptyset$, such that inputs are double graphs whose positive and negative parts are

determined by positive and negative variables assigned with Boolean value 1. I.e., with every Boolean assignment β in question we correlate double graph

$$D[\beta] := \langle \{\pi(i) : \beta(x_i) = 1\}, \{\pi(j) : \beta(y_j) = 1\} \rangle \in \mathcal{D}.$$

Define $f : \mathcal{D} \rightarrow \{0, 1\}$ by $f(D) = 1 \Leftrightarrow D \in \text{CLIQ}_2$ and suppose that f is computable by a polynomial-size Boolean circuit C . Thus $\text{cs}(C) = \mathcal{O}(m^c)$ for a fixed $c > 0$. Also let $g(\beta) := f(D[\beta]) \in \{0, 1\}$. Hence

$$g(\beta) = 1 \Leftrightarrow f(D[\beta]) = 1 \Leftrightarrow D[\beta] \in \text{CLIQ}_2$$

holds for any Boolean assignment $\beta : \{x_1, \dots, x_n, y_1, \dots, y_n\} \rightarrow \{0, 1\}$, while g is expressible by a suitable Boolean formula with variables from the list $\{x_1, \dots, x_n, y_1, \dots, y_n\}$ whose circuit size is polynomial in m .

Now turning to our 3-valued semantic (cf. 3.3.2), for any $\vartheta \in \text{VA}$ we let

$$D[\vartheta] := \langle \{\pi(i) : \vartheta(i) = 1\}, \{\pi(j) : \vartheta(j) = 0\} \rangle \in \mathcal{D}$$

and note that $D[\vartheta] = D[\beta[\vartheta]]$, where the assignment $\beta[\vartheta]$ is given by

$$(\beta[\vartheta])(x_i) := \begin{cases} 1, & \text{if } \vartheta(i) = 1 \\ 0, & \text{else,} \end{cases} \quad \text{and } (\beta[\vartheta])(y_j) := \begin{cases} 1, & \text{if } \vartheta(j) = 0 \\ 0, & \text{else.} \end{cases}$$

Furthermore let $h(\vartheta) := g(\beta[\vartheta])$. Thus for any $\vartheta \in \text{VA}$ we have

$$\begin{aligned} h(\vartheta) &= 1 \Leftrightarrow g(\beta[\vartheta]) = 1 \Leftrightarrow \\ &f(D[\beta[\vartheta]]) = 1 \Leftrightarrow f(D[\vartheta]) = 1 \\ &\Leftrightarrow D[\vartheta] \in \text{CLIQ}_2. \end{aligned}$$

Moreover $h : \text{VA} \rightarrow \{0, 1\}$ is expressible by $\psi = \varphi^* \in \mathcal{A}$ for a suitable formula $\varphi \in \mathcal{B}$ such that $\text{cs}(\psi)$ is polynomial in m . Thus

$$(\forall \vartheta \in \text{VA}) (\|\psi\|_{\vartheta} = 1 \Leftrightarrow h(\vartheta) = 1)$$

which for any $\vartheta \in \text{VA}$ yields

$$\begin{aligned} \|\psi\|_{\vartheta} = 1 &\Leftrightarrow D[\vartheta] \in \text{CLIQ}_2 \Leftrightarrow \\ &(\exists D \in \text{CLIQ}_2) \|D\|_{\vartheta} = 1 \\ &\Leftrightarrow \|\text{CLIQ}_2\|_{\vartheta} = 1, \end{aligned}$$

i.e. $\psi \approx \text{CLIQ}_2$. Hence by Theorem 14, $\text{cs}(\psi) > m^{\frac{1}{5}m^{\frac{1}{30}}}$ for $m \gg 2$. But $\text{cs}(\psi) = \mathcal{O}(m^d)$ for a fixed $d > 0$ – a contradiction. The same argument shows that any Boolean solution of CLIQ_2 requires exponential-size circuits. ■

Corollary 26 *Since CLIQ_2 is a **NP** problem, $\text{NP} \not\subseteq \text{P/poly}$ is the case. In particular $\text{P} \subsetneq \text{NP}$ and hence $\text{P} \neq \text{NP}$.*

Proof. Boolean circuit complexity is quadratic in deterministic time (cf. e.g. [3]: Proposition 11.1, [7]: Theorem 9.30). Hence the assertion easily follows from Theorem 24 as CLIQ_2 is NP complete. ■

Remark 27 Our double-graph generalization of plain-graph approach used in standard proofs for monotone circuits (formulas) leads to a more sophisticated “non-monotone” approximations than the ones discussed in [6]. For consider a following plain-graph problem CLIQ_2^* : Given a natural number $k > 2$ and a subgraph G of a fixed graph H on k^{15} vertices decide whether G and complement $H \setminus G$ both contain k -cliques. Obviously CLIQ_2^* is an instance of CLIQ_2 . Now CLIQ_2^* is solvable by iterating plain-graph solutions of the monotone problem CLIQ (first ask if G contains a k -clique and if the answer is “yes” then ask if $H \setminus G$ also contains a k -clique). However CLIQ_2^* is not monotone, since G and $H \setminus G$ both containing (disjoint) k -cliques does not necessarily infer the same for any G' and corresponding $H \setminus G'$, provided that $G \subset G'$. Thus standard “monotone” approach is not applicable to CLIQ_2^* (and hence to CLIQ_2).⁹

3.6 Application

Denote by \mathcal{A}_0 positive (monotone) subalgebra of \mathcal{A} . Thus formulas in \mathcal{A}_0 are built up from variables and constants by positive operations \vee and \wedge . So CNF and/or DNF formulas $\varphi \in \mathcal{A}_0$ don’t include negated variables.

Theorem 28 *There is no polynomial time algorithm f converting arbitrary CNF formulas $\varphi \in \mathcal{A}$ (or just CNF $\varphi \in \mathcal{A}_0$) into equivalent DNF formulas $f(\varphi) \in \mathcal{A}$.*

Proof. Suppose $(\forall \vartheta \in \text{VA}) (\|\varphi\|_{\vartheta} = 1 \Leftrightarrow \|f(\varphi)\|_{\vartheta} = 1 \Leftrightarrow \|\neg f(\varphi)\|_{\vartheta} = 0)$. Thus $\varphi \in \text{SAT} \Leftrightarrow f(\varphi) \in \text{SAT} \Leftrightarrow \neg f(\varphi) \notin \text{TAU}$, while by the assumption the size of $f(\varphi)$ is polynomial in that of φ . Now $\neg f(\varphi) \in \mathcal{B}$ is equivalent to CNF formula $(\neg f(\varphi))^* \in \mathcal{A}$ whose size is roughly the same as that of $f(\varphi)$, and hence polynomial in the size of φ .¹⁰ Now general CNF validity problem $(\neg f(\varphi))^* \in^? \text{TAU}$ is solvable in polynomial time. Hence so is the satisfiability problem $\varphi \in^? \text{SAT}$. By the NP completeness of SAT this yields $\mathbf{P} = \mathbf{NP}$, – a contradiction. ■

References

- [1] A. E. Andreev, *A method for obtaining lower bounds on the complexity of individual monotone functions*, Dokl. Akad. Nauk SSSR 282:5, 1033–1037 (1985), Engl. transl. in Soviet Math. Doklady 31, 530–534
- [2] R. B. Boppana, M. Sipser, *The complexity of finite functions*, in: **Handbook of Theoretical Computer Science A: Algorithms and Complexity**, 758–804, MIT Press (1990)

⁹Recall that there are monotone problems in \mathbf{P} (e.g. PERFECT MATCHING) that require exponential-size monotone circuits (cf. [5], [9]).

¹⁰The difference between plain (linear) and circuit length is inessential for CNF and/or DNF formulas under consideration.

- [3] C. H. Papadimitriou, **Computational Complexity**, Addison-Wesley (1995)
- [4] A. A. Razborov, *Lower bounds for the monotone complexity of some Boolean functions*, Dokl. Akad. Nauk SSSR 281:4, 798–801 (1985), Engl. transl. in Soviet Math. Doklady 31, 354–357 (1985)
- [5] A. A. Razborov, *Lower bounds on monotone complexity of the logical permanent*, Mat. Zametki 37:6, 887–900 (1985), Engl. transl. in Mat. Notes of the Acad. of Sci. of the USSR 37, 485–493 (1985)
- [6] A. A. Razborov, *On the method of approximation*, Proc. of the 21st Annual Symposium on Theory of Computing, 167–176 (1989)
- [7] M. Sipser, **Introduction to the Theory of Computation**, PWS Publishing (1997)
- [8] Yuh-Dauh Lyuu, *P vs. NP*, <https://www.csie.ntu.edu.tw/~lyuu/complexity/2021/20220106.pdf>
- [9] É. Tardos, *The gap between monotone and non-monotone circuit complexity is exponential*, Combinatorica 8:1, 141–142 (1988)
- [10] P. Erdős, R. Rado, *Intersection theorems for systems of sets*, Journal of London Math. Society 35, 85–90 (1960)

4 Appendix A: On $|\mathcal{R}_{\subseteq}(A, G)|$

Let $A \subseteq [m]$, $|A| \geq 2$, $G \in \mathcal{G}^\ell$, $\mathcal{R}_{\subseteq}(A, G) = \{f \in \mathcal{F} : \text{Dom}^\circ(f) = A \& G \subseteq C_f\}$. We calculate the probability that a given coloring function $f \in \mathcal{F} : \text{Dom}^\circ(f) = A$ is in $\mathcal{R}_{\subseteq}(A, G)$, i.e. every pair of nodes x, y connected by an edge in G is colored differently by $f(x) \neq f(y) < k$. Thus to color every next node in $\mathcal{V}(G)$ we have to choose an arbitrary color among those not previously used. This yields the probability

$$\frac{k-1}{k-1} \cdot \frac{k-2}{k-1} \cdots \frac{k-1-|\mathcal{V}(G)|}{k-1} > \left(\frac{k-1-|\mathcal{V}(G)|}{k-1} \right)^{|\mathcal{V}(G)|} \geq \left(1 - \frac{\ell}{k-1} \right)^\ell \geq \left(1 - \frac{\ell}{k} \right)^\ell = \left(1 - \frac{1}{2\ell} \right)^\ell \rightarrow \frac{1}{\sqrt{e}} > \frac{1}{2} \text{ as } k = 2\ell^2 \rightarrow \infty.$$

Hence $|\mathcal{R}_{\subseteq}(A, G)| \geq \frac{1}{2} |\{f \in \mathcal{F} : \text{Dom}^\circ(f) = A\}| = \frac{1}{2} (k-1)^{|A|}$ for large k .

5 Appendix B: Proof of Lemma 12

We use Lemma 3 and boolean inclusion $A \setminus B \subseteq (A \setminus C) \cup (C \setminus B)$.

$$\begin{aligned} 1. \quad \partial^P(\sigma \vee \tau) &= \text{AC}^P(\text{DN}(\sigma) \cup \text{S}(\tau)) \setminus \text{AC}^P(\text{AP}(\sigma) \sqcup \text{AP}(\tau)) \\ &\subseteq \text{AC}^P(\text{DN}(\sigma) \cup \text{DN}(\tau)) \setminus [\text{AC}^P(\text{AP}(\sigma)) \cup \text{AC}^P(\text{AP}(\tau))] \cup \end{aligned}$$

$$\begin{aligned}
& [\text{AC}^{\text{P}}(\text{AP}(\sigma)) \cup \text{AC}^{\text{P}}(\text{AP}(\tau))] \setminus \text{AC}^{\text{P}}(\text{AP}(\sigma) \sqcup \text{AP}(\tau)) \\
&= [\text{AC}^{\text{P}}(\sigma) \cup \text{AC}^{\text{P}}(\tau)] \setminus [\text{AC}^{\text{P}}(\text{AP}(\sigma)) \cup \text{AC}^{\text{P}}(\text{AP}(\tau))] \cup \\
&\quad [\text{AC}^{\text{P}}(\text{AP}(\sigma)) \cup \text{AC}^{\text{P}}(\text{AP}(\tau))] \setminus \text{AC}^{\text{P}}(\text{AP}(\sigma) \sqcup \text{AP}(\tau)) \\
&\subseteq [\text{AC}^{\text{P}}(\sigma) \setminus \text{AC}^{\text{P}}(\text{AP}(\sigma))] \cup [\text{AC}^{\text{P}}(\tau) \setminus \text{AC}^{\text{P}}(\text{AP}(\tau))] \cup \\
&\quad [\text{AC}^{\text{P}}(\text{AP}(\sigma)) \cup \text{AC}^{\text{P}}(\text{AP}(\tau))] \setminus \text{AC}^{\text{P}}(\text{AP}(\sigma) \sqcup \text{AP}(\tau)) \\
&= \partial^{\text{P}}(\sigma) \cup \partial^{\text{P}}(\tau) \cup \partial_{\sqcup}^{\text{P}}(\text{AP}(\sigma), \text{AR}(\tau)). \\
2. \quad & \partial^{\text{P}}(\sigma \wedge \tau) = \text{AC}^{\text{P}}(\text{DN}(\sigma) \odot \text{DN}(\tau)) \setminus \text{AC}^{\text{P}}(\text{AP}(\sigma) \sqcap \text{AP}(\tau)) \\
&\subseteq \text{AC}^{\text{P}}(\text{DN}(\sigma) \odot \text{DN}(\tau)) \setminus [\text{AC}^{\text{P}}(\text{AP}(\sigma)) \cap \text{AC}^{\text{P}}(\text{AP}(\tau))] \cup \\
&\quad [\text{AC}^{\text{P}}(\text{AP}(\sigma)) \cap \text{AC}^{\text{P}}(\text{AP}(\tau))] \setminus \text{AC}^{\text{P}}(\text{AP}(\sigma) \sqcap \text{AP}(\tau)) \\
&= [\text{AC}^{\text{P}}(\sigma) \cap \text{AC}^{\text{P}}(\tau)] \setminus [\text{AC}^{\text{P}}(\text{AP}(\sigma)) \cap \text{AC}^{\text{P}}(\text{AP}(\tau))] \cup \\
&\quad [\text{AC}^{\text{P}}(\text{AP}(\sigma)) \cap \text{AC}^{\text{P}}(\text{AP}(\tau))] \setminus \text{AC}^{\text{P}}(\text{AP}(\sigma) \sqcap \text{AP}(\tau)) \\
&\subseteq \text{AC}^{\text{P}}(\sigma) \setminus \text{AC}^{\text{P}}(\text{AP}(\sigma)) \cup \text{AC}^{\text{P}}(\tau) \setminus \text{AC}^{\text{P}}(\text{AP}(\tau)) \cup \\
&\quad \partial_{\sqcap}^{\text{P}}(\text{AP}(\sigma), \text{AR}(\tau)) \\
&= \partial^{\text{P}}(\sigma) \cup \partial^{\text{P}}(\tau) \cup \partial_{\sqcap}^{\text{P}}(\text{AP}(\sigma), \text{AR}(\tau)). \\
3. \quad & \partial^{\text{N}}(\sigma \vee \tau) = \text{AC}^{\text{N}}(\text{AP}(\sigma) \sqcup \text{AP}(\tau)) \setminus \text{AC}^{\text{N}}(\text{DN}(\sigma) \cup \text{DN}(\tau)) \\
&\subseteq \text{AC}^{\text{N}}(\text{AP}(\sigma) \sqcup \text{AP}(\tau)) \setminus [\text{AC}^{\text{N}}(\text{AP}(\sigma)) \cup \text{AC}^{\text{N}}(\text{AP}(\tau))] \cup \\
&\quad [\text{AC}^{\text{N}}(\text{AP}(\sigma)) \cup \text{AC}^{\text{N}}(\text{AP}(\tau))] \setminus \text{AC}^{\text{N}}(\text{DN}(\sigma) \cup \text{DN}(\tau)) \\
&= \text{AC}^{\text{N}}(\text{AP}(\sigma) \sqcup \text{AP}(\tau)) \setminus [\text{AC}^{\text{N}}(\text{AP}(\sigma)) \cup \text{AC}^{\text{N}}(\text{AP}(\tau))] \cup \\
&\quad [\text{AC}^{\text{N}}(\text{AP}(\sigma)) \cup \text{AC}^{\text{N}}(\text{AP}(\tau))] \setminus [\text{AC}^{\text{N}}(\sigma) \cup \text{AC}^{\text{N}}(\tau)] \\
&\subseteq \partial_{\sqcup}^{\text{N}}(\text{AP}(\sigma), \text{AR}(\tau)) \cup \text{AC}^{\text{N}}(\text{AP}(\sigma)) \setminus \text{AC}^{\text{N}}(\sigma) \cup \text{AC}^{\text{N}}(\text{AP}(\tau)) \setminus \text{AC}^{\text{N}}(\tau) \\
&= \partial_{\sqcup}^{\text{N}}(\text{AP}(\sigma), \text{AR}(\tau)) \cup \partial^{\text{N}}(\sigma) \cup \partial^{\text{N}}(\tau). \\
4. \quad & \partial^{\text{N}}(\sigma \wedge \tau) = \text{AC}^{\text{N}}(\text{AP}(\sigma) \sqcap \text{AP}(\tau)) \setminus \text{AC}^{\text{N}}(\text{DN}(\sigma) \odot \text{DN}(\tau)) \\
&\subseteq \text{AC}^{\text{N}}(\text{AP}(\sigma) \sqcap \text{AP}(\tau)) \setminus [\text{AC}^{\text{N}}(\text{AP}(\sigma)) \cap \text{AC}^{\text{N}}(\text{AP}(\tau))] \cup \\
&\quad [\text{AC}^{\text{N}}(\text{AP}(\sigma)) \cap \text{AC}^{\text{N}}(\text{AP}(\tau))] \setminus \text{AC}^{\text{N}}(\text{DN}(\sigma) \odot \text{DN}(\tau)) \\
&= \text{AC}^{\text{N}}(\text{AP}(\sigma) \sqcap \text{AP}(\tau)) \setminus [\text{AC}^{\text{N}}(\text{AP}(\sigma)) \cap \text{AC}^{\text{N}}(\text{AP}(\tau))] \cup \\
&\quad [\text{AC}^{\text{N}}(\text{AP}(\sigma)) \cap \text{AC}^{\text{N}}(\text{AP}(\tau))] \setminus [\text{AC}^{\text{N}}(\sigma) \cap \text{AC}^{\text{N}}(\tau)] \\
&\subseteq \partial_{\sqcap}^{\text{N}}(\text{AP}(\sigma), \text{AR}(\tau)) \cup \text{AC}^{\text{N}}(\text{AP}(\sigma)) \setminus \text{AC}^{\text{N}}(\sigma) \cup \text{AC}^{\text{N}}(\text{AP}(\tau)) \setminus \text{AC}^{\text{N}}(\tau) \\
&= \partial_{\sqcap}^{\text{N}}(\text{AP}(\sigma), \text{AR}(\tau)) \cup \partial^{\text{N}}(\sigma) \cup \partial^{\text{N}}(\tau).
\end{aligned}$$

■

6 Appendix C: Basic inequalities

We have $k = 2\ell^2 = m^{\frac{1}{15}}$, $p = \ell \log_{\frac{4}{3}} m$, $L = (p-1)^{3\ell} \ell!$, $m \gg 0$.

$$\ell! \sim \sqrt{2\pi\ell} \left(\frac{\ell}{e}\right)^{\ell} = \sqrt{\sqrt{2\pi} m^{\frac{1}{30}}} \left(\frac{\frac{1}{\sqrt{2}} m^{\frac{1}{30}}}{\sqrt{2}e}\right)^{\frac{1}{\sqrt{2}} m^{\frac{1}{30}}} < \sqrt{\sqrt{2\pi}} m^{\frac{1}{60} + \frac{1}{30\sqrt{2}} m^{\frac{1}{30}}} (\sqrt{2}e)^{\frac{1}{\sqrt{2}} m^{\frac{1}{30}}}$$

$$\begin{aligned}
&< m^{\frac{1}{30\sqrt{2}}} m^{\frac{1}{30}} < m^{\frac{1}{30}} m^{\frac{1}{30}} \text{ holds for sufficiently large } m \text{ (via} \\
&\sqrt{\sqrt{2}\pi} \cdot m^{\frac{1}{2}\alpha} \cdot m^{\beta m^\alpha} < (\sqrt{2}e)^{\beta m^\alpha} \cdot m^{\beta m^\alpha} \Leftrightarrow \sqrt{\sqrt{2}\pi} \cdot m^{\frac{1}{2}\alpha} < (\sqrt{2}e)^{\beta m^\alpha} \\
&\Leftrightarrow \ln \sqrt{\sqrt{2}\pi} + \frac{1}{2}\alpha \ln n < \frac{3}{2}\beta n^\alpha.
\end{aligned}$$

Now $p = \ell \log_{\frac{4}{3}} m < m^{\frac{1}{30}+\varepsilon}$ and hence $(p-1)^{3\ell} < p^{3\ell} < m^{(\frac{1}{10}+\varepsilon)m^{\frac{1}{30}}}$ holds for sufficiently small $\varepsilon > 0$.

$$\text{Hence } L = (p-1)^{3\ell} \ell! < m^{(\frac{1}{10}+\varepsilon)m^{\frac{1}{30}}} m^{\frac{1}{30}} m^{\frac{1}{30}} < m^{\frac{1}{7}m^{\frac{1}{30}}}, \quad L^2 < m^{\frac{2}{7}m^{\frac{1}{30}}}.$$

$$\text{So } \left(\frac{m-\ell}{k}\right)^\ell = \left(\frac{m - \frac{1}{\sqrt{2}}m^{\frac{1}{30}}}{m^{\frac{1}{15}}}\right)^{\frac{1}{\sqrt{2}}m^{\frac{1}{30}}} > \left(m^{\frac{14}{15}} - 1\right)^{\frac{1}{\sqrt{2}}m^{\frac{1}{30}}} > m^{\frac{9}{15}m^{\frac{1}{30}}},$$

$$\left(\frac{m-\ell}{k}\right)^\ell L^{-2} > \frac{m^{\frac{9}{15}m^{\frac{1}{30}}}}{m^{\frac{2}{7}m^{\frac{1}{30}}}} > m^{\frac{1}{5}m^{\frac{1}{30}}} \text{ and}$$

$$\frac{1}{8} \left(\frac{4}{3}\right)^p L^{-2} > \frac{1}{8} \frac{m^{\frac{1}{\sqrt{2}}m^{\frac{1}{30}}}}{m^{\frac{2}{7}m^{\frac{1}{30}}}} > m^{\frac{1}{5}m^{\frac{1}{30}}}.$$

7 Appendix D: Proof of Lemma 23

Proof. For brevity we switch to circuit formalism. Consider any Boolean circuit (i.e. rooted *dag*) B whose leaves and other (inner) vertices are labeled with elements of $\text{VAR} \cup \{\top, \perp\}$ and $\{\vee, \wedge, \neg\}$, respectively. To put it in formal terms we let $B = \langle V, E, \lambda \rangle$ where $V \subset^{fin} \mathbb{N}$ and $E \subset \{\langle x, y \rangle : x < y \in V\}$ are the vertices and (bottom-up directed) edges, respectively, while $\lambda : V \rightarrow \text{VAR} \cup \{\top, \perp, \vee, \wedge, \neg\}$ and $0 \in V$ being the labeling function and the root (i.e. bottom) of B . Thus $\langle \lambda(x), \lambda(y) \rangle$ with $\langle x, y \rangle \in E$ are the labeled edges. Moreover we assume that each inner vertex $x \in V$ with label $\lambda(x) \in \{\vee, \wedge\}$ or $\lambda(x) = \neg$ has respectively two or just one successor(s) $y \in B$, $\langle x, y \rangle \in E$, $\lambda(y) \neq \neg$. To determine the required De-Morgan circuit $B^* = \langle V^*, E^*, \lambda^* \rangle$ we first stipulate $W := \{0 \neq x \in V : \lambda(x) \neq \neg\}$ and let W_1 be a disjoint copy of W together with dual labeling function $\lambda_1 : W_1 \rightarrow \text{VAR}^* \cup \{\top, \perp, \vee, \wedge\}$ defined by $\lambda_1(x) := \lambda(x)^*$ where $v_j^* = \neg v_j$, $\top^* = \perp$, $\perp^* := \top$, $\vee^* = \wedge$ and $\wedge^* = \vee$ (thus $\text{VAR}^* = \{\neg v_1, \dots, \neg v_n\}$). $x_1 \sim x$ will express that x_1 is a copy of $x \in W$ in W_1 . Now let $V_0^* := \{r\} \cup W \cup W_1$, where $r = 0$, if $0 \in W$, else $r \notin W \cup W_1$, and let $\lambda^* : V_0^* \rightarrow \text{VAR} \cup \{\top, \perp, \vee, \wedge\}$ extend $\lambda \cup \lambda_1$ by $\lambda^*(r) := \begin{cases} \lambda(0), & \text{if } 0 \in W, \\ \lambda(x)^*, & \text{if } \langle 0, x \rangle \in E \text{ \& } \lambda(0) = \neg. \end{cases}$ Crude structure of $E^* \subset V^* \times V^*$ is determined by defining clauses 1–4, while using in 3, 4 an abbreviation $\langle x, y \rangle \in \neg E \Leftrightarrow (\exists z \in V) (\lambda(z) = \neg \wedge \langle x, z \rangle \in E \wedge \langle z, y \rangle \in E)$.

1. Suppose $x, y \in W$. Then $\langle x, y \rangle \in E^* \Leftrightarrow \langle x, y \rangle \in E$.

2. Suppose $x_1, y_1 \in W_1$, $x_1 \sim x \in W$ and $y_1 \sim y \in W$.

Then $\langle x_1, y_1 \rangle \in E^* \Leftrightarrow \langle x, y \rangle \in E$.

3. Suppose $x \in W$, $y_1 \in W_1$, $y_1 \sim y \in W$ and $\langle x, y \rangle \in_{\neg} E$.
Then $\langle x, y_1 \rangle \in E^* \Leftrightarrow \langle x, y \rangle \in E$.
4. Suppose $x_1 \in W_1$, $y \in W$, $x_1 \sim x \in W$ and $\langle x, y \rangle \in_{\neg} E$.
Then $\langle x_1, y \rangle \in E^* \Leftrightarrow \langle x, y \rangle \in E$.

To complete the entire definition we assert r to be the root of B^* , i.e. let V^* be the subset of V_0^* whose vertices are reachable from r by chains of edges occurring in E^* . Obviously $|V^*| \leq 2|V|$. It remains to verify the correctness of conversion $B \hookrightarrow B^*$, i.e., that B^* is dag-like presentation of φ^* provided that B is dag-like presentation of φ . To this end note that defining clauses 1–4 imitate conversions 1–3 of $\varphi \hookrightarrow \varphi^*$. The operations (Boolean connectives) correspond to the labels $\lambda(-)$ and $\lambda^*(-)$, respectively. Vertices of W correspond to “positive” gates (subformulas) that remain unchanged, whereas those of W_1 are “negative” ones that are dual to “positive” origins (these occur within the odd number of \neg -scopes); both “positive” and “negative” gates can occur simultaneously due to underlying dag-like structure of B . The crucial observation: every original gate in B requires at most one dual gate occurring in B^* . This yields the required estimate $\text{cs}(\varphi^*) \leq 2\text{cs}(\varphi)$ (for brevity we omit further details). ■