

# On P Versus NP <sup>1</sup>

L. Gordeev

lew.gordeew@uni-tuebingen.de

Dec. 2020

**Abstract.** I generalize a well-known result that  $\mathbf{P} = \mathbf{NP}$  fails for monotone polynomial circuits – more precisely, that the clique problem  $\text{CLIQUE}(k^4, k)$  is not solvable by Boolean  $(\vee, \wedge)$ -circuits of size polynomial in  $k$  (cf. [1]–[9], et al). In the other words, there is no  $(\vee, \wedge)$ -formula  $\varphi$  with  $\binom{k^4}{2}$  Boolean variables expressing that a given graph with  $k^4$  vertices contains a clique of  $k$  elements, provided that the circuit size  $|\varphi|$  (= total number of pairwise distinct subformulas of  $\varphi$ ) is polynomial in  $k$ . In fact, for any solution  $\varphi$  in question,  $|\varphi|$  is exponential in  $k$ . Using a more sophisticated logical framework I extrapolate this result onto DeMorgan normal (DMN)  $(\vee, \wedge)$ -formulas  $\varphi$  that allow negated variables. Based on the latter observation I consider an arbitrary Boolean formula  $\varphi$  and recall that standard  $\neg$ -conversions to DMN at most double its circuit size. Hence for any Boolean solution  $\varphi$  of  $\text{CLIQUE}(k^4, k)$ ,  $|\varphi|$  is exponential in  $k$ . Thus  $\text{CLIQUE}(k^4, k)$  is not solvable by polynomial-size Boolean circuits, and hence  $\mathbf{P} \neq \mathbf{NP}$ . The entire proof is formalizable by standard methods in the exponential function arithmetic **EFA**.

## 1 Introduction and survey of contents

The paper deals with the open problem **P versus NP** <sup>2</sup>. Arguing in favor of  $\mathbf{P} \neq \mathbf{NP}$  let us recall three familiar observations (cf. e.g. [4], [8]):

- (A) The well-known graph theoretic problem **CLIQUE** is NP-complete. Thus in order to prove  $\mathbf{P} \neq \mathbf{NP}$  it will suffice e.g. to show that for sufficiently large natural number  $k$  there is no Boolean circuit  $C$  of  $k$ -polynomial size expressing that a given graph with  $k^4$  vertices has a clique of  $k$  elements; this particular case of **CLIQUE** we'll abbreviate as  $\text{CLIQUE}(k^4, k)$ .
- (B)  $\mathbf{P} = \mathbf{NP}$  fails for monotone polynomial-size circuits. More precisely,  $\mathbf{P} \neq \mathbf{NP}$  holds for  $\text{CLIQUE}(k^4, k)$  with respect to monotone, i.e. negation-free  $(\vee, \wedge)$ -circuits only. Moreover, the size of monotone solutions  $C$  of  $\text{CLIQUE}(k^4, k)$  in question is exponential in  $k$ .
- (C) Computational complexity of Boolean circuits is linear in that of DeMorgan normal (abbr.: DMN) circuits that enrich monotone circuits by negated inputs.

Summing up, in order to prove  $\mathbf{P} \neq \mathbf{NP}$  it would suffice to show that for sufficiently large natural number  $k$  there is no DMN-circuit solution  $C$  of  $\text{CLIQUE}(k^4, k)$  whose size is polynomial in  $k$ . The paper implements this idea and generalizes monotone approach of (B) [§§2, 3] while modifying its method of approximation. Moreover, aside from plain graphs, it deals with *double graphs*

<sup>1</sup>It is a slight extension of arXiv.org/pdf/2005.00809.pdf.

<sup>2</sup>See e.g. [https://en.wikipedia.org/wiki/P\\_versus\\_NP\\_problem](https://en.wikipedia.org/wiki/P_versus_NP_problem).

(= pairs of disjoint graphs consisting of positive and negative parts thereof) and – instead of circuits and related considerations – Boolean formulas and standard formalism of Boolean algebra in which DMN formulas are converted to “large” (locally consistent) disjunctive normal forms (DNFs) and special “small” DNFs, called approximations. Erdős-Rado lemma is applied to positive parts of double graphs. Useless probabilistic background of the monotone approach is neglected while estimating deviations between total numbers of canonical test graphs POS and NEG accepted (rejected) by formulas and their approximations [Lemma 12]. Estimates thus obtained show that the (circuit) size of any formula  $\varphi$  that behaves correctly on the test graphs is at least exponential in  $k$  [Theorem 13]. A suitable semantic approach shows that the assumptions of Theorem 13 are fulfilled by any affirmative DMN solution  $\varphi$  of  $\text{CLIQUE}(k^4, k)$  [Theorem 22]. Together with (C) this yields the result.

The paper should demonstrate that a desired proof of  $\mathbf{P} \neq \mathbf{NP}$  does not necessarily require new groundbreaking ideas. Instead, it suffices to carefully analyze already known techniques in a more sophisticated Boolean framework. In comparison with standard monotone approach (B), there are three basic novelties.

1. Double graphs enable to consider monotone circuits enriched by negated inputs (equivalently: positive Boolean formulas with atomic negation). Namely, sets of double (plain) graphs are viewed as the DNFs containing corresponding graphs as clauses (plain graphs are the ones considered in standard monotone approach). Positive (negative) parts of double graphs express reducts to positive (negated) inputs.

2. Our approximations are asymmetric. I.e., the approximations are sets  $\mathcal{A}$  consisting of double graphs  $D$  of bounded positive length  $|D^+|$  such that the total number of positive parts  $D^+$ ,  $D \in \mathcal{A}$ , is also bounded. There are no restrictions concerning negative parts  $D^-$ . These approximations preserve usual “monotone” deviations from POS and NEG with regard to positive parts of double graphs and on the other hand enable a desired DMN generalization.

3. The DMN generalization is carried out within Boolean formalism via appropriate elimination of negative parts of double graphs [Lemma 19] while using a crucial *base property*  $\text{POS} = \text{BAS}(\text{CLIQUE})$  [Lemma 17]. This yields [Theorem 22], as desired.

A more formal exposition is as follows.

The DNFs involved are viewed as sets  $\mathcal{X}$  consisting of pairs  $\langle \vec{u}, \neg \vec{v} \rangle$  where  $\vec{u} = u_1 \cdots u_r$  and  $\vec{v} = v_1 \cdots v_s$  for  $r, s \leq \binom{k^4}{2}$  are disjoint strings of variables that encode arbitrary edges with  $k^4$  vertices; any  $u_i$  ( $v_j$ ) is supposed to lie inside (outside) a given input graph  $G$  under consideration. For brevity let  $\mathcal{X}^+ := \{ \vec{u} : (\exists \vec{v}) \langle \vec{u}, \neg \vec{v} \rangle \}$  and  $\mathcal{X}^- := \{ \vec{v} : (\exists \vec{u}) \langle \vec{u}, \neg \vec{v} \rangle \}$  denote corresponding positive and negative parts of  $\mathcal{X}$ , respectively.  $G$  is called *accepted* by  $\mathcal{X}$  if there exists  $\langle \vec{u}, \neg \vec{v} \rangle \in \mathcal{X}$  such that  $\vec{u} \subseteq G$  and  $\vec{v} \cap G = \emptyset$ .

The *approximations* are size-bounded DNFs  $\mathcal{A}$  such that  $(\forall \vec{u} \in \mathcal{A}^+) |\vec{u}| \leq \ell$  and  $|\mathcal{A}^+| \leq L$  for  $\ell = \sqrt{k}$  and  $L = (4\ell \log_{1.5} k - 1)^\ell \ell!$  (there are no constraints on the size of  $\mathcal{A}^-$ ).

Erdős-Rado plucking lemma provides approximations for arbitrary DNFs. It is applied as usual to the positive parts of inputs. Moreover, if  $\mathcal{A}$  approximates  $\mathcal{X}$ , then  $(\forall \langle \vec{u}, \neg \vec{v} \rangle \in \mathcal{A}) (\exists \vec{w} \supseteq \vec{u}) \langle \vec{w}, \neg \vec{v} \rangle \in \mathcal{X}$ . Corresponding *deviations* (also called *errors*) are the total numbers of special positive and negative test graphs that are accepted (rejected) by  $\mathcal{A}$  but rejected (accepted) by  $\mathcal{X}$ . The test graphs and upper bounds on the deviations are similar to those used and (respectively) obtained in standard monotone approach [Lemmata 9, 10, 12]. By standard methods it follows that the (circuit) size of any DMN formula  $\varphi$  whose DNF  $\mathcal{X}$  accepts all positive test graphs and rejects all negative ones is necessarily exponential in  $k$  [Theorem 13].

A desired conclusion that the exponential lower bound holds true if  $\varphi$  is an affirmative solution of CLIQUE [Theorem 22] now follows in Boolean algebra by an admissible elimination of negative literals occurring in  $\mathcal{X}$ .

## 2 Preliminaries

In the sequel we assume  $2 < p < \ell < k$ ,  $m := k^4$  and  $L := \ell!(p-1)^\ell$  to be fixed. For any  $n > 0$  and sets  $X, Y$  we let  $[n] := \{1, \dots, n\}$  and consider products  $X \cdot Y := \{\{x, y\} : x \in X \wedge y \in Y \wedge x \neq y\}$  and  $X^{(2)} := X \cdot X$ . Thus  $|[m]^{(2)}| = \frac{1}{2}m(m-1)$ , where  $|X| := \text{card}(X)$ . Set  $\mathcal{F} := \{f : [m] \rightarrow [k-1]\}$  (the *coloring functions*), so  $|\mathcal{F}| = (k-1)^m$ .

### 2.1 Plain graphs

This is a recollection of graph theoretic background in standard approach (cf. e.g. [2]–[4]). Plain (unordered) graphs with  $m$  vertices are nonempty subsets of  $[m]^{(2)}$ . For any graph  $\emptyset \neq G \subseteq [m]^{(2)}$  we regard pairs  $\{x, y\} \in G$  as *edges* and define its *vertices*  $v(G) := \{x \in [m] : (\exists y \in [m]) \{x, y\} \in G\}$ .  $\mathcal{G} = \wp[m]^{(2)} \setminus \{\emptyset\}$  will denote the set of all graphs and  $\mathcal{K} = \{K \in \mathcal{G} : |K| = k \wedge K = v(K)^{(2)}\} \subset \mathcal{G}$  the set of *complete graphs* with  $k$  vertices. Below we identify CLIQUE( $m, k$ ) problem with the set of its affirmative solutions  $G \in \mathcal{G}$  and use abbreviation

$$\boxed{\text{CLIQUE} := \{G \in \mathcal{G} : (\exists K \in \mathcal{K}) K \subseteq G\}}$$

### 2.2 Test graphs

Consider basic affirmative and negative solutions of CLIQUE, called *positive* and *negative test graphs*  $\boxed{\text{POS} := \mathcal{K}}$  and  $\boxed{\text{NEG} := \{C_f\}_{f \in \mathcal{F}}}$ , respectively, where  $C_f := \{\{x, y\} \in [m]^{(2)} : f(x) \neq f(y)\} \in \mathcal{G}$ . It holds  $\text{CLIQUE}, \text{POS}, \text{NEG} \subset \mathcal{G}$ .

**Lemma 1**  $\text{POS} \subset \text{CLIQUE}$  and  $\text{NEG} \cap \text{CLIQUE} = \emptyset$ . Moreover  $|\text{POS}| = \binom{m}{k}$  and  $|\text{NEG}| = (k-1)^m$ , while NEG is viewed as multiset indexed by  $f \in \mathcal{F}$ .

**Proof.** Clear. ■

## 2.3 Double graphs

Pairs of disjoint plain graphs are called *double graphs*. More precisely, the set of double graphs is defined by

$$\mathcal{D} := \{\langle G_1, G_2 \rangle : G_1 \cap G_2 = \emptyset \neq G_1 \cup G_2\}_{G_1, G_2 \in \mathcal{G} \cup \{\emptyset\}}$$

For any  $D = \langle G_1, G_2 \rangle \in \mathcal{D}$  and  $\mathcal{X} \subseteq \mathcal{D}$  we let  $D^+ := G_1 \in \mathcal{G}$ ,  $D^- := G_2 \in \mathcal{G}$  and  $\mathcal{X}^+ := \{D^+ : D \in \mathcal{X}\} \subseteq \mathcal{G}$ ,  $\mathcal{X}^- := \{D^- : D \in \mathcal{X}\} \subseteq \mathcal{G}$ .  $D^+$  ( $D^-$ ) and  $\mathcal{X}^+$  ( $\mathcal{X}^-$ ) are called positive (negative) parts of  $D$  and  $\mathcal{X}$ , respectively.  $\mathcal{G}$  is regarded part of  $\mathcal{D}$  e.g. by canonical embeddings  $\mathcal{G} \ni G \hookrightarrow \langle G, \emptyset \rangle \in \mathcal{D}$  and/or  $\mathcal{G} \ni G \hookrightarrow \langle G, \mathcal{G} \setminus G \rangle \in \mathcal{D}$ .

*Intended meaning:*  $\mathcal{D}$  encodes the collection of complementary extensions of plain graphs. Any  $G \in \mathcal{G}$  gives rise to the set of  $D \in \mathcal{D}$  such that  $D^+ \subseteq G$  and  $D^- \cap G = \emptyset$  (i.e.  $D \subseteq^\pm G$  as in 4 below).

### 2.3.1 Basic operations

For any  $D, E \in \mathcal{D}$  and  $\mathcal{X}, \mathcal{Y} \subseteq \mathcal{D}$  we define  $D \uplus E \in \mathcal{D}$ ,  $\mathcal{X} \odot \mathcal{Y} \subseteq \mathcal{D}$ .

1.  $D \uplus E := \begin{cases} \langle D^+ \cup E^+, D^- \cup E^- \rangle, & \text{if } (D^+ \cup E^+) \cap (D^- \cup E^-) = \emptyset, \\ \emptyset, & \text{else.} \end{cases}$
2.  $\mathcal{X} \odot \mathcal{Y} := \{D \uplus E : \langle D, E \rangle \in \mathcal{X} \times \mathcal{Y}\}.$   
We also use abbreviations  $D \subseteq^\pm E$  and  $D \subseteq^\pm G$  for  $G \in \mathcal{G}$ .
3.  $D \subseteq^\pm E \Leftrightarrow D^+ \subseteq E^+ \& D^- \subseteq E^-.$
4.  $D \subseteq^\pm G \Leftrightarrow D^+ \subseteq G \& D^- \cap G = \emptyset \Leftrightarrow D \subseteq^\pm \langle G, \mathcal{G} \setminus G \rangle.$

Sets  $\mathcal{X} \subseteq \mathcal{D}$  are viewed as (locally consistent) disjunctive normal forms (DNFs) of DMN formulas, while  $D \in \mathcal{X}$  encode pairs of conjunctions of positive and negative literals occurring in  $D^+$  and  $D^-$ , respectively. Basic operations  $\uplus$  and  $\odot$  on  $\wp \mathcal{D}$  imitate join and meet of corresponding DNFs. Note that  $(D \uplus E)^+$  is a (possibly) proper subset of  $D^+ \uplus E^+$ , and hence  $(\mathcal{X} \odot \mathcal{Y})^+$  might be different from corresponding positive join  $\mathcal{X}^+ \wedge \mathcal{Y}^+$ .

## 3 Proof proper

We generalize standard ‘monotone’ arguments (cf. [1]–[6], et al). However, we use conventional formalism of Boolean algebra and avoid explicit references to probabilistic connections.

### 3.1 Basic case

We expand on  $\mathcal{D}$  basic notions and ideas used in ‘monotone’ considerations related to  $\mathcal{G}$  (cf. [2]–[4], see also Remark 27).

### 3.1.1 Acceptability

With any given set of double graphs  $\mathcal{X} \subseteq \mathcal{D}$  we correlate the set of *accepted* plain graphs  $\text{ACC}(\mathcal{X})$  and its complement  $\text{REJ}(\mathcal{X})$  (called *rejected* plain graphs).

**Definition 2** For any  $G \in \mathcal{G}$  and  $\mathcal{X} \subseteq \mathcal{D}$  let:

1.  $\mathcal{X} \Vdash G \Leftarrow (\exists D \in \mathcal{X}) D \subseteq^\pm G$  ( $\mathcal{X}$  accepts  $G$ ),
2.  $\text{ACC}(\mathcal{X}) := \{G \in \mathcal{G} : \mathcal{X} \Vdash G\}$ ,
3.  $\text{REJ}(\mathcal{X}) := \mathcal{G} \setminus \text{ACC}(\mathcal{X})$ .

**Lemma 3** Following conditions 1–3 hold for any  $\mathcal{X}, \mathcal{Y} \subseteq \mathcal{D}$ .

1.  $\text{ACC}(\mathcal{X} \cup \mathcal{Y}) = \text{ACC}(\mathcal{X}) \cup \text{ACC}(\mathcal{Y})$ ,  
 $\text{REJ}(\mathcal{X} \cup \mathcal{Y}) = \text{REJ}(\mathcal{X}) \cap \text{REJ}(\mathcal{Y})$ .
2.  $\text{ACC}(\mathcal{X} \cap \mathcal{Y}) \subseteq \text{ACC}(\mathcal{X}) \cap \text{ACC}(\mathcal{Y}) = \text{ACC}(\mathcal{X} \odot \mathcal{Y})$ ,  
 $\text{REJ}(\mathcal{X} \cap \mathcal{Y}) \supseteq \text{REJ}(\mathcal{X}) \cup \text{REJ}(\mathcal{Y}) = \text{REJ}(\mathcal{X} \odot \mathcal{Y})$ .
3.  $\mathcal{X}^+ \subseteq \text{ACC}(\mathcal{X})$ .

**Proof.** 1: trivial.

2: It suffices to prove  $\text{ACC}(\mathcal{X}) \cap \text{ACC}(\mathcal{Y}) = \text{ACC}(\mathcal{X} \odot \mathcal{Y})$ . So suppose  $G \in \text{ACC}(\mathcal{X} \odot \mathcal{Y})$ , i.e. there are  $D \in \mathcal{X}$  and  $E \in \mathcal{Y}$  such that  $D \uplus E \in \mathcal{X} \odot \mathcal{Y}$  and  $D \uplus E \subseteq^\pm G$ , i.e.  $D^+ \cup E^+ \subseteq G$  and  $D^- \cup E^- \subseteq \overline{G} := \mathcal{G} \setminus G$ , which by

$$\begin{aligned} D^+ \cup E^+ \subseteq G \ \& \ D^- \cup E^- \subseteq \overline{G} \Leftrightarrow \\ D^+ \subseteq G \ \& \ D^- \subseteq \overline{G} \ \& \ E^+ \subseteq G \ \& \ E^- \subseteq \overline{G} \end{aligned}$$

yields both  $G \in \text{ACC}(\mathcal{X})$  and  $G \in \text{ACC}(\mathcal{Y})$ . Suppose  $G \in \text{ACC}(\mathcal{X}) \cap \text{ACC}(\mathcal{Y})$ . So there are  $D \in \mathcal{X}$  and  $E \in \mathcal{Y}$  with  $D \subseteq^\pm G$  and  $E \subseteq^\pm G$ , i.e.  $D^+ \subseteq G$ ,  $D^- \subseteq \overline{G}$ ,  $E^+ \subseteq G$  and  $E^- \subseteq \overline{G}$ , which by the same token yields  $G \in \text{ACC}(\mathcal{X} \odot \mathcal{Y})$ .

3: Let  $G := D^+ \in \mathcal{X}^+$  where  $D \in \mathcal{X}$ . Then  $G \cap D^- = \emptyset$  and hence  $\mathcal{X} \Vdash G$ .

■

### 3.1.2 Approximations and deviations

We supply basic operations  $\cup$  and  $\odot$  on  $\wp\mathcal{D}$  with appropriate *approximators*  $\sqcup$  and  $\sqcap$  operating on arbitrary subsets  $\mathcal{X} \subseteq \mathcal{D}$  such that  $(\forall D \in \mathcal{X}) |\mathbf{v}(D^+)| \leq \ell$  and  $|\{\mathbf{v}(D^+) : D \in \mathcal{X}\}| \leq L$ ; note that we approximate only positive parts of  $D \in \mathcal{X}$  and leave negative parts unchanged. We show that the corresponding *deviations*  $\partial_{\sqcup}^{\text{POS}}, \partial_{\sqcup}^{\text{NEG}}, \partial_{\sqcap}^{\text{POS}}, \partial_{\sqcap}^{\text{NEG}}$  from  $\cup$  and  $\odot$  with respect to accepted or rejected test graphs make only “small” fractions thereof (cf. Lemmata 9, 10). The deviations are similar to the errors caused by positive approximations used

in conventional monotone approach; actually, our double-graphs preserve basic combinatorial plain-graph estimates from [3]–[4]. So let

$$\begin{aligned}\mathcal{G}^\ell &:= \{G \in \mathcal{G} : |v(G)| \leq \ell\}, \quad \mathcal{D}^\ell := \{D \in \mathcal{D} : D^+ \in \mathcal{G}^\ell\}, \\ \wp_V^L \mathcal{D}^\ell &:= \{\mathcal{X} \subseteq \mathcal{D}^\ell : |v(\mathcal{X}^+)| \leq L\},\end{aligned}$$

where  $v(\mathcal{X}^+) := \{v(D^+) : D \in \mathcal{X}\}$ .<sup>3</sup> For any  $D, E \in \mathcal{D}^\ell$  and  $\mathcal{X}, \mathcal{Y} \subseteq \mathcal{D}^\ell$  let

$$\begin{aligned}D \uplus^\ell E &:= \begin{cases} D \uplus E, & \text{if } D \uplus E \in \mathcal{D}^\ell, \\ \emptyset, & \text{else,} \end{cases} \\ \mathcal{X} \odot^\ell \mathcal{Y} &:= \{D \uplus^\ell E : D \in \mathcal{X} \text{ \& } E \in \mathcal{Y}\}.\end{aligned}$$

As usual our approach is based on the Erdős-Rado lemma.

**Definition 4** A set  $\mathcal{S} = \{S_1, \dots, S_q\} \subset \wp[m]$  is called a sunflower with petals  $S_1, \dots, S_q$  ( $q > 1$ ) if  $S_1 \cap S_2 = S_i \cap S_j$  holds for all  $i < j \in [q]$ .  $S_1 \cap S_2 = \bigcap_{i=1}^q S_i$  is called the core of  $\mathcal{S}$ .

**Lemma 5** (Erdős-Rado) Let  $\wp_\ell[m] := \{X \subset [m] : |X| \leq \ell\}$ . Every  $\mathcal{X} \subseteq \wp_\ell[m]$  of cardinality  $|\mathcal{X}| > L$  contains a sunflower  $\mathcal{S} \subseteq \mathcal{X}$  of cardinality  $q \geq p$ .

**Proof.** Standard (cf. [10]). ■

**Definition 6** Plucking algorithm  $\wp \mathcal{D}^\ell \ni \mathcal{X} \mapsto \text{PLU}(\mathcal{X}) \in \wp_V^L \mathcal{D}^\ell$  is defined as follows by recursion on  $\tau(\mathcal{X}) := |v(\mathcal{X}^+)|$ . If  $\tau(\mathcal{X}) \leq L$ , let  $\text{PLU}(\mathcal{X}) := \mathcal{X}$ . Otherwise, we have  $\tau(\mathcal{X}) = |v(\mathcal{X}^+)| > L$ . By the Erdős-Rado lemma we choose a sunflower  $\mathcal{S} = \{v(G_1), \dots, v(G_q)\} \subseteq v(\mathcal{X}^+)$  of maximal cardinality  $q \geq p$  and let  $\mathcal{U} := \{E \in \mathcal{X} : v(E^+) \in \mathcal{S}\}$ . Rewrite  $\mathcal{X}$  to  $\mathcal{X}_1$  that arises by replacing every  $E \in \mathcal{U}$  by  $E_\odot \in \mathcal{D}^\ell$  such that  $E_\odot^+ = \bigcap_{E \in \mathcal{U}} E^+$  and  $E_\odot^- = E^-$ .<sup>4</sup> Note that  $v(E_\odot^+)$  is contained in the core of  $\mathcal{S}$ . Moreover  $|\mathcal{X}_1^+| = |\mathcal{X}^+| - q + 1 \leq |\mathcal{X}^+| - p + 1$ . If  $\tau(\mathcal{X}) \leq L$ , let  $\text{PLU}(\mathcal{X}) := \mathcal{X}_1$ . Otherwise, if  $\tau(\mathcal{X}_1) > L$  then we analogously pass from  $\mathcal{X}_1 \subseteq \mathcal{D}^\ell$  to  $\mathcal{X}_2 \subseteq \mathcal{D}^\ell$  such that  $|\mathcal{X}_2^+| \leq |\mathcal{X}_1^+| - p + 1$ . Proceeding this way we eventually obtain  $\mathcal{X}_r \subseteq \mathcal{D}^\ell$  with  $\tau(\mathcal{X}_r) \leq L$  and let  $\text{PLU}(\mathcal{X}) := \mathcal{X}_r$ .

**Lemma 7** For any  $\mathcal{X} \in \wp \mathcal{D}^\ell$ ,  $\text{PLU}(\mathcal{X})$  requires  $\leq \tau(\mathcal{X})(p-1)^{-1}$  elementary pluckings. Thus if  $\text{PLU}(\mathcal{X}) = \mathcal{X}_r$  as above then  $r \leq |v(\mathcal{X}^+)|(p-1)^{-1}$ .

**Proof.** Every single plucking reduces  $|v(\mathcal{X}^+)|$  by  $q-1 \geq p-1$ . This yields the required upper bound  $r \leq |v(\mathcal{X}^+)|(p-1)^{-1}$ . ■

**Definition 8** For any  $\mathcal{X}, \mathcal{Y} \in \wp_V^L \mathcal{D}^\ell$  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 approximations, respectively. These determine corresponding deviations  $\partial_{\sqcup}^{\text{POS}}, \partial_{\sqcup}^{\text{NEG}}, \partial_{\sqcap}^{\text{POS}}, \partial_{\sqcap}^{\text{NEG}}$  with respect to accepted and rejected test graphs.<sup>5</sup>

<sup>3</sup>Note that  $G \in \mathcal{G}^\ell$  implies  $|G| \leq \frac{1}{2}\ell(\ell-1)$ .

<sup>4</sup>This operation will be referred to as elementary plucking. It is more sophisticated than conventional plucking that collapses underlying (positive) sunflower to its core (as singleton).

<sup>5</sup>We write  $\partial$  instead of  $\delta$  used in [5]–[7].

1.  $\mathcal{X} \sqcup \mathcal{Y} := \text{PLU}(\mathcal{X} \cup \mathcal{Y}) \in \wp_V^L \mathcal{D}^\ell$ .
2.  $\mathcal{X} \sqcap \mathcal{Y} := \text{PLU}(\mathcal{X} \odot^\ell \mathcal{Y}) \in \wp_V^L \mathcal{D}^\ell$ .
3.  $\partial_{\sqcup}^{\text{POS}}(\mathcal{X}, \mathcal{Y}) := \text{POS} \cap \text{ACC}(\mathcal{X} \cup \mathcal{Y}) \cap \text{REJ}(\mathcal{X} \sqcup \mathcal{Y})$ .
4.  $\partial_{\sqcap}^{\text{POS}}(\mathcal{X}, \mathcal{Y}) := \text{POS} \cap \text{ACC}(\mathcal{X} \odot \mathcal{Y}) \cap \text{REJ}(\mathcal{X} \sqcap \mathcal{Y})$ .
5.  $\partial_{\sqcup}^{\text{NEG}}(\mathcal{X}, \mathcal{Y}) := \text{NEG} \cap \text{REJ}(\mathcal{X} \cup \mathcal{Y}) \cap \text{ACC}(\mathcal{X} \sqcup \mathcal{Y})$ .
6.  $\partial_{\sqcap}^{\text{NEG}}(\mathcal{X}, \mathcal{Y}) := \text{NEG} \cap \text{REJ}(\mathcal{X} \odot \mathcal{Y}) \cap \text{ACC}(\mathcal{X} \sqcap \mathcal{Y})$ .

In the sequel we assume that  $m$  is sufficiently large and  $k = \ell^2$ .

**Lemma 9** *Let  $\mathcal{Z} = \text{PLU}(\mathcal{X} \cup \mathcal{Y}) \in \wp_V^L \mathcal{D}^\ell$  for  $\mathcal{X}, \mathcal{Y} \in \wp_V^L \mathcal{D}^\ell$ ,  $\mathcal{X} \cup \mathcal{Y} \in \wp \mathcal{D}^\ell$ , so  $|\mathbf{v}(\mathcal{Z}^+)| \leq L$ , whereas  $|\mathbf{v}(\mathcal{X} \cup \mathcal{Y})^+| \leq 2L$ .  $\mathcal{Z}$  creates less than  $2L \left(\frac{2}{3}\right)^p (k-1)^m$  fake negative test graphs and preserves positive ones. That is,  $|\partial_{\sqcup}^{\text{POS}}(\mathcal{X}, \mathcal{Y})| = 0$  while  $|\partial_{\sqcup}^{\text{NEG}}(\mathcal{X}, \mathcal{Y})| < 2L \left(\frac{2}{3}\right)^p (k-1)^m$ .*

**Proof.** We argue along the lines of [3]–[4] via Lemma 3 (1).  $\partial_{\sqcup}^{\text{POS}}(\mathcal{X}, \mathcal{Y}) = \emptyset$  is clear as elementary pluckings replace some (double) graphs by (double) subgraphs and hence preserve the accepted positive test graphs. Consider  $\partial_{\sqcup}^{\text{NEG}}(\mathcal{X}, \mathcal{Y})$ . Let  $\mathcal{S} = \{\mathbf{v}(G_1), \dots, \mathbf{v}(G_q)\} \subseteq \mathbf{v}(\mathcal{W}^+)$ ,  $\mathcal{W} \subseteq \mathcal{X} \cup \mathcal{Y}$ ,  $q \geq p$ , be the sunflower of an elementary plucking involved and set  $\mathcal{U} := \{E \in \mathcal{W} : \mathbf{v}(E^+) \in \mathcal{S}\}$ ,  $r := |\mathcal{U}| \geq q$ . Let  $E_{\odot} \in \mathcal{D}^\ell$ ,  $E_{\odot}^+ = \bigcap_{E_i \in \mathcal{U}} E_i^+ \in \mathcal{D}^\ell$ ,  $i \in [q]$ , be as in Definition 6. For the sake of brevity let  $V := \mathbf{v}(E_{\odot}^+)$ ,  $V_i := \mathbf{v}(E_i^+)$ ,  $V_{i-\odot} := V_i \setminus V$ ,  $s := |V|$ ,  $s_i := |V_i|$ ,  $t_i := |V_{i-\odot}| = s_i - s$ ,  $f \in \mathcal{F}$  and for any  $\mathcal{Z} \subseteq \mathcal{F}$  let  $\mathbb{P}[\mathcal{Z}] := |\mathcal{Z}| |\mathcal{F}|^{-1} = |\mathcal{Z}| (k-1)^{-m}$ ; note that  $s, t_i \leq s_i \leq \ell$ . Now suppose that  $C_f \in \text{NEG}$ ,  $f : [m] \rightarrow [k-1]$ , is a fake negative test graph created by  $E_{\odot}$ . That is,  $E_{\odot} \subseteq^\pm C_f$  although  $(\forall E_i \in \mathcal{U}) E_i \not\subseteq^\pm C_f$ . Thus  $f(x) \neq f(y)$  holds for all edges  $\{x, y\} \in E_{\odot}^+$ , although every  $E_i^+ \in \mathcal{U}^+$ ,  $i \in [q]$ , contains an edge  $\{x, y\}$  with  $f(x) = f(y)$ . That is,  $f \in \bigcap_{i=1}^q \mathcal{R}_i$  where

$$\mathcal{R}_i := \left\{ f : \left( \forall \{x, y\} \in V^{(2)} \right) (f(x) \neq f(y)) \ \& \ \left( \exists \{x, y\} \in V_{i-\odot}^{(2)} \right) (f(x) = f(y)) \right\}.$$

Hence  $f \in \mathcal{F} \setminus \mathcal{T}_i$  for  $\mathcal{T}_i := \{f : (\forall x \neq y \in V_{i-\odot}) (f(x) \neq f(y))\}$ . Moreover

$$\begin{aligned} \mathbb{P}[\mathcal{T}_i] &= \frac{k-1-1}{k-1} \cdot \frac{k-1-2}{k-1} \dots \frac{k-1-(t_i-1)}{k-1} \geq \left(1 - \frac{t_i-1}{k-1}\right)^{t_i-1} \\ &\geq \left(1 - \frac{\ell-1}{\ell^2-1}\right)^{\ell-1} \geq \left(1 - \frac{1}{\ell}\right)^\ell \xrightarrow[\ell \rightarrow \infty]{} e^{-1} > \frac{1}{3} \end{aligned}$$

which yields  $\mathbb{P}[\mathcal{F} \setminus \mathcal{T}_i] < \frac{2}{3}$  for large  $m$ . Since  $(\forall i \neq j \in [q]) V_{i-\odot} \cap V_{j-\odot} = \emptyset$ ,

$$\mathbb{P} \left[ \bigcap_{i=1}^q \mathcal{R}_i \right] \leq \mathbb{P} \left[ \bigcap_{i=1}^q (\mathcal{F} \setminus \mathcal{T}_i) \right] = \prod_{i=1}^q \mathbb{P}[\mathcal{F} \setminus \mathcal{T}_i] \leq \left(\frac{2}{3}\right)^q \leq \left(\frac{2}{3}\right)^p$$

and hence there are less than  $(\frac{2}{3})^p (k-1)^m$  fake negative test graphs created by  $E_{\oplus}^+$ . By Lemma 7 there are at most  $2L(p-1)^{-1} < 2L$  elementary pluckings involved, and hence  $|\partial_{\square}^{\text{NEG}}(\mathcal{X}, \mathcal{Y})| < 2L(\frac{2}{3})^p (k-1)^m$ . ■

**Lemma 10** *Let  $\mathcal{Z} = \text{PLU}(\mathcal{X} \odot^{\ell} \mathcal{Y}) \in \wp_V^L \mathcal{D}^{\ell}$  for  $\mathcal{X}, \mathcal{Y} \in \wp_V^L \mathcal{D}^{\ell}$ ,  $\mathcal{X} \odot^{\ell} \mathcal{Y} \in \wp \mathcal{D}^{\ell}$ , so  $|\mathbf{v}(\mathcal{Z}^+)| \leq L$  and  $|\mathbf{v}(\mathcal{X} \odot^{\ell} \mathcal{Y})^+| \leq L^2$ .  $\mathcal{Z}$  requires  $\leq \frac{L^2}{p-1}$  plucking steps and creates less than  $L^2(\frac{2}{3})^p (k-1)^m$  fake negative test graphs while missing at most  $L^2 \binom{m-\ell-1}{k-\ell-1}$  positive test graphs. That is, we have  $|\partial_{\square}^{\text{POS}}(\mathcal{X}, \mathcal{Y})| \leq L^2 \binom{m-\ell-1}{k-\ell-1}$  and  $|\partial_{\square}^{\text{NEG}}(\mathcal{X}, \mathcal{Y})| < L^2(\frac{2}{3})^p (k-1)^m$ .*

**Proof.**  $|\partial_{\square}^{\text{NEG}}(\mathcal{X}, \mathcal{Y})| < L^2(\frac{2}{3})^p (k-1)^m$  holds analogously to the inequality for  $\partial_{\square}^{\text{NEG}}(\mathcal{X}, \mathcal{Y})$ . Consider  $\partial_{\square}^{\text{POS}}(\mathcal{X}, \mathcal{Y})$ . Using Lemma 3 (2) we adapt standard arguments used in familiar “monotone” proofs (cf. e.g. [3]–[4]). It is readily seen that deviations can only arise by deleting a  $H = D \uplus E \notin \mathcal{D}^{\ell}$  for some  $D, E \in \mathcal{D}^{\ell}$  while passing from  $\mathcal{X} \odot \mathcal{Y}$  to  $\mathcal{X} \odot^{\ell} \mathcal{Y}$ . Thus  $H^+ \in (\mathcal{X} \odot^{\ell} \mathcal{Y})^+ \setminus \mathcal{G}^{\ell}$ , and hence  $\ell < |\mathbf{v}(H^+)| \leq 2\ell$ . We wish to estimate  $|\mathcal{S}_H|$  for  $\mathcal{S}_H := \{K \in \text{POS} : H \subseteq^{\pm} K\} \subseteq \{K \in \text{POS} : H^+ \subset K\} =: \mathcal{S}_{H^+}$ . For any  $K \in \mathcal{S}_{H^+}$  we have  $\ell < |\mathbf{v}(H^+)| < |\mathbf{v}(K)| = k$  and hence  $|\mathcal{S}_H| \leq |\mathcal{S}_{H^+}| \leq \binom{m-\ell-1}{k-\ell-1}$ . Since  $|\mathbf{v}(\mathcal{X} \odot^{\ell} \mathcal{Y})^+| \leq L^2$ , this yields  $|\partial_{\square}^{\text{POS}}(\mathcal{X}, \mathcal{Y})| \leq L^2 \binom{m-\ell-1}{k-\ell-1}$ . ■

### 3.1.3 DMN 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  $\varphi$  we generalize 2.1.1–2.1.2 defining the double graph *approximations*  $\text{APR}(\varphi)$  and the sets of *accepted (rejected)* plain graphs  $\text{ACC}(\varphi)$  (resp.  $\text{REJ}(\varphi)$ ) and  $\text{ACC}(\text{APR}(\varphi))$  (resp.  $\text{REJ}(\text{APR}(\varphi))$ ) augmented with *total deviations*  $\partial^{\text{POS}}(\varphi) \subseteq \text{POS}$  and  $\partial^{\text{NEG}}(\varphi) \subseteq \text{NEG}$ . Using estimates on  $\partial_{\square}^{\text{POS}}, \partial_{\square}^{\text{NEG}}, \partial_{\square}^{\text{POS}}, \partial_{\square}^{\text{NEG}}$  we show that assumptions  $\text{POS} \subseteq \text{ACC}(\varphi)$  and  $\text{NEG} \subseteq \text{REJ}(\varphi)$  infer exponential circuit size of  $\varphi$  (cf. Theorem 13 below).

#### 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.:  $\varphi, \psi$ ) 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  $\top \wedge \varphi = \varphi \wedge \top = \perp \vee \varphi = \varphi \vee \perp := \varphi$ . Let  $[\varphi]$  denote structural complexity (= circuit size) of  $\varphi$ . To put it more precisely we let  $[\varphi] := |\text{SUB}(\varphi)|$  where the set of subformulas  $\text{SUB}(\varphi)$  is defined as follows by recursive clauses 1–2.



1.  $\text{SUB}(\varphi) := \{\varphi\}$ , if  $\varphi$  is any literal  $\top, \perp, v_i, \neg v_i$  ( $i = 1, \dots, n$ ).
2.  $\text{SUB}(\varphi \circ \psi) := \{\varphi \circ \psi\} \cup \text{SUB}(\varphi) \cup \text{SUB}(\psi)$ , where  $\circ \in \{\vee, \wedge\}$ .

To adapt  $\mathcal{A}$  to our graph theoretic models we define by following recursive clauses 1–4 two assignments

$$\mathcal{A} \ni \varphi \mapsto \text{SET}(\varphi) \in \{\top\} \cup \wp \mathcal{D} \quad \text{and} \quad \mathcal{A} \ni \varphi \mapsto \text{APR}(\varphi) \in \{\top\} \cup \wp_V^L \mathcal{D}^\ell$$

that represent DNFs and corresponding approximations of  $\varphi$ , respectively.

1.  $\text{SET}(\top) = \text{APR}(\top) := \top$ ,  $\text{SET}(\perp) = \text{APR}(\perp) := \emptyset$ .
2.  $\text{SET}(v_i) = \text{APR}(v_i) := \{\{\pi(i)\}, \emptyset\}$ ,  $\text{SET}(\neg v_i) = \text{APR}(\neg v_i) := \{\{\emptyset, \{\pi(i)\}\}\}$ .
3.  $\text{SET}(\varphi \vee \psi) := \text{SET}(\varphi) \cup \text{SET}(\psi)$ ,  $\text{APR}(\varphi \vee \psi) := \text{APR}(\varphi) \sqcup \text{APR}(\psi)$ .
4.  $\text{SET}(\varphi \wedge \psi) := \text{SET}(\varphi) \odot \text{SET}(\psi)$ ,  $\text{APR}(\varphi \wedge \psi) := \text{APR}(\varphi) \sqcap \text{APR}(\psi)$ .

In the sequel we use abbreviations  $\text{ACC}(\varphi) := \text{ACC}(\text{SET}(\varphi))$ ,  $\text{REJ}(\varphi) := \text{REJ}(\text{SET}(\varphi))$ ,  $\text{ACC}(\top) := \mathcal{G}$  and (hence)  $\text{REJ}(\top) := \emptyset$ . Moreover for any  $\varphi \in \mathcal{A}$ , we define *total deviations*  $\partial^{\text{POS}}(\varphi)$  and  $\partial^{\text{NEG}}(\varphi)$ .

1.  $\partial^{\text{POS}}(\varphi) := \text{POS} \cap \text{ACC}(\varphi) \cap \text{REJ}(\text{APR}(\varphi))$ .
2.  $\partial^{\text{NEG}}(\varphi) := \text{NEG} \cap \text{REJ}(\varphi) \cap \text{ACC}(\text{APR}(\varphi))$ .

**Lemma 11** *For any  $\varphi, \psi \in \mathcal{A}$  and  $*$   $\in \{\text{POS}, \text{NEG}\}$  the following inclusions hold.*

1.  $\partial^*(\varphi \vee \psi) \subseteq \partial_\sqcup^*(\text{APR}(\varphi), \text{APR}(\psi)) \cup \partial^*(\varphi) \cup \partial^*(\psi)$ , and hence  $[\partial^*(\varphi \vee \psi)] \leq [\partial_\sqcup^*(\text{APR}(\varphi), \text{APR}(\psi))] + [\partial^*(\varphi)] + [\partial^*(\psi)]$ .
2.  $\partial^*(\varphi \wedge \psi) \subseteq \partial_\sqcap^*(\text{APR}(\varphi), \text{APR}(\psi)) \cup \partial^*(\varphi) \cup \partial^*(\psi)$ , and hence  $[\partial^*(\varphi \wedge \psi)] \leq [\partial_\sqcap^*(\text{APR}(\varphi), \text{APR}(\psi))] + [\partial^*(\varphi)] + [\partial^*(\psi)]$ .

**Proof.** Straightforward via  $A \setminus B \subseteq (A \setminus C) \cup (C \setminus B)$  (see Appendix B). ■

**Lemma 12** *Following conditions 1–3 hold for any formula  $\varphi \in \mathcal{A}$ .*

1.  $|\partial^{\text{POS}}(\varphi)| \leq \lfloor \varphi \rfloor \cdot L^2 \binom{m-\ell-1}{k-\ell-1}$ .
2.  $|\partial^{\text{NEG}}(\varphi)| < \lfloor \varphi \rfloor \cdot L^2 \left(\frac{2}{3}\right)^p (k-1)^m$ .
3.  $\text{POS} \cap \text{ACC}(\text{APR}(\varphi)) \neq \emptyset$  implies  $|\text{NEG} \cap \text{ACC}(\text{APR}(\varphi))| > \frac{1}{3}(k-1)^m$ .

**Proof.** 1–2: These follow from Lemmata 9–11 by induction on  $\lfloor \varphi \rfloor$ .

3:  $\text{POS} \cap \text{ACC}(\text{APR}(\varphi)) \neq \emptyset$  implies  $\text{APR}(\varphi) \neq \emptyset$ , so there exists  $E \in \text{APR}(\varphi)$ ,  $|V(E^+)| \leq \ell$ . Let  $\mathcal{T} := \{f \in \mathcal{F} : (\forall x \neq y \in V(E^+)) (f(x) \neq f(y))\}$ . Now  $|\mathcal{T}|(k-1)^{-m} = 1 - \mathbb{P}[\mathcal{F} \setminus \mathcal{T}] > \frac{1}{3}$ , i.e.  $|\mathcal{T}| > \frac{1}{3}(k-1)^m$  for sufficiently large  $m$  (cf. proof of Lemma 9), which yields  $|\text{NEG} \cap \text{ACC}(\text{APR}(\varphi))| > \frac{1}{3}(k-1)^m$ . ■

- In the sequel  $\boxed{\ell = m^{\frac{1}{8}}, p = \ell \log_{1.5} m, L = (p-1)^\ell \ell!, k = m^{\frac{1}{4}}, m \gg 0.}$

**Theorem 13** *Suppose that  $\text{POS} \subseteq \text{ACC}(\varphi)$  and  $\text{NEG} \subseteq \text{REJ}(\varphi)$  hold for a given  $\varphi \in \mathcal{A}$ . Then for sufficiently large  $m$ ,  $\lfloor \varphi \rfloor > \sqrt[7]{m}^{\frac{8}{7}m} = k^{\frac{4}{7}\sqrt{k}}$ .*

**Proof.** Consider two cases (see also Appendix A).

1: Suppose  $\text{POS} \cap \text{ACC}(\text{APR}(\varphi)) = \emptyset$ . Now  $\text{POS} \subseteq \text{ACC}(\varphi)$  implies  $\partial^{\text{POS}}(\varphi) = \text{POS} \cap \text{ACC}(\varphi) \cap \text{REJ}(\text{APR}(\varphi)) = \text{POS} \cap \text{REJ}(\text{APR}(\varphi)) = \text{POS}$ . Then by Lemma 12 (2) we have  $\lfloor \varphi \rfloor \cdot L^2 \binom{m-\ell-1}{k-\ell-1} \geq |\partial^{\text{POS}}(\varphi)| = |\text{POS}| = \binom{m}{k}$ , and hence  $\lfloor \varphi \rfloor \geq L^{-2} \binom{m}{k} \binom{m-\ell-1}{k-\ell-1}^{-1} > L^{-2} \left(\frac{m-\ell}{k}\right)^\ell > m^{\frac{1}{7}m^{\frac{1}{8}}} = \sqrt[7]{m}^{\frac{8}{7}m}$ .

2: Suppose  $\text{POS} \cap \text{ACC}(\text{APR}(\varphi)) \neq \emptyset$ . Now  $\text{NEG} \subseteq \text{REJ}(\varphi)$  implies  $\partial^{\text{NEG}}(\varphi) = \text{NEG} \cap \text{ACC}(\text{APR}(\varphi))$ . So by Lemma 12 (2, 3) we have  $\lfloor \varphi \rfloor \cdot L^2 \left(\frac{2}{3}\right)^p (k-1)^m > |\partial^{\text{NEG}}(\varphi)| \geq \frac{1}{3}(k-1)^m$ , and hence  $\lfloor \varphi \rfloor > \frac{1}{3}L^{-2}(1.5)^p > m^{\frac{1}{3}m^{\frac{1}{8}}} > \sqrt[7]{m}^{\frac{8}{7}m}$ . ■

It remains to show that the assumptions of Theorem 13 are fulfilled by any formula  $\varphi \in \mathcal{A}$  that provides affirmative solution of  $\text{CLIQUE}(k^4, k)$ . To this end we supply  $\mathcal{G}$  and  $\mathcal{D}$  with natural semantic, as follows.

### Semantic

**Definition 14** *We consider variable assignments  $\text{VAS} = \{\vartheta : [n] \longrightarrow \{0, 1\}\}$ . For any  $\varphi \in \mathcal{A}$ ,  $i \in [n]$ ,  $D \in \mathcal{D}$ ,  $G \in \mathcal{G}$ ,  $\mathcal{X} \subseteq \mathcal{D}$ ,  $\mathcal{Y} \subseteq \mathcal{D}$ , any given  $\vartheta \in \text{VAS}$  extends by following clauses 1–7 to Boolean evaluations of  $\varphi$ ,  $D$ ,  $G$ ,  $\mathcal{X}$ ,  $\mathcal{Y}$ .*

$$1. \|\top\|_\vartheta := 1, \|\perp\|_\vartheta := 0.$$

$$2. \|v_i\|_\vartheta := \vartheta(i).$$

$$3. \|\neg v_i\|_\vartheta := 1 - \vartheta(i).$$

$$4. \|\varphi \vee \psi\|_\vartheta := \max\{\|\varphi\|_\vartheta, \|\psi\|_\vartheta\}.$$

$$5. \|\varphi \wedge \psi\|_\vartheta := \min\{\|\varphi\|_\vartheta, \|\psi\|_\vartheta\}.$$

$$6. \|D\|_\vartheta := \left\| \bigwedge_{\pi(i) \in D^+} v_i \wedge \bigwedge_{\pi(j) \in D^-} \neg v_j \right\|_\vartheta, \|G\|_\vartheta := \|\langle G, \mathcal{G} \setminus G \rangle\|_\vartheta.$$

Thus  $\|D\|_\vartheta = 1 \Leftrightarrow (\forall \pi(i) \in D^+) \vartheta(i) = 1 \ \& \ (\forall \pi(j) \in D^-) \vartheta(j) = 0$  and hence  $\|G\|_\vartheta = 1 \Leftrightarrow (\forall \pi(i) \in G) \vartheta(i) = 1 \ \& \ (\forall \pi(j) \notin G) \vartheta(j) = 0$ .

$$7. \|\mathcal{X}\|_\vartheta := \left\| \bigvee_{D \in \mathcal{X}} D \right\|_\vartheta, \|\mathcal{Y}\|_\vartheta := \left\| \bigvee_{G \in \mathcal{Y}} G \right\|_\vartheta.$$

**Lemma 15**  $\|\varphi\|_\vartheta = \|\text{SET}(\varphi)\|_\vartheta$  holds for any  $\varphi \in \mathcal{A}$  and  $\vartheta \in \text{VAS}$ .

**Proof.** We argue by induction on  $[\varphi]$  via Lemma 3.

Consider induction step  $\varphi = \phi \wedge \psi$  where  $\text{SET}(\phi), \text{SET}(\psi) \neq \emptyset$ . We have  $\text{SET}(\varphi) = \text{SET}(\phi) \odot \text{SET}(\psi) = \{D \uplus E : \langle D, E \rangle \in \text{SET}(\phi) \times \text{SET}(\psi)\}$ , which yields

$$\begin{aligned} \|\text{SET}(\varphi)\|_{\vartheta} &= \max \{ \|D \uplus E\|_{\vartheta} : \langle D, E \rangle \in \text{SET}(\phi) \times \text{SET}(\psi) \} \\ &= \max \{ \|D^+ \cup E^-\|_{\vartheta} \cdot \|D^- \cup E^-\|_{\vartheta} : D \in \text{SET}(\phi) \text{ \& } E \in \text{SET}(\psi) \}. \end{aligned}$$

Hence by the induction hypothesis we have  $\|\text{SET}(\varphi)\|_{\vartheta} = 1 \Leftrightarrow$

$$\begin{aligned} &(\exists D \in \text{SET}(\phi)) (\exists E \in \text{SET}(\psi)) \\ &\quad \left[ \begin{array}{c} (D^+ \cup E^+) \cap (D^- \cup E^-) = \emptyset \text{ \& } \\ (\forall v_i \in D^+ \cup E^+) \|v_i\|_{\vartheta} = 1 \text{ \& } (\forall v_j \in D^- \cup E^-) \|v_j\|_{\vartheta} = 0 \end{array} \right] \Leftrightarrow \\ &(\exists D \in \text{SET}(\phi)) (\exists E \in \text{SET}(\psi)) \\ &\quad [(\forall v_i \in D^+ \cup E^+) \|v_i\|_{\vartheta} = 1 \text{ \& } (\forall v_j \in D^- \cup E^-) \|v_j\|_{\vartheta} = 0] \Leftrightarrow \\ &(\exists D \in \text{SET}(\phi)) [(\forall v_i \in D^+) \|v_i\|_{\vartheta} = 1 \text{ \& } (\forall v_j \in E^-) \|v_j\|_{\vartheta} = 0] \\ &\wedge (\exists E \in \text{SET}(\psi)) [(\forall v_i \in E^+) \|v_i\|_{\vartheta} = 1 \text{ \& } (\forall v_j \in E^-) \|v_j\|_{\vartheta} = 0] \Leftrightarrow \\ &\|\text{SET}(\phi)\|_{\vartheta} = 1 = \|\text{SET}(\psi)\|_{\vartheta} \Leftrightarrow \|\phi\|_{\vartheta} = 1 = \|\psi\|_{\vartheta} \Leftrightarrow \|\phi \wedge \psi\|_{\vartheta} = 1, \end{aligned}$$

which yields  $\|\phi \wedge \psi\|_{\vartheta} = \|\text{SET}(\varphi)\|_{\vartheta}$ .

Basis of induction and case  $\varphi = \phi \vee \psi$  are trivial. ■

To complete this chapter we consider appropriate *positive bases*.

### 3.1.4 Positive bases

*Base* of a given set of plain graphs is the collection of its minimal (modulo inclusion) elements. Our crucial observation says that Boolean-equivalent sets have equal bases (cf. Lemma 19 below and [13]: Ch. 2.1–2.2). This yields a desired link to Theorem 13.

**Definition 16** For any  $\mathcal{X} \subseteq \mathcal{G}$  let

$$\text{BAS}(\mathcal{X}) := \bigcap \{ \mathcal{Y} \subseteq \mathcal{X} : (\forall X \in \mathcal{X}) (\exists Y \in \mathcal{Y}) Y \subseteq X \}.$$

Obviously  $\mathcal{Y} \subseteq \mathcal{X} \subseteq \mathcal{G}$  implies  $\text{BAS}(\mathcal{Y}) \subseteq \text{BAS}(\mathcal{X}) \subseteq \mathcal{X}$ , while  $\mathcal{X} \subseteq \text{BAS}(\mathcal{X})$  implies  $\mathcal{X} = \text{BAS}(\mathcal{X})$ .

**Lemma 17**  $\text{POS} = \text{BAS}(\text{CLIQUE})$ .

**Proof.** Clear. ■

**Definition 18 (Boolean equivalence)** For any  $\mathcal{X}, \mathcal{Y} \subseteq \mathcal{G}$  or  $\mathcal{X} \subseteq \mathcal{D}, \mathcal{Y} \subseteq \mathcal{G}$  let  $\mathcal{X} \sim \mathcal{Y} \Leftrightarrow (\forall \vartheta \in \text{VAS}) \|\mathcal{X}\|_{\vartheta} = \|\mathcal{Y}\|_{\vartheta}$ .

**Lemma 19** For any  $\mathcal{X}, \mathcal{Y}$  as above, if  $\mathcal{X} \sim \mathcal{Y}$  then  $\mathcal{X}^+ \sim \mathcal{Y}$  and  $\text{BAS}(\mathcal{X}^+) = \text{BAS}(\mathcal{Y})$ .

**Proof.** Obviously it will suffice to assume  $\mathcal{X} \subseteq \mathcal{D}$ . So suppose  $\mathcal{D} \supseteq \mathcal{X} \sim \mathcal{Y} \subseteq \mathcal{G}$ , where  $\mathcal{Y} = \{G_i : i \in T\}$  and  $\mathcal{X} = \{D_i : i \in S\}$ . For any  $i \in S$  let  $D_i^+ = \{\pi(j) : j \in S_i^+\}$ ,  $D_i^- = \{\pi(j) : j \in S_i^-\}$ ,  $S_i^+ \cap S_i^- = \emptyset$ . Thus  $\mathcal{X}^+ =$

$\{D_i^+ : i \in S\}$ . For any  $i \in T$  let  $G_i = \{\pi(j) : j \in T_i\}$ . We prove  $\mathcal{X}^+ \sim \mathcal{Y}$  by induction on the number of nonempty  $S_i^-$ ,  $i \in S$ . Induction basis is obvious. Consider induction step. Suppose that  $S_a^- \neq \emptyset$  for  $a \in S$  and let

$$\mathcal{X}_a := \{\langle D_a^+, \emptyset \rangle\} \cup \{D_i : a \neq i \in S\}.$$

Clearly  $\mathcal{X}_a^+ \sim \mathcal{X}^+$ . Define  $\vartheta_a \in \text{VAS}$  by  $\vartheta_a(j) := \begin{cases} 1, & \text{if } j \in S_a^+, \\ 0, & \text{else,} \end{cases}$  then

$$\|\mathcal{Y}\|_{\vartheta_a} = \|\mathcal{X}\|_{\vartheta_a} = \|\mathcal{X}_a\|_{\vartheta_a} = \|D_a^+\|_{\vartheta_a} = 1.$$

Hence there exists  $b \in T$  such that  $T_b \subseteq S_a^+$ . Moreover  $(\forall \vartheta \in \text{VAS}) \|\mathcal{Y}\|_{\vartheta} = \|\mathcal{X}\|_{\vartheta} \leq \|\mathcal{X}_a\|_{\vartheta}$ . Now suppose that for some  $\vartheta \in \text{VAS}$ ,  $\|\mathcal{Y}\|_{\vartheta} < \|\mathcal{X}_a\|_{\vartheta}$  and hence

$$0 = \|\mathcal{Y}\|_{\vartheta} = \|\mathcal{X}\|_{\vartheta} \stackrel{\forall i \in S}{=} \|D_i\|_{\vartheta} < 1 = \|\mathcal{X}_a\|_{\vartheta} = \|D_a^+\|_{\vartheta}.$$

But then  $(\forall j \in S_a^+) \vartheta(j) = 1$  and hence  $(\forall j \in T_b) \vartheta(j) = 1$ , which yields  $1 = \|G_b\|_{\vartheta} = \|\mathcal{Y}\|_{\vartheta}$ , – a contradiction that proves  $\mathcal{Y} \sim \mathcal{X}_a$ . Hence by the induction hypothesis we have  $\mathcal{Y} \sim \mathcal{X}_a^+ \sim \mathcal{X}^+$ , as required. It remains to prove  $\text{BAS}(\mathcal{Y}) = \text{BAS}(\mathcal{X}^+)$ . So recall that  $\mathcal{Y} = \{G_i : i \in T\}$  and  $\mathcal{X}^+ = \{D_i^+ : i \in S\}$  and let  $\text{BAS}(\mathcal{Y}) = \{G_i : i \in T'\}$ ,  $T' \subseteq T$ , and  $\text{BAS}(\mathcal{X}^+) = \{D_i^+ : i \in S'\}$ ,  $S' \subseteq S$ . It is readily seen that

$$\mathcal{X}^+ \sim \mathcal{Y} \Rightarrow (\forall i \in T) (\exists j \in S) (T_j \subseteq S_i) \ \& \ (\forall j \in S) (\exists i \in T) (S_i \subseteq T_j)$$

which by the minimality of  $\text{BAS}(-)$  yields

$$\begin{aligned} \mathcal{X}^+ \sim \mathcal{Y} &\Rightarrow (\forall i \in T') (\exists j \in S') (T'_j = S'_i) \ \& \ (\forall j \in S') (\exists i \in T') (S'_i = T'_j) \\ &\Rightarrow \text{BAS}(\mathcal{X}^+) = \text{BAS}(\mathcal{Y}). \end{aligned}$$

Summing up  $\mathcal{X} \sim \mathcal{Y} \Rightarrow \mathcal{X}^+ \sim \mathcal{X} \sim \mathcal{Y} \Rightarrow \text{BAS}(\mathcal{X}^+) = \text{BAS}(\mathcal{Y})$ . ■

Now Lemma 17 yields

**Corollary 20** *For any  $\mathcal{X} \subseteq \mathcal{D}$ ,  $\text{CLIQUE} \sim \mathcal{X}$  implies  $\text{POS} = \text{BAS}(\mathcal{X}^+)$ .*

**Lemma 21** *Suppose that  $\varphi \in \mathcal{A}$  satisfies  $\text{SET}(\varphi) \sim \text{CLIQUE}$ . Then  $\text{POS} \subseteq \text{ACC}(\varphi)$  and  $\text{NEG} \subseteq \text{REJ}(\varphi)$ .*

**Proof.** By Lemma 17 and Corollary 20 we obtain  $\text{POS} = \text{BAS}(\text{SET}(\varphi)^+)$ , which by Lemma 3 (2) yields  $\text{POS} \subseteq \text{SET}(\varphi)^+ \subseteq \text{ACC}(\varphi)$ . Now suppose there is a  $C_f \in \text{ACC}(\varphi)$ . So  $(\exists D \in \text{SET}(\varphi)) D^+ \subseteq C_f$ , hence  $(\exists E \in \text{BAS}(\text{SET}(\varphi)^+)) E \subseteq C_f$ , which implies  $(\exists K \in \text{POS}) K \subseteq C_f$ . But this yields  $C_f \in \text{CLIQUE}$ , – a contradiction to Lemma 1. So  $\text{NEG} \cap \text{ACC}(\varphi) = \emptyset$ , i.e.  $\text{NEG} \subseteq \text{REJ}(\varphi)$ . ■

**Theorem 22** *Suppose that  $\varphi \in \mathcal{A}$  provides affirmative solution of  $\text{CLIQUE}(k^4, k)$ . Then for sufficiently large  $k$ ,  $\lfloor \varphi \rfloor > k^{\frac{4}{7}\sqrt{k}}$ .*

**Proof.** Let  $\varphi \in \mathcal{A}$  be any solution in question. We assume that any  $G \in \mathcal{G}$  is represented by the canonical input  $\vartheta_G \in \text{VAS}$ ,  $\vartheta_G(i) := \begin{cases} 1, & \text{if } \pi(i) \in G, \\ 0, & \text{else.} \end{cases}$  By the assumption we have  $G \in \text{CLIQUE} \Leftrightarrow \|\varphi\|_{\vartheta_G} = 1$ . Then by Definition 14, for any given  $\vartheta \in \text{VAS}$  we obtain

$$\begin{aligned} \|\text{CLIQUE}\|_{\vartheta} = 1 &\Rightarrow (\exists G \in \text{CLIQUE}) \|\varphi\|_{\vartheta_G} = 1 \\ &\Rightarrow (\exists G \in \text{CLIQUE}) (\vartheta = \vartheta_G) \Rightarrow \|\varphi\|_{\vartheta} = 1, \end{aligned} \quad (1)$$

$$\begin{aligned} \|\varphi\|_{\vartheta} = 1 &\Rightarrow (\exists G \in \mathcal{G}) (\vartheta = \vartheta_G \ \& \ \|\varphi\|_{\vartheta_G} = 1) \\ &\Rightarrow (\exists G \in \text{CLIQUE}) \|\varphi\|_{\vartheta_G} = 1 \Rightarrow \|\text{CLIQUE}\|_{\vartheta} = 1, \end{aligned} \quad (2)$$

which by Lemma 15 yields  $\|\text{CLIQUE}\|_{\vartheta} = 1 \Leftrightarrow \|\varphi\|_{\vartheta} = 1 \Leftrightarrow \|\text{SET}(\varphi)\|_{\vartheta} = 1$ . Thus  $\text{SET}(\varphi) \sim \text{CLIQUE}$ . The assertion now follows from Theorem 13 and Lemma 21. ■

**Corollary 23**  *$\text{CLIQUE}(k^4, k)$  is not solvable by DMN  $(\vee, \wedge, \neg)$ -circuits of the size polynomial in  $k$ .*

**Proof.** This is because  $\lfloor \varphi \rfloor$  is the minimum size of circuit representations of formula  $\varphi$ . Note that  $\text{SET}(\varphi)^+$  might be different from analogous DNF presentation of underlying positive (hereditarily) subformula  $\varphi^+$  (cf. last remark in 2.3.1). Thus, loosely speaking, there is no obvious correlation between  $\lfloor \varphi \rfloor$  and its “purely monotone” counterpart  $\lfloor \varphi^+ \rfloor$ . ■

### 3.2 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 De Morgan rules 1–4.

1.  $\neg \top \hookrightarrow \perp, \neg \perp \hookrightarrow \top$ .
2.  $\neg(\varphi \vee \psi) \hookrightarrow \neg\varphi \wedge \neg\psi$ .
3.  $\neg(\varphi \wedge \psi) \hookrightarrow \neg\varphi \vee \neg\psi$ .
4.  $\neg\neg\varphi \hookrightarrow \varphi$ .

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

**Lemma 24**  $\lfloor \varphi^* \rfloor \leq 2 \lfloor \varphi \rfloor$  holds for any  $\varphi \in \mathcal{B}$ .

**Proof.** See e.g. Appendix C. ■

**Theorem 25** Suppose that  $\varphi \in \mathcal{B}$  provides affirmative solution of  $\text{CLIQUE}(k^4, k)$ . Then for sufficiently large  $k$ ,  $\lfloor \varphi \rfloor > k^{\frac{4}{7}\sqrt{k}}$ .

**Proof.**  $\lfloor \varphi \rfloor > \frac{1}{2}k^{\frac{4}{7}\sqrt{k}}$  follows directly from Theorem 22 and Lemma 24. The required refinement is obtained as in Theorem 13 via  $\lfloor \varphi \rfloor \geq \frac{1}{2}m^{(\frac{1}{6}-\varepsilon)m^{\frac{1}{8}}} > m^{\frac{1}{7}m^{\frac{1}{8}}} = k^{\frac{4}{7}\sqrt{k}}$  (cf. Appendix A). ■

**Corollary 26**  $\mathbf{NP} \not\subseteq \mathbf{P/poly}$ . In particular  $\mathbf{P} \subsetneq \mathbf{NP}$  and hence  $\mathbf{P} \neq \mathbf{NP}$ .

**Proof.** Boolean circuit complexity is quadratic in deterministic time (cf. e.g. [4]: Proposition 11.1, [8]: Theorem 9.30). Hence the assertion easily follows from Theorem 25 as  $\text{CLIQUE}(k^4, k)$  is NP complete. ■

**Remark 27** DMN case is crucial for our proof. Indeed, there are monotone problems in  $\mathbf{P}$  (e.g. *PERFECT MATCHING*) that require exponential-size monotone circuits (cf. [6], [9]). Note that our double-graph generalization of plain-graph approach used in familiar proofs for monotone circuits (formulas) leads to a more sophisticated approximations than the ones discussed in [7], [11], [12]. In contrast to [7], we approximate only positive parts of double graphs (see Definition 6); the admissibility thereof is justified in Ch. 2.1.4 (which is a loose recollection of [13]: Ch. 2.1–2.2).

### 3.3 Application

Denote by  $\mathcal{A}_0$  positive (or 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 any boolean CNF formula  $\varphi \in \mathcal{A}$  (or just any CNF  $\varphi \in \mathcal{A}_0$ ) into equivalent DNF formula  $f(\varphi) \in \mathcal{A}$ ,  $\varphi \sim f(\varphi)$ .

**Proof.** Suppose  $(\forall \vartheta \in \text{VAS}) (\|\varphi\|_{\vartheta} = 1 \Leftrightarrow \|f(\varphi)\|_{\vartheta} = 1 \Leftrightarrow \|\neg f(\varphi)\|_{\vartheta} = 0)$ . Thus  $\varphi \in \text{SAT} \Leftrightarrow f(\varphi) \in \text{SAT} \Leftrightarrow \neg f(\varphi) \notin \text{VAL}$ , while by the assumption the size of  $f(\varphi)$  is polynomial in that of  $\varphi$ . 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  $\varphi$ .<sup>6</sup> Now general CNF validity problem  $(\neg f(\varphi))^* \in^? \text{VAL}$  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. ■

<sup>6</sup>The difference between plain (linear) and circuit length is inessential for CNF and/or DNF formulas under consideration.

## 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)
- [3] W. T. Gowers, *Razborov’s method of approximations*,  
gowers.files.wordpress.com/2009/05/razborov2.pdf
- [4] C. H. Papadimitriou, **Computational Complexity**, Addison-Wesley (1995)
- [5] 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)
- [6] 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)
- [7] A. A. Razborov, *On the method of approximation*, Proc. of the 21st Annual Symposium on Theory of Computing, 167–176 (1989)
- [8] M. Sipser, **Introduction to the Theory of Computation**, PWS Publishing (1997)
- [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)
- [11] N. Blum, *A Solution of the P versus NP Problem*,  
arXiv.org/pdf/1708.03486v1.pdf (revised as [12])
- [12] N. Blum, *On the Approximation Method and the P versus NP Problem*,  
arXiv.org/pdf/1708.03486v3.pdf
- [13] L. Gordeev, *Toward combinatorial proof of  $P < NP$* , CiE 2006, Swansea, UK, Report # CSR 7-2006, 119–128 (2006)

## 4 Appendix A

We have  $\ell = m^{\frac{1}{8}}$ ,  $p = \ell \log_{1.5} m$ ,  $L = (p-1)^\ell \ell!$ ,  $k := m^{\frac{1}{4}}$ .

$$\text{Hence } \ell! \sim \sqrt{2\pi\ell} \left(\frac{\ell}{e}\right)^\ell = \sqrt{2\pi m^{\frac{1}{8}}} \left(\frac{m^{\frac{1}{8}}}{e}\right)^{m^{\frac{1}{8}}} = \sqrt{2\pi} \frac{m^{\frac{1}{16} + \frac{1}{8}m^{\frac{1}{8}}}}{e^{m^{\frac{1}{8}}}} < m^{\frac{1}{8}m^{\frac{1}{8}}},$$

$$(p-1)^\ell < p^\ell = \left(m^{\frac{1}{8}} \log_{1.5} m\right)^{m^{\frac{1}{8}}} < m^{(\frac{1}{8}+\varepsilon)m^{\frac{1}{8}}}, \text{ for any chosen } \varepsilon > 0,$$

$$L = (p-1)^\ell \ell! < m^{(\frac{1}{8}+\varepsilon)m^{\frac{1}{8}}} \cdot m^{\frac{1}{8}m^{\frac{1}{8}}} = m^{(\frac{1}{4}+\varepsilon)m^{\frac{1}{8}}} \text{ and hence } L^2 < m^{(\frac{1}{2}+\varepsilon)m^{\frac{1}{8}}}.$$

$$\text{Moreover } \left(\frac{m-\ell}{k}\right)^\ell = \left(\frac{m-m^{\frac{1}{8}}}{m^{\frac{1}{4}}}\right)^{m^{\frac{1}{8}}} > \left(m^{\frac{3}{4}} - 1\right)^{m^{\frac{1}{8}}} > m^{\frac{2}{3}m^{\frac{1}{8}}}.$$

$$\text{Hence } \left(\frac{m-\ell}{k}\right)^\ell L^{-2} > m^{\frac{2}{3}m^{\frac{1}{8}}} \cdot m^{-(\frac{1}{2}+\varepsilon)m^{\frac{1}{8}}} = m^{(\frac{1}{6}-\varepsilon)m^{\frac{1}{8}}} > m^{\frac{1}{7}m^{\frac{1}{8}}} \text{ and}$$

$$\frac{1}{3}L^{-2} (1.5)^p = \frac{1}{3}L^{-2} m^{\frac{1}{8}} > m^{(\frac{1}{2}-\varepsilon)m^{\frac{1}{8}}} > m^{\frac{1}{3}m^{\frac{1}{8}}}. \blacksquare$$

## 5 Appendix B: Proof of Lemma 11

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

$$\begin{aligned} 1. \quad & \partial^{\text{POS}}(\varphi \vee \psi) = \text{POS} \cap \text{ACC}^{\text{POS}}(\text{SET}(\varphi \vee \psi)) \cap \text{REJ}^{\text{POS}}(\text{APR}(\varphi \vee \psi)) \\ & \subseteq \text{POS} \cap \text{ACC}^{\text{POS}}(\text{SET}(\varphi \vee \psi)) \cap \text{REJ}^{\text{POS}}(\text{APR}(\varphi) \cup \text{APR}(\psi)) \cup \\ & \quad \text{POS} \cap \text{ACC}^{\text{POS}}(\text{APR}(\varphi) \cup \text{APR}(\psi)) \cap \text{REJ}^{\text{POS}}(\text{APR}(\varphi \vee \psi)) \\ & = \text{POS} \cap \text{ACC}^{\text{POS}}(\text{SET}(\varphi \vee \psi)) \cap \text{REJ}^{\text{POS}}(\text{APR}(\varphi) \cup \text{APR}(\psi)) \cup \\ & \quad \text{POS} \cap \text{ACC}^{\text{POS}}(\text{APR}(\varphi) \cup \text{APR}(\psi)) \cap \text{REJ}^{\text{POS}}(\text{APR}(\varphi) \sqcup \text{APR}(\psi)) \\ & = \partial_{\sqcup}^{\text{POS}}(\text{APR}(\varphi), \text{APR}(\psi)) \cup \\ & \quad \text{POS} \cap \text{ACC}^{\text{POS}}(\text{SET}(\varphi \vee \psi)) \cap \text{REJ}^{\text{POS}}(\text{APR}(\varphi) \cup \text{APR}(\psi)) \\ & = \partial_{\sqcup}^{\text{POS}}(\text{APR}(\varphi), \text{APR}(\psi)) \cup \\ & \quad \text{POS} \cap \text{ACC}^{\text{POS}}(\text{SET}(\varphi) \cup \text{SET}(\psi)) \cap \text{REJ}^{\text{POS}}(\text{APR}(\varphi) \cup \text{APR}(\psi)) \\ & = \partial_{\sqcup}^{\text{POS}}(\text{APR}(\varphi), \text{APR}(\psi)) \cup \\ & \quad [\text{POS} \cap \text{ACC}^{\text{POS}}(\text{SET}(\varphi)) \cap \text{REJ}^{\text{POS}}(\text{APR}(\varphi))] \cup \\ & \quad [\text{POS} \cap \text{ACC}^{\text{POS}}(\text{SET}(\psi)) \cap \text{REJ}^{\text{POS}}(\text{APR}(\psi))] \\ & = \partial_{\sqcup}^{\text{POS}}(\text{APR}(\varphi), \text{APR}(\psi)) \cup \partial^{\text{POS}}(\varphi) \cup \partial^{\text{POS}}(\psi). \\ 2. \quad & \partial^{\text{POS}}(\varphi \wedge \psi) = \text{POS} \cap \text{ACC}^{\text{POS}}(\text{SET}(\varphi \wedge \psi)) \cap \text{REJ}^{\text{POS}}(\text{APR}(\varphi \wedge \psi)) \\ & \subseteq \text{POS} \cap \text{ACC}^{\text{POS}}(\text{SET}(\varphi \wedge \psi)) \cap \text{REJ}^{\text{POS}}(\text{APR}(\varphi) \odot \text{APR}(\psi)) \cup \\ & \quad \text{POS} \cap \text{ACC}^{\text{POS}}(\text{APR}(\varphi) \odot \text{APR}(\psi)) \cap \text{REJ}^{\text{POS}}(\text{APR}(\varphi \wedge \psi)) \\ & = \text{POS} \cap \text{ACC}^{\text{POS}}(\text{SET}(\varphi \wedge \psi)) \cap \text{REJ}^{\text{POS}}(\text{APR}(\varphi) \odot \text{APR}(\psi)) \cup \\ & \quad \text{POS} \cap \text{ACC}^{\text{POS}}(\text{APR}(\varphi) \odot \text{APR}(\psi)) \cap \text{REJ}^{\text{POS}}(\text{APR}(\varphi) \sqcap \text{APR}(\psi)) \\ & = \partial_{\sqcap}^{\text{POS}}(\text{APR}(\varphi), \text{APR}(\psi)) \cup \\ & \quad \text{POS} \cap \text{ACC}^{\text{POS}}(\text{SET}(\varphi \wedge \psi)) \cap \text{REJ}^{\text{POS}}(\text{APR}(\varphi) \odot \text{APR}(\psi)) \\ & = \partial_{\sqcap}^{\text{POS}}(\text{APR}(\varphi), \text{APR}(\psi)) \cup \end{aligned}$$



$$\begin{aligned}
& \text{POS} \cap \text{ACC}^{\text{POS}}(\text{SET}(\varphi) \odot \text{SET}(\psi)) \cap \text{REJ}^{\text{POS}}(\text{APR}(\varphi) \odot \text{APR}(\psi)) \\
&= \partial_{\square}^{\text{POS}}(\text{APR}(\varphi), \text{APR}(\psi)) \cup \\
&\quad [\text{POS} \cap \text{ACC}^{\text{POS}}(\text{SET}(\varphi)) \cap \text{REJ}^{\text{POS}}(\text{APR}(\varphi))] \cup \\
&\quad [\text{POS} \cap \text{ACC}^{\text{POS}}(\text{SET}(\psi)) \cap \text{REJ}^{\text{POS}}(\text{APR}(\psi))] \\
&= \partial_{\square}^{\text{POS}}(\text{APR}(\varphi), \text{APR}(\psi)) \cup \partial^{\text{POS}}(\varphi) \cup \partial^{\text{POS}}(\psi). \\
3. \quad & \partial^{\text{NEG}}(\varphi \vee \psi) = \text{NEG} \cap \text{ACC}^{\text{NEG}}(\text{APR}(\varphi \vee \psi)) \cap \text{REJ}^{\text{NEG}}(\text{SET}(\varphi \vee \psi)) \\
&\subseteq \text{NEG} \cap \text{ACC}^{\text{NEG}}(\text{APR}(\varphi \vee \psi)) \cap \text{REJ}^{\text{NEG}}(\text{APR}(\varphi) \cup \text{APR}(\psi)) \cup \\
&\quad \text{NEG} \cap \text{ACC}^{\text{NEG}}(\text{APR}(\varphi) \cup \text{APR}(\psi)) \cap \text{REJ}^{\text{NEG}}(\text{SET}(\varphi \vee \psi)) \\
&= \text{NEG} \cap \text{ACC}^{\text{NEG}}(\text{APR}(\varphi) \sqcup \text{APR}(\psi)) \cap \text{REJ}^{\text{NEG}}(\text{APR}(\varphi) \cup \text{APR}(\psi)) \cup \\
&\quad \text{NEG} \cap \text{ACC}^{\text{NEG}}(\text{APR}(\varphi) \cup \text{APR}(\psi)) \cap \text{REJ}^{\text{NEG}}(\text{SET}(\varphi \vee \psi)) \\
&= \partial_{\sqcup}^{\text{NEG}}(\text{APR}(\varphi), \text{APR}(\psi)) \cup \\
&\quad \text{NEG} \cap \text{ACC}^{\text{NEG}}(\text{APR}(\varphi) \cup \text{APR}(\psi)) \cap \text{REJ}^{\text{NEG}}(\text{SET}(\varphi \vee \psi)) \\
&= \partial_{\sqcup}^{\text{NEG}}(\text{APR}(\varphi), \text{APR}(\psi)) \cup \\
&\quad \text{NEG} \cap \text{ACC}^{\text{NEG}}(\text{APR}(\varphi) \cup \text{APR}(\psi)) \cap \text{REJ}^{\text{NEG}}(\text{SET}(\varphi)) \cap \text{REJ}^{\text{NEG}}(\text{SET}(\psi)) \\
&= \partial_{\sqcup}^{\text{NEG}}(\text{APR}(\varphi), \text{APR}(\psi)) \cup \\
&\quad [\text{NEG} \cap \text{ACC}^{\text{NEG}}(\text{APR}(\varphi)) \cap \text{REJ}^{\text{NEG}}(\text{SET}(\varphi))] \cup \\
&\quad [\text{NEG} \cap \text{ACC}^{\text{NEG}}(\text{APR}(\psi)) \cap \text{REJ}^{\text{NEG}}(\text{SET}(\psi))] \\
&= \partial_{\sqcup}^{\text{NEG}}(\text{APR}(\varphi), \text{APR}(\psi)) \cup \partial^{\text{NEG}}(\varphi) \cup \partial^{\text{NEG}}(\psi). \\
4. \quad & \partial^{\text{NEG}}(\varphi \wedge \psi) = \text{NEG} \cap \text{ACC}^{\text{NEG}}(\text{APR}(\varphi \wedge \psi)) \cap \text{REJ}^{\text{NEG}}(\text{SET}(\varphi \wedge \psi)) \\
&\subseteq \text{NEG} \cap \text{ACC}^{\text{NEG}}(\text{APR}(\varphi \wedge \psi)) \cap \text{REJ}^{\text{NEG}}(\text{APR}(\varphi) \odot \text{APR}(\psi)) \cup \\
&\quad \text{NEG} \cap \text{ACC}^{\text{NEG}}(\text{APR}(\varphi) \odot \text{APR}(\psi)) \cap \text{REJ}^{\text{NEG}}(\text{SET}(\varphi \wedge \psi)) \\
&= \text{NEG} \cap \text{ACC}^{\text{NEG}}(\text{APR}(\varphi) \sqcap \text{APR}(\psi)) \cap \text{REJ}^{\text{NEG}}(\text{APR}(\varphi) \odot \text{APR}(\psi)) \cup \\
&\quad \text{NEG} \cap \text{ACC}^{\text{NEG}}(\text{APR}(\varphi) \odot \text{APR}(\psi)) \cap \text{REJ}^{\text{NEG}}(\text{SET}(\varphi \wedge \psi)) \\
&= \partial_{\sqcap}^{\text{NEG}}(\text{APR}(\varphi), \text{APR}(\psi)) \cup \\
&\quad \text{NEG} \cap \text{ACC}^{\text{NEG}}(\text{APR}(\varphi) \odot \text{APR}(\psi)) \cap \text{REJ}^{\text{NEG}}(\text{SET}(\varphi \wedge \psi)) \\
&= \partial_{\sqcap}^{\text{NEG}}(\text{APR}(\varphi), \text{APR}(\psi)) \cup \\
&\quad \text{NEG} \cap \text{ACC}^{\text{NEG}}(\text{APR}(\varphi) \odot \text{APR}(\psi)) \cap \text{REJ}^{\text{NEG}}(\text{SET}(\varphi) \odot \text{SET}(\psi)) \\
&= \partial_{\sqcap}^{\text{NEG}}(\text{APR}(\varphi), \text{APR}(\psi)) \cup \\
&\quad [\text{NEG} \cap \text{ACC}^{\text{NEG}}(\text{APR}(\varphi)) \cap \text{REJ}^{\text{NEG}}(\text{SET}(\varphi))] \cup \\
&\quad [\text{NEG} \cap \text{ACC}^{\text{NEG}}(\text{APR}(\psi)) \cap \text{REJ}^{\text{NEG}}(\text{SET}(\psi))] \\
&= \partial_{\sqcap}^{\text{NEG}}(\text{APR}(\varphi), \text{APR}(\psi)) \cup \partial^{\text{NEG}}(\varphi) \cup \partial^{\text{NEG}}(\psi).
\end{aligned}$$

■

## 6 Appendix C: Proof of Lemma 24

**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)  $y \in B$ ,  $\langle x, y \rangle \in E$ ,  $\lambda(y) \neq \neg$ .<sup>7</sup> 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  $\varphi^*$  provided that  $B$  is dag-like presentation of  $\varphi$ . 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  $[\varphi^*] \leq 2[\varphi]$  (for brevity we omit further details). ■

---

<sup>7</sup>The latter corresponds to trivial applications of the last De Morgan rule.