Intersection Theorems: A Potential Approach to Proof Complexity Lower Bounds

Yaroslav Alekseev
Technion – Israel Institute of Technology, Haifa, Israel

Nikita Gaevoy
Technion – Israel Institute of Technology, Haifa, Israel

Abstract

Recently, Göös et al. [14] showed that Res ↾ uSA = RevRes in the following sense: if a formula φ has refutations of size at most s and width/degree at most w in both Res and uSA, then there is a refutation for φ of size at most poly$(s \cdot 2^w)$ in RevRes. Their proof relies on the TFNP characterization of the aforementioned proof systems.

In our work, we give a direct and simplified proof of this result, simultaneously achieving better bounds: we show that if for a formula φ there are refutations of size at most s in both Res and uSA, then there is a refutation of φ of size at most poly(s) in RevRes. This potentially allows us to "lift" size lower bounds from RevRes to Res for the formulas for which there are upper bounds in uSA. This kind of lifting was not possible before because of the exponential blow-up in size from the width.

Similarly, we improve the bounds in another intersection theorem from [14] by giving a direct proof of Res ↾ uNS = RevResT.

Finally, we generalize those intersection theorems to some proof systems for which we currently do not have a TFNP characterization. For example, we show that Res(⊕) ↾ u-wRes(⊕) = RevRes(⊕), which effectively allows us to reduce the problem of proving Pigeonhole Principle lower bounds in Res(⊕) to proving Pigeonhole Principle lower bounds in RevRes(⊕), a potentially weaker proof system.

2012 ACM Subject Classification Theory of computation → Proof complexity

Keywords and phrases proof complexity, intersection theorems

Digital Object Identifier 10.4230/LIPIcs.ITCS.2026.8

Related Version *Full Version*: https://eccc.weizmann.ac.il/report/2025/160/

Funding *Yaroslav Alekseev*: Supported by ISF grant 507/24.

Acknowledgements We want to thank Yuval Filmus for the fruitful discussions.

1 Introduction

Propositional proof systems are used to certify that given Boolean formulas are unsatisfiable. Cook and Rekhow [9] noticed that NP ≠ coNP implies that for every propositional proof system, there is a family of hard formulas that require superpolynomial proof size. However, currently, we cannot prove superpolynomial proof-size lower bounds for many particular proof systems.

In this paper, we study a new promising direction in proving proof complexity lower bounds, which is called *intersection theorems*. Intersection theorems in proof complexity take their origin from TFNP intersection theorems. The complexity class TFNP consists of total search problems whose solutions can be verified in NP. This means that every valid input is guaranteed to have at least one correct output, and any proposed output can be efficiently checked – even though actually finding such an output may be difficult. These problems are


© Yaroslav Alekseev and Nikita Gaevoy;
licensed under Creative Commons License CC-BY 4.0

often categorized into subclasses according to the type of reasoning that proves solutions must exist, which can also be interpreted as the kind of inherently inefficient algorithm that could, in principle, be used to solve them.

Initially, it was proved by Fearnley et al. [13] that CLS class is equal to PPAD ∩ PLS. After that, many other TFNP intersections were proved [14, 17]. Given those TFNP intersections and the proof complexity characterizations of the corresponding TFNP classes, one can naturally get *proof complexity intersection theorems*. Due to the nature of these characterizations, all the intersection theorems have the following form: suppose that formula φ has a refutation of size s and width (or degree) d in both proof systems P and Q. Then there is a refutation of size $\text{poly}(s \cdot 2^w)$ and width/degree $O(d)$ in some other proof system H.

[14, 17] showed that those kind of intersection theorems actually make sense by providing an example of proof systems P, Q and H, where $P \curlywedge Q = H$, but H is strictly weaker than both P and Q. Now, imagine that for some formula φ we were able to prove a superpolynomial size lower bound in the proof system H and a polynomial size upper bound in the proof system Q. Ideally, we would like to use both of these facts to prove a size lower bound in the system P. Unfortunately, the aforementioned intersection theorems only give us a $\max(w, \log s)$ lower bound in this case.

In this paper, we address this issue by giving a simplified and direct proof that captures *all known proof complexity intersection theorems*, without getting an exponential size blow-up from width. Moreover, we extend intersection theorems to proof systems without known TFNP characterizations or even lower bounds.

1.1 Our Results

Blackboard Proofs

In this work, we introduce a new framework for proving intersection theorems, which will use a *blackboard* as the key element. Informally, this means that we consider proof systems using some inference rules, and every time we apply the inference rule in our derivation, we replace the premises with the conclusion. This notion has some similarities with bounded clause space (see [1, 3, 12]), although they are not directly related.

This framework allows us to define several classes of proof systems:

- Reversible proof systems. These proof systems will be the base of our work. The key property of these proof systems is that if we can derive a collection of clauses $\mathcal{F}$ from $\mathcal{G}$, then we can also derive $\mathcal{G}$ from $\mathcal{F}$. The most natural example of such a proof system is *Reversible Resolution* [14].
- Proof systems with the Copy rule. These proof systems allow to replace any clause with two copies of the clause. Intuitively, this rule serves to remove the blackboard property. Most of the classical systems such as Resolution and AC^0-Frege belong to this class.
- Proof systems with *catalyst*. This is a new class of proof systems, usually with a reversible and strongly sound set of rules, that allows the initial blackboard state to contain some *catalyst*, which is some arbitrary set of clauses. However, to ensure soundness, we require the final state of the board also to contain the clauses of the *catalyst*. Reversible Resolution with a catalyst, which is equivalent to Unary Weighted Resolution [7], serves as a prime example of a proof system from this class.

Informally, our main Theorem can be stated as follows:

▶ **Theorem 1** (Informal statement of Theorem 21). *Let* RevP *be a proof system formed by a reasonable set of reversible rules* $\mathcal{R}$*,* P *be a proof system formed by* $\mathcal{R}$ + Copy*, and* CatP *be a catalytic version of* RevP*. Then*

RevP *is p-equivalent to* P $\curlywedge$ CatP.

We also prove this theorem for the case of proof systems with *terminals*, i.e. proof systems in which the final state of the blackboard consists of $\bot$ and some weakenings of clauses from the initial formula φ.

Corollaries and parameters

Theorem 1 immediately implies the following corollaries:

- RevRes is p-equivalent to Res $\curlywedge$ uSA (Theorem 24).
- RevRes(k) is p-equivalent to Res(k) $\curlywedge$ u-wRes(k) (Theorem 28).
- Informally, reversible bounded depth Frege $\mathcal{F}$ is p-equivalent to $\mathcal{F}^{\text{Copy}}$ $\curlywedge$ Cat$\mathcal{F}$ (Theorem 29).
- RevRes($\oplus$) is p-equivalent to Res($\oplus$) $\curlywedge$ u-wRes($\oplus$) (Theorem 26).

For the definition of the aforementioned proof systems, we refer to Section 4 (see also Appendix A). All these corollaries also have versions with terminals. The first two corollaries can be viewed as improvements of similar results from [10, 14], achieving better parameters. More precisely, in Theorem 1, we prove p-equivalence in a more general sense compared to the previous works: we show that if there are refutations of size S in both P and CatP, then there is a refutation of size poly(S) in RevP, while in previous results there was a $2^{O(w)}$ blow-up in the size.

The latter two corollaries are novel, and achieving them through TFNP seems unlikely because we do not have a TFNP characterization for these proof systems.

We use our intersection theorems to reduce the problem of proving lower bounds in stronger systems to some potentially weaker systems. For example, we can show the following corollary:

▶ **Corollary 2** (Informal statement of Corollary 27)**.** *Superpolynomial lower bounds for Pigeonhole Principle in* RevRes($\oplus$) *imply superpolynomial lower bounds for Pigeonhole Principle in* Res($\oplus$)*.*

This corollary raises the following natural question:

▶ **Question 3.** *Can we prove superpolynomial lower bounds for Pigeonhole Principle in* RevRes($\oplus$)*?*

Pigeonhole principle is one of the most famous examples of an unsatisfiable CNF formula, which is hard to refute in many classical proof systems (see [4, 15, 18]). Although it is not clear whether RevRes($\oplus$) is weaker than Res($\oplus$), it seems to be highly likely due to the fact that RevRes is exponentially weaker than Resolution (see [14]). Given the recent progress on Res($\oplus$) (see [2, 5, 6, 11]), it might be possible that RevRes($\oplus$) is a right candidate for solving the long-standing question of proving Res($\oplus$) lower bounds. It might also be possible to use proof systems different from RevRes($\oplus$) to prove lower bounds through intersection theorems. The only known limitation to the choice of the proof system is the feasible disjunction property [16].

Other intersection theorems

Although our framework covers most of the known intersection theorems, there are some theorems from [17] which cannot be expressed in our language. However, in the proof complexity formulation, the proofs are quite succinct, as we show in Section 5.

1.2 Organization of the paper

In Section 2, we define the framework we work with, provide formal definitions of the proof systems, and give basic examples of them. In Section 3, we explain the techniques used in the intersection theorem and provide the proof itself. In Section 4, we explore the direct applications of our main result. Finally, we give a direct proof of the other intersection theorems in Section 5.

2 Preliminaries

We start by defining a general framework for the proof complexity intersection theorems, which is slightly different from the one used in both [14] and [17] in the sense that it does not require the size of the resulting refutation to depend on anything besides the *sizes* of the initial refutations.

Following Cook and Reckhow [9], a propositional proof system for CNF is a polynomial-time algorithm $P\colon \{0,1\}^* \times \{0,1\}^* \to \{0,1\}$ such that:

- If $\varphi \in \{0,1\}^*$ is an encoding of unsatisfiable CNF, then there is a refutation π such that
$$P(\varphi, \pi) = 1.$$
- If φ is an encoding of a satisfiable CNF or not an encoding of a CNF, then for any refutation π
$$P(\varphi, \pi) = 0.$$

We say that the size of the refutation π is the length of its binary encoding. For an unsatisfiable CNF formula φ we denote by $\mathrm{Size}_P(\varphi)$ the size of the smallest π such that $P(\varphi, \pi) = 1$.

▶ **Definition 4** (Proof system intersection). *Let P and Q be two propositional proof systems. The proof system $P \curlywedge Q$ is defined as follows: for a CNF formula φ, any refutation in $P \curlywedge Q$ is a pair (ζ, ξ), where ζ is a valid refutation of φ in P and ξ is a valid refutation of φ in Q.*

We say that a propositional proof system P *p-simulates* a propositional proof system Q if there is a polynomial-time function $f\colon \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*$ such that

$$P(\varphi, \pi) = 1 \iff Q(\varphi, f(\varphi, \pi)) = 1.$$

If P p-simulates Q and Q p-simulates P, we say that P and Q are *p-equivalent*.

2.1 Inference-based proof systems

In this work, we focus on inference-based proof systems. One of the best-studied examples of inference-based proof systems is the *Resolution proof system*, which operates using *clauses*. A clause is a finite disjunction of literals, meaning Boolean variables x or their negations $\neg x$. The empty clause is represented by $\bot$.

The system can be defined as follows.

▶ **Definition 5** (Resolution). *Let $\varphi = C_1 \wedge C_2 \wedge \cdots \wedge C_m$ be an unsatisfiable CNF formula over variables $x_1, \ldots, x_n$. A Resolution refutation of φ is a sequence of* clauses *$P_1, P_2, \ldots, P_r$, where $P_r = \bot$ and each P_i is either equal to one of the C_j or is derived by one of the following rules:*

$$\frac{A \vee x \quad A \vee \neg x}{A}\ \textit{(Cut)} \qquad \frac{A}{A \vee B}\ \textit{(Weakening)} \qquad \frac{}{x \vee \neg x}\ \textit{(Excluded Middle).}$$

The size *of the Resolution derivation is r (up to a polynomial factor in the sense of Cook and Reckhow), and* the width *of the derivation is the maximum width (that is, the number of literals) among the P_i.*

▶ Remark 6. There are two primary methods for defining Resolution: one involves viewing clauses as *sets*, and the other involves viewing clauses as multisets, allowing for the derivation of the excluded middle. In this paper, we choose the latter method, so clauses such as $x \vee x \vee y$ may potentially appear in the derivation. For example, to derive $x \vee A$ from $x \vee x \vee A$, we can use following derivation.

$$\dfrac{x \vee x \vee A \qquad \dfrac{\dfrac{}{x \vee \neg x}\ \text{Excluded Middle}}{x \vee \neg x \vee A}\ \text{Weakening}}{x \vee A}\ \text{Cut}$$

We consider several extensions and restrictions of Resolution. Some of them operate with more general entries. We define those first.

Disjunctions of terms

We consider more general entities such as disjunctions of *XORs*, disjunctions of k-conjunctions, or even AC^0-formulas with a top OR gate. All these entities share a common feature: a top OR gate.

For the set of variables $x_1, x_2, \ldots, x_n$ we define a *collection of terms* $\mathcal{T}_n$ as a collection of binary strings, denoting functions $f_T \colon \{0,1\}^n \to \{0,1\}$, including functions equal to x_i and $\neg x_i$ for all i. Given $\mathcal{T} = \bigcup_n \mathcal{T}_n$, we naturally define $\mathcal{T}$-clauses as disjunctions of terms from $\mathcal{T}_n$ for some n: each disjunction of terms $D = T_1 \vee T_2 \vee \cdots \vee T_k$ corresponds to a function $f_D = f_{T_1} \vee f_{T_2} \vee \cdots \vee f_{T_k}$. We denote the collection of all $\mathcal{T}$-clauses as $\mathcal{D}(\mathcal{T})$. Most of the time, we omit the parameter $\mathcal{T}$ in our notation and just write "clauses" instead. By the *size* of a clause we denote the total length of all its terms, interpreted as binary strings.

Although we do allow repetitions of terms, we do not distinguish between two disjunctions if they differ only by a permutation (i.e., $T_1 \vee T_2 = T_2 \vee T_1$). $\mathcal{D}(\mathcal{T})$ includes the empty clause corresponding to the empty disjunction (and equal to the constant 0), which we also denote by $\bot$.

If the collection of terms $\mathcal{T}$ admits a notion of width, we define *width* of a $\mathcal{T}$-clause as the sum of widths of terms it contains.[1] The system of disjunctions of terms $D_1, D_2, \ldots, D_k \in \mathcal{D}(\mathcal{T})$ is called *unsatisfiable* if

$$f_{D_1} \wedge f_{D_2} \wedge \cdots \wedge f_{D_k} \equiv 0.$$

Inference rules

An inference rule is a pair $(\mathcal{F}, \mathcal{G})$, where both $\mathcal{F}$ and $\mathcal{G}$ are multisets of clauses. The clauses in $\mathcal{F}$ are called premises, and the clauses in $\mathcal{G}$ are called conclusions.

▶ **Definition 7.** *We say that a set of inference rules $\mathcal{R}$ is* stable under weakening*, if for each rule $(\mathcal{F}, \mathcal{G})$ and term T, if $(\mathcal{F}, \mathcal{G}) \in \mathcal{R}$, then $(\mathcal{F} \vee T, \mathcal{G} \vee T) \in \mathcal{R}$, where $\mathcal{F} \vee T$ denotes the collection of clauses $F \vee T$ for all $F \in \mathcal{F}$.*

[1] Usually, the width of a term is constant 1.

Blackboard derivations

In this work, we consider *blackboard inference-based proof systems*, where each time we apply an inference rule, we *replace the premises with the conclusions*. So, at each particular moment of time, we maintain a multiset of clauses.

▶ **Definition 8** (Soundness). *An inference rule $\mathcal{F} \vdash \mathcal{G}$ is* sound *if any truth assignment that satisfies all the terms in $\mathcal{F}$, also satisfies all the terms in $\mathcal{G}$.*

▶ **Definition 9** (Blackboard inference-based derivation). *Given a set of sound inference rules $\mathcal{R}$, an initial multiset of clauses $\mathcal{L}$, and a goal multiset of clauses $\mathcal{H}$, a derivation of $\mathcal{H}$ from $\mathcal{L}$, using the rules in $\mathcal{R}$, is a sequence of multisets of clauses $\mathcal{L}_1, \mathcal{L}_2, \ldots, \mathcal{L}_t$, where*

- *$\mathcal{L}_1 = \mathcal{L}$ and $\mathcal{L}_t = \mathcal{H}$.*
- *For $1 < i \leq t$, $\mathcal{L}_i$ is derived from $\mathcal{L}_{i-1}$ by one of the rules from $\mathcal{R}$ in the sense that if this rule can derive a multiset of clauses $\mathcal{G}$ from $\mathcal{F}$, then $\mathcal{F}$ is a subset of $\mathcal{L}_{i-1}$ and*

$$\mathcal{L}_i = (\mathcal{L}_{i-1} \setminus \mathcal{F}) \cup \mathcal{G}.$$

The length of this derivation is t and the size is the total size of all clauses appearing in premises and conclusions of the rules applied in the derivation. The width is the maximum width of a term appearing in $\mathcal{L}_i$ (if it is possible to define such a measure for a clause).

▶ Remark 10. The size in Definition 9 is the same as in the Cook-Reckhow definition. In most cases, the size and the length of the derivation differ only by a polynomial factor. However, even in other cases, all of our theorems preserve both size and length, even though we state them only for size.

Now we are ready to define blackboard proof systems.

▶ **Definition 11** (Blackboard proof system). *We say that the collection of sound inference rules $\mathcal{R}$ forms a blackboard proof system if for any unsatisfiable collection of terms $\mathcal{P} = \{C_1, C_2, \ldots, C_m\}$ there exist multisets of terms $\mathcal{L}$ and $\mathcal{H}$ such that*

- *If $C \in \mathcal{L}$, then $C \in \mathcal{P}$.*
- *$\bot \in \mathcal{H}$ and there is a derivation with rules from $\mathcal{R}$ of $\mathcal{H}$ from $\mathcal{L}$.*

2.2 Reversible rules, copy rule, and applications of weakening

Due to the nature of our work, we consider some particular classes of rules.

▶ **Definition 12** (Strong soundness). *An inference rule $\mathcal{F} \vdash \mathcal{G}$ is* strongly sound *if for any truth assignment, the number of falsified clauses in $\mathcal{F}$ equals the number of falsified clauses in $\mathcal{G}$.*

▶ **Definition 13** (Reversible rules). *We say that a collection of rules $\mathcal{R}$ is* reversible *if*

- *All the rules in $\mathcal{R}$ are strongly sound.*
- *For any pair $(\mathcal{F}, \mathcal{G}) \in \mathcal{R}$, the pair $(\mathcal{G}, \mathcal{F})$ also belongs to $\mathcal{R}$.*

▶ **Definition 14** (Copy rule). *By the* copy *rule, we mean the following rule:*

$$\frac{C}{C \quad C}.$$

▶ Remark 15. The Copy rule is a sound rule, but not strongly sound.

▶ **Definition 16** (Efficient weakening). *Given a sound blackboard proof system P, we say that clause A is a* weakening *of clause B if there exists a derivation in P that starts with the single clause A and obtains a multiset of clauses containing B.*

We say that a proof system admits efficient weakening *if the system is stable under weakening and for any clauses C and D there exists a derivation of $C \vee D$ from C of size polynomial in $|C| + |D|$ and width equal to the width of $C \vee D$ (if the notion of width is applicable).*

▶ **Definition 17** (Inference with terminals). *Given an unsatisfiable formula φ, its refutation $\mathcal{L}$ in a blackboard proof system P is called an* inference with terminals *if the last step $\mathcal{L}_t$ of the inference consists of exactly one copy of the empty clause $\bot$ and weakenings of (not necessarily distinct) clauses of φ.*

Examples of proof systems.

- *Reversible Resolution* (RevRes) is a blackboard proof system with the following two *strongly sound reversible* rules.

$$\frac{C}{C \vee x \quad C \vee \neg x}\ \text{(Reversible Weakening)} \qquad \frac{C \vee x \quad C \vee \neg x}{C}\ \text{(Reversible Cut)}$$

$$\frac{}{x \vee \neg x}\ \text{(Excluded Middle)} \qquad \frac{}{x \vee \neg x}\ \text{(Reversed Excluded Middle)}$$

- *Resolution* (Res) has the same rules as RevRes with the addition of the *copy* rule. One can easily observe that this definition is equivalent to Definition 5.
- *Reversible Resolution with Terminals* (RevResT) has the same rules as RevRes, but has a restriction from Definition 17 of the last configuration of the board.

Note that all of the aforementioned proof systems admit efficient weakening in the sense of Definition 16.

2.3 Catalytic proof systems

We also need another generalization of strongly sound blackboard proof systems: catalytic proof systems.

▶ **Definition 18.** *A proof system Q is a* catalytic version *of a strongly sound blackboard proof system P if its proofs have the following form. Given an unsatisfiable formula φ, the proof starts with a collection $\mathcal{L}_1$ of possibly repeated clauses of φ and arbitrary* catalytic *clauses $D_1, D_2, \ldots, D_k$. Then, it proceeds with a blackboard derivation in P that ends in a state $\mathcal{L}_t$ that consists of the empty clause $\bot$, all catalytic clauses $D_1, D_2, \ldots, D_k$, and possibly some other clauses.*

▶ Remark 19. The strong soundness of P ensures that the number of falsified clauses is the same across all states $\mathcal{L}_i$ for any substitution. Therefore, since $\bot$ is falsified by any substitution and catalytic clauses appear both in $\mathcal{L}_1$ and $\mathcal{L}_t$, the refutation exists only for unsatisfiable formulas. Thus, catalytic proof systems are sound and complete.

Similarly to blackboard proof systems, we can also define a version of the derivation with terminals for catalytic proof systems.

▶ **Definition 20** (Catalytic derivation with terminals). *Similarly to Definition 17, we say that a derivation in a catalytic proof system is a* catalytic derivation with terminals *if the last step $\mathcal{L}_t$ consists of exactly one copy of the empty clause $\bot$, all catalytic clauses $D_1, D_2, \ldots, D_k$, and weakenings of clauses of the formula φ.*

Examples of catalytic proof systems.

- *Catalytic Reversible Resolution* is the catalytic version of the RevRes proof system. We show in Appendix A that this system is equivalent to *unary weighted Resolution* from [14] (u-wRes), which is also equivalent to uSA (see [7]).
- *Catalytic Reversible Resolution with Terminals* is the catalytic version of the RevRes proof system with terminals. This proof system is equivalent to *unary weighted Resolution with Terminals* from [14] (u-wResT) (see Appendix A), which is also equivalent to uNS (see [7]).

3 Main intersection theorem

In this section, we prove the following theorem:

▶ **Theorem 21.** *Suppose that the set of rules $\mathcal{R}$ over $\mathcal{D}(\mathcal{T})$ is reversible and admits efficient weakening. Let* RevP *be the proof system formed by $\mathcal{R}$,* P *be the proof system formed by* $\mathcal{R} + \text{Copy}$*, and* CatP *be the catalytic version of* RevP*. Then*

$$\text{RevP} \text{ is p-equivalent to } \text{P} \curlywedge \text{CatP}.$$

Moreover, if CatP^{T} *is the catalytic version of* RevP *with terminals and* RevP^{T} *is* RevP *with terminals, then*

$$\text{RevP}^{\text{T}} \text{ is p-equivalent to } \text{P} \curlywedge \text{CatP}^{\text{T}}.$$

More precisely, for any CNF φ if there are proofs of size at most S and width at most w in both P *and* CatP *(or* CatP^{T}*), then there is a proof of size $O(\text{poly}(S))$ and width at most $O(w)$ in* RevP *(*RevP^{T}*, respectively).*

First, we prove the statement without the terminals, and after that, we show how to extend the proof for the version with terminals. Here is a high-level idea of the proof without terminals:

- We want to directly simulate a P derivation in RevP step by step. We cannot do it directly since there is no way to simulate the Copy rule.
- To overcome this issue, instead of deriving one copy of each clause in the P derivation, we derive S copies of the clause at a time.
- Given S copies of an arbitrary clause C and a catalytic refutation of φ of size S, we will show that we can derive $S + 1$ copies of C with an additional use of clauses from φ. Formally, this statement is proved in Lemma 22. This allows us to efficiently simulate the Copy rule.

Proof. We begin by proving the version of Theorem 21 without terminals. Throughout the proof, we will use the following notation: by $k \cdot A$ we denote k copies of the clause A. For a multiset of clauses $\mathcal{L} = \{A_1, \dots, A_\ell\}$, we define

$$k \cdot \mathcal{L} = k \cdot A_1 \cup k \cdot A_2 \cup \dots \cup k \cdot A_\ell.$$

For a formula $\varphi = C_1 \vee C_2 \vee \dots \vee C_m$ we have a P derivation $\mathcal{N}_0, \mathcal{N}_1, \dots, \mathcal{N}_t$ of size at most S and width at most w, where $\mathcal{N}_0$ consists of the clauses of φ and $\bot \in \mathcal{N}_t$. Our goal is to simulate each step of this derivation in RevP. We will show that, given a blackboard state $\mathcal{M}_i$ such that

$$S \cdot \mathcal{N}_i \subseteq \mathcal{M}_i,$$

we can derive with a $\text{poly}(S)$ size derivation, given unlimited access to clauses from φ, a state $\mathcal{M}_{i+1}$ such that

$$S \cdot \mathcal{N}_{i+1} \subseteq \mathcal{M}_{i+1}.$$

Equivalently, this means that we can derive with a $\text{poly}(S)$ size derivation a state $\mathcal{M}_{i+1}$ from $\mathcal{M}_i \cup \mathcal{G}_i$, where all the $\mathcal{G}_i \subseteq \text{poly}(S) \cdot \{C_1, C_2, \ldots, C_m\}$. Having this derivation, we can construct a RevP-derivation where we add all $\mathcal{G}_i$ to the initial state, and carry each $\mathcal{G}_i$ until we get to the state $\mathcal{M}_i$, where we use it to derive $\mathcal{M}_{i+1}$.

We start with $\mathcal{M}_0 = S \cdot \mathcal{N}_0$. We have two cases at each step of simulation:

- $\mathcal{N}_{i+1}$ was derived from $\mathcal{N}_i$ by an application of any rule from $\mathcal{R}$, then we just apply this rule S times to $\mathcal{M}_i$ to derive $\mathcal{M}_{i+1}$.
- $\mathcal{N}_{i+1}$ was derived from $\mathcal{N}_i$ by an application of the Copy rule. In this case we use the fact that there is a CatP derivation of size S and width w and apply the following lemma S times to derive $\mathcal{M}_{i+1}$ from $\mathcal{M}_i$.

▶ **Lemma 22.** *Suppose that there is a* RevP *derivation of size S and width w from $\mathcal{L}$ to $\mathcal{L}'$, where $k \leq S$ and*

$$\{D_1, D_2, \ldots, D_k\} \cup \alpha_1 \cdot C_1 \cup \alpha_2 \cdot C_2 \cup \cdots \cup \alpha_m \cdot C_m = \mathcal{L},$$
$$\{D_1, D_2, \ldots, D_k, \bot\} \subseteq \mathcal{L}'.$$

Then for any clause A there are some parameters $\beta_1, \beta_2, \ldots, \beta_m$ such that $\beta_i \leq \alpha_i \cdot S$ and there is a RevP *derivation of size* $\text{poly}(S)$ *and width $w + w_{\text{RevP}}(A)$ from $\mathcal{P}$ to $\mathcal{P}'$, where*

$$k \cdot A \cup \beta_1 \cdot C_1 \cup \beta_2 \cdot C_2 \cup \cdots \cup \beta_m \cdot C_m = \mathcal{P},$$
$$(k+1) \cdot A \subseteq \mathcal{P}'.$$

Given Lemma 22 we get a RevP derivation of size $\text{poly}(S)$ and width $O(w)$ that starts with clauses from φ and ends with $\mathcal{M}_t \supseteq \bot$, which is enough for us.

Proof of Lemma 22. Consider a state $\mathcal{P}_0$ such that

$$k \cdot A \cup \alpha_1 \cdot C_1 \cup \alpha_2 \cdot C_2 \cup \cdots \cup \alpha_m \cdot C_m = \mathcal{P}_0,$$

By using RevP weakening derivation (see Definition 16), we can derive some multiset $\mathcal{Q}$ from $k \cdot A$ such that

$$\{D_1 \vee A, D_2 \vee A, \ldots, D_k \vee A\} \subseteq \mathcal{Q}.$$

Note that we can also derive $k \cdot A$ from $\mathcal{Q}$, since all the rules in RevP are reversible.

Now, by using the weakening derivation, we can derive from

$$\alpha_1 \cdot C_1 \cup \alpha_2 \cdot C_2 \cup \cdots \cup \alpha_m \cdot C_m$$

a multiset $\mathcal{H}$ such that

$$\alpha_1 \cdot (C_1 \vee A) \cup \alpha_2 \cdot (C_2 \vee A) \cup \cdots \cup \alpha_m \cdot (C_m \vee A) \subseteq \mathcal{H}.$$

Altogether, this allows us to derive a blackboard state $\mathcal{Q} \cup \mathcal{H}$ from $\mathcal{P}$ with size $O(S)$ and width $w + |A|$ derivation in RevP. Now, observe that the derivation of $\mathcal{L}'$ from $\mathcal{L}$ can be transformed into a derivation of $\mathcal{L}' \vee A$ from $\mathcal{L} \vee A$ (see Definition 7). Note that this derivation has size $\text{poly}(S)$ and width $w + |A|$.

So, we have a derivation in RevP

from $\mathcal{Q} \cup \mathcal{H}$ to $(\mathcal{Q} \cup \mathcal{H}) \setminus (\mathcal{L} \vee A) \cup (\mathcal{L}' \vee A)$.

Observe that $\mathcal{L} \vee A$ and $\mathcal{L}' \vee A$ both contain $\{D_1 \vee A, D_2 \vee A, \ldots, D_k \vee A\}$. Also, we know we did not use clauses from $\mathcal{Q} \setminus ((D_1 \vee A) \cup (D_2 \vee A) \cup \cdots \cup (D_k \vee A))$ to derive $(\mathcal{L}' \vee A)$. Finally, we know that $A \in \mathcal{L}' \vee A$. All together, this gives us

$$(\mathcal{Q} \cup \mathcal{H}) \setminus (\mathcal{L} \vee A) \cup (\mathcal{L}' \vee A) \supseteq \{A\} \cup \mathcal{Q}.$$

Finally, as mentioned before, from $\mathcal{Q}$ we can derive $k \cdot A$. By doing so, we get a state $\mathcal{P}'$, such that

$$(k+1) \cdot A \subseteq \mathcal{P}'.$$ ◀

Proof with terminals. From the proofs without the terminals, we know that we can construct *some* RevP-derivation starting in $\mathcal{H}_0$, consisting of clauses from φ only, and ending in $\mathcal{H}_m$, in which we have S copies of $\bot$. Now the main idea is the following: we want to copy $\bot$ and revert the clauses from $\mathcal{H}_m$ back into $\mathcal{H}_0$ by using the property of *reversibility*. To do so, we need the following generalization of Lemma 22.

▶ **Lemma 23.** *Suppose that there is a* RevP *derivation of size S and width w from $\mathcal{L}$ to $\mathcal{L}'$, where $k \leq S$ and $\mathcal{G}$ consists of weakening of clauses from φ and*

$$\{D_1, D_2, \ldots, D_k\} \cup \alpha_1 \cdot C_1 \cup \alpha_2 \cdot C_2 \cup \cdots \cup \alpha_m \cdot C_m = \mathcal{L},$$
$$\{D_1, D_2, \ldots, D_k, \bot\} \cup \mathcal{G} = \mathcal{L}'.$$

Then for any clause A there are some parameters $\beta_1, \beta_2, \ldots, \beta_m$ such that $\beta_i \leq \alpha_i \cdot S$ and there is a RevP *derivation of size* $\mathrm{poly}(S)$ *and width $w + w_{\mathrm{RevP}}(A)$ from $\mathcal{P}$ to $\mathcal{P}'$, where $\mathcal{G}'$ consists of weakenings of clauses from φ and*

$$k \cdot A \cup \beta_1 \cdot C_1 \cup \beta_2 \cdot C_2 \cup \cdots \cup \beta_m \cdot C_m = \mathcal{P},$$
$$(k+1) \cdot A \cup \mathcal{G}' = \mathcal{P}'.$$

Let $\mathcal{P}$ and $\mathcal{P}'$ be the states of the blackboard from Lemma 23, where we take $A = \bot$ and $\mathcal{L}$ and $\mathcal{L}'$ are the initial and final states of the $\mathrm{CatP}^{\mathrm{T}}$ refutation of φ. Now, given a derivation of $\mathcal{H}_m$ from $\mathcal{H}_0$, we transform it into a RevP derivation of $\mathcal{H}_m \cup (\mathcal{P} \setminus (S \cdot \bot))$ from $\mathcal{H}_0 \cup (\mathcal{P} \setminus (S \cdot \bot))$ by adding clauses from $(\mathcal{P} \setminus (S \cdot \bot))$ to all states in the derivation.

Now, from $\mathcal{H}_m \cup (\mathcal{P} \setminus (S \cdot \bot))$ we derive $\mathcal{H}_m \cup (\mathcal{P}' \setminus (S \cdot \bot))$ with Lemma 23. And here comes the main trick: we *revert* this derivation in the sense that we take the $\mathcal{H}_m$ part of our blackboard state and derive $\mathcal{H}_0$ from it. So, in the end, we get a RevP-proof, which starts with $\mathcal{H}_0 \cup (\mathcal{P} \setminus (S \cdot \bot))$ and ends with $\mathcal{H}_0 \cup (\mathcal{P}' \setminus (S \cdot \bot))$. The last state in this proof consists only of one copy of $\bot$ and weakenings of clauses from φ.

The only thing that remains is to prove Lemma 23. We only give a sketch of the proof since it is just a slight modification of the proof of Lemma 22.

Sketch of proof of Lemma 23. We use exactly the same construction as in Lemma 22. This allows us to produce the blackboard state $\mathcal{P}' = (k+1) \cdot A \cup \mathcal{G}'$. We want to show that $\mathcal{G}'$ consists only of weakenings from φ.

Indeed, all the clauses in $\mathcal{G}'$ may emerge from two sources:

- These clauses may result as a byproduct of the first step of the proof, which in our case derives $C_i \vee A$ from C_i. This step produces only weakenings of clause C_i by the definition of weakening (see Section 2.2).
- These clauses also emerge from the conclusion of the original catalytic derivation. $\mathcal{P}'$ does not contain any clauses from the catalyst; therefore, these clauses are weakenings of φ, as a refutation with terminals was used. ◀

◀

4 Direct applications of the intersection theorem

4.1 Res ⅄ u-wRes = RevRes

In Sections 2.2 and 2.3 we defined Resolution, Reversible Resolution, Reversible Resolution with Terminals, Unary Weighted Resolution (Catalytic Reversible Resolution in our notation), and Unary Weighted Resolution with Terminals.

The next two theorems are immediate corollaries of Theorem 21:

▶ **Theorem 24.** Res ⅄ u-wRes *is p-equivalent to* RevRes*. More precisely, for any CNF formula* φ*, if there is a refutation of size* S *and width* w *in both* Res *and* u-wRes*, then there is a* RevRes *refutation of* φ *of size* $\mathrm{poly}(S)$ *and width* $O(w)$*.*

▶ **Theorem 25.** Res ⅄ u-wResT *is p-equivalent to* RevResT*. More precisely, for any CNF formula* φ*, if there is a refutation of size* S *and width* w *in both* Res *and* u-wResT*, then there is a* RevResT *refutation of* φ *of size* $\mathrm{poly}(S)$ *and width* $O(w)$*.*

Both Theorem 24 and 25 are improvements of similar intersection theorems from [14], in the sense that the resulting size is $\mathrm{poly}(S)$ rather than $\mathrm{poly}(S) \cdot 2^{O(w)}$.

4.2 Res(⊕) ⅄ u-wRes(⊕) = RevRes(⊕)

Resolution over parities operates with the disjunctions of linear equations. In our notation, this means that the set of terms is the set of all linear equations. We define the set of rules of RevRes(⊕) as the following rules, together with their reversed versions:

$$\frac{}{(\ell = 0) \vee (\ell = 1)} \text{ (Excluded Middle)}$$

$$\frac{A \vee (\ell = 1) \qquad A \vee (\ell = 0)}{A} \text{ (Reversible Cut)}$$

$$\frac{A}{B} \text{ if } \neg A \text{ and } \neg B \text{ define the same linear subspace (Reversible Equivalence)}$$

The width of a clause A is then the number of linear equations in it.

If we add the Copy rule to this list, we get the Res(⊕) proof system. By u-wRes(⊕) we denote the catalytic version of RevRes(⊕). Similarly, we can define versions of these proof systems with terminals.

Note that currently it is not clear whether there is a TFNP formulation for the Res(⊕) proof system. The following theorem is an immediate corollary of Theorem 21:

▶ **Theorem 26.** Res(⊕) ⅄ u-wRes(⊕) *is p-equivalent to* RevRes(⊕) *and* Res(⊕) ⅄ u-wResT(⊕) *is p-equivalent to* RevResT(⊕)*.*

The Pigeonhole Principle (PHP_n^{n+1}, for short) is the following unsatisfiable formula:

$\bigvee_{j=1}^{n} p_{i,j}$ for $i \in [n+1]$,

$\neg p_{i,j} \vee \neg p_{k,j}$ for $i, k \in [n+1], j \in [n]$.

Theorem 26 implies the following surprising corollary:

▶ **Corollary 27.** *Suppose that* PHP_n^{n+1} *has a size* S *refutation in* $\mathrm{RevRes}(\oplus)$*. Then* PHP_n^{n+1} *has a* $\mathrm{Res}(\oplus)$*-refutation of the size* $\mathrm{poly}(S, n)$*.*

Proof. Clearly, u-wRes(⊕) p-simulates u-wRes, which is equiavlent to uSA, which admits polynomial size refuations of PHP_n^{n+1} (see [7], for example). ◀

We conjecture that it might be easier to prove lower bounds for PHP in RevRes(⊕) for the following reason: RevRes is strictly weaker than Res, so it is highly likely that RevRes(⊕) is strictly weaker than Res(⊕).

4.3 $\mathbf{Res}(k) \curlywedge \mathbf{u\text{-}wRes}(k) = \mathbf{RevRes}(k)$

The set of terms in the proof system RevRes(k) is the set of conjunctions of at most k literals. The width of a term is defined as the number of literals it contains. The rules of RevRes(k) are the following (together with their reverse):

$$\frac{C \vee \bigwedge_i l_i \qquad C \vee \bigvee_i \neg l_i}{A} \text{ (Cut)}$$

$$\frac{C \vee l_1 \quad \cdots \quad C \vee l_t}{C \vee \bigwedge_{i=1}^{t} l_i} \text{ (∧-Introduction)}$$

$$\frac{}{\bigwedge_i l_i \vee \bigvee_i \neg l_i} \text{ (Excluded Middle)}$$

Similarly to Res and Res(⊕), Res(k) is defined as RevRes(k) with the addition of the Copy rule. The catalytic version of RevRes(k) (which we call u-wRes(k)) and the versions of these proof systems with terminals are defined straightforwardly.

Again, the following theorem is an immediate corollary of Theorem 21:

▶ **Theorem 28.** $\mathrm{Res}(k) \curlywedge \text{u-wRes}(k)$ *is p-equivalent to* $\mathrm{RevRes}(k)$ *and* $\mathrm{Res}(k) \curlywedge \text{u-wResT}(k)$ *is p-equivalent to* $\mathrm{RevResT}(k)$*.*

Substituting $k = \mathrm{poly}\log(n)$, we obtain the intersection theorem from [10] with better parameters.

4.4 Fragments of Frege

In a more general setting, we can apply Theorem 21 to any fragment of the Frege system with reversible rules and supporting ∨-gates. This applies to systems like constant-depth Frege with ∨-gate on the top.

Formally, we can prove the following theorem:

▶ **Theorem 29.** *Let* $\mathcal{F}$ *be a blackboard proof system that has a complete and reversible set of rules over bounded-depth circuits with a top* ∨*-gate. Then* $\mathcal{F}^{\mathrm{Copy}} \curlywedge \mathrm{Cat}\mathcal{F}$ *is p-equivalent to* $\mathcal{F}$*.*

Given a Frege system with a set of sound inference rules $\mathcal{R}$, we can construct a reversible system using the following transformation for all rules (for simplicity, we show the case of two premises only).

$$\frac{C_1 \quad C_2}{D} \quad \longmapsto \quad \frac{C_1 \quad C_2}{D \quad E_1 \quad E_2},$$

where formulas E_1 and E_2 should encode the following Boolean functions:

$$E_1 = \{\neg C_1 + \neg C_2 - \neg D \geq 1\} \quad E_2 = \{\neg C_1 + \neg C_2 - \neg D \geq 2\}$$

This encoding can increase the size of the derivation only polynomially, and the depth of the derivation by at most a constant.

▶ Remark 30. In the case of unbounded depth Frege systems, Theorem 29 becomes trivial since both $\mathcal{F}$ and $\mathcal{F}^{\text{Copy}}$ are equivalent to the tree-like version of $\mathcal{F}$.

5 Other intersection theorems

Li, Pires, and Robere [17] proved the following TFNP intersection theorems:

$$\mathsf{SOL}_q = \mathsf{PPA}_q \cap \mathsf{PPADS}, \tag{1}$$

$$\mathsf{EOPL}_q = \mathsf{PPA}_q \cap \mathsf{SOPL}, \tag{2}$$

$$\mathsf{MaxOdd} = \mathsf{PPA} \cap \mathsf{PLS}. \tag{3}$$

These theorems imply the weaker versions of the following proof complexity intersection theorems:

1. SA_q is p-equivalent to NS^*_q ↓ uSA.
2. $\mathrm{RevResT}_{\mathcal{R}_q^-}$ is p-equivalent to $\mathrm{RevResT}_{\mathcal{R}_q}$ ↓ RevRes.
3. $\mathrm{RevResT}_{\mathcal{R}_2^{\text{Copy}}}$ is p-equivalent to $\mathrm{RevResT}_{\mathcal{R}_2}$ ↓ Res.

The proof of the first intersection theorem is the most succinct in the algebraic formulation. Since this formulation does not fit our framework, we postpone it to the Appendix B.

To define the proof systems appearing in the second and the third intersection theorems, we need to introduce the following rules:

$$\frac{C \ldots C}{} \quad (\mathbb{F}_q\text{-Elim}) \qquad \frac{}{C \ldots C} \quad (\mathbb{F}_q\text{-Intro})$$

where the two rules above allow us to remove q copies of an arbitrary clause C from a blackboard or add them, respectively. Also, we need the following rule:

$$\frac{C}{C \quad C \quad C} \quad (\mathbb{F}_2\text{-Copy}).$$

The set of rules $\mathcal{R}_q$ can be defined as

$$\mathcal{R}_q = \{\text{Rev-Cut}, \text{Rev-Weaken}, \mathbb{F}_q\text{-Elim}, \mathbb{F}_q\text{-Intro}\},$$

where the Rev-Cut and Rev-Weaken are taken from the definition of RevRes in Section 2.2. Then

$$\mathcal{R}_q^- = \mathcal{R}_q \setminus \{\mathbb{F}_q\text{-Intro}\} \text{ and } \mathcal{R}_2^{\text{Copy}} = \mathcal{R}_2 \cup \{\mathbb{F}_2\text{-Copy}\} \setminus \{\mathbb{F}_q\text{-Intro}\}.$$

Now, the proof systems can be defined in the following way:

- $\mathrm{RevResT}_{R_q}$ is the blackboard system with terminals based on $\mathcal{R}_q$, where the final blackboard state *contains exactly* c copies of $\bot$ for some $1 \leq c < q$ (there might be some other clauses, which are weakenings of clauses from φ).
- $\mathrm{RevResT}_{\mathcal{R}_q^-}$ is the blackboard system with terminals based on $\mathcal{R}_q^-$, where the final blackboard state *contains exactly* c copies of $\bot$ for some $1 \leq c < q$.
- $\mathrm{RevResT}_{\mathcal{R}_2^{\mathrm{Copy}}}$ is the blackboard system with terminals based on $\mathcal{R}_2^{\mathrm{Copy}}$, where the final blackboard state *contains only one copy of* $\bot$.

▶ Remark 31. These definitions slightly differ from the ones presented in [17]. However, these variants are p-equivalent to the ones from [17].

Proof sketches of the second and third intersection theorems

To prove the second intersection theorem, one can do the following: copy $q \cdot S$ times the RevRes-proof, eliminate everything, except for the copies of $\bot$, then use the weakening rule on the copies of $\bot$ together with $\mathbb{F}_q$-Elim to simulate $\mathbb{F}_q$-Intro.

The proof of the third intersection theorem is more involved. First, given a Resolution refutation, we simulate it directly by replacing all the applications of the usual Copy rule with the $\mathbb{F}_2$-Copy rule. In the end, this will produce us 1 copy of $\bot$ and some other "garbage" clauses $\mathcal{G}$. Then we isolate ourselves on this one copy of $\bot$, and will emulate the $\mathrm{RevResT}_{R_2}$ refutation directly: every time we would like to do the $\mathbb{F}_2$-Intro of two copies of clause C, we do the following instead:

$$\dfrac{\dfrac{\bot}{\bot \quad \bot \quad \bot}\ \mathbb{F}_2\text{-Copy}}{\bot \quad C \quad C}\ \text{Rev-Weaken} + \mathbb{F}_2\text{-Elim}$$

In the end, we get a separate derivation of exactly one copy of $\bot$. Then, we revert back the derivation of $\mathcal{G} \cup \{\bot\}$ to the initial clauses, since all the rules in $\mathrm{RevResT}_{\mathcal{R}_2^{\mathrm{Copy}}}$. This will effectively provide us a $\mathrm{RevResT}_{\mathcal{R}_2^{\mathrm{Copy}}}$ derivation with exactly one copy of $\bot$ at the end and some weakenings of the clauses from φ.

References

1. Michael Alekhnovich, Eli Ben-Sasson, Alexander A., and Avi Wigderson. Space complexity in propositional calculus. In *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing*, STOC '00, pages 358–367, New York, NY, USA, 2000. Association for Computing Machinery. doi:10.1145/335305.335347.
2. Yaroslav Alekseev and Dmitry Itsykson. Lifting to bounded-depth and regular resolutions over parities via games. In *Proceedings of the 57th Annual ACM Symposium on Theory of Computing*, STOC '25, pages 584–595, New York, NY, USA, 2025. Association for Computing Machinery. doi:10.1145/3717823.3718150.
3. Eli Ben-Sasson and Nicola Galesi. Space complexity of random formulae in resolution. In *Proceedings of the 16th Annual Conference on Computational Complexity*, CCC '01, page 42, USA, 2001. IEEE Computer Society.
4. Eli Ben-Sasson and Avi Wigderson. Short proofs are narrow—resolution made simple. *J. ACM*, 48(2):149–169, 2001. doi:10.1145/375827.375835.
5. Sreejata Kishor Bhattacharya and Arkadev Chattopadhyay. Exponential lower bounds on the size of ResLin proofs of nearly quadratic depth, 2025. doi:10.48550/arXiv.2507.23008.
6. Sreejata Kishor Bhattacharya, Arkadev Chattopadhyay, and Pavel Dvorák. Exponential separation between powers of regular and general resolution over parities. In Rahul Santhanam, editor, *39th Computational Complexity Conference, CCC 2024, July 22-25, 2024, Ann Arbor, MI, USA*, volume 300 of *LIPIcs*, pages 23:1–23:32. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2024. doi:10.4230/LIPIcs.CCC.2024.23.

7 Ilario Bonacina, Maria Luisa Bonet, and Jordi Levy. Weighted, circular and semi-algebraic proofs. *J. Artif. Int. Res.*, 79, 2024. doi:10.1613/jair.1.15075.

8 Maria Luisa Bonet and Jordi Levy. Equivalence between systems stronger than resolution. In Luca Pulina and Martina Seidl, editors, *Theory and Applications of Satisfiability Testing – SAT 2020*, pages 166–181, Cham, 2020. Springer International Publishing. doi:10.1007/978-3-030-51825-7_13.

9 Stephen A. Cook and Robert A. Reckhow. The relative efficiency of propositional proof systems. *Journal of Symbolic Logic*, 44(1):36–50, 1979. doi:10.2307/2273702.

10 Ben Davis and Robert Robere. Colourful TFNP and Propositional Proofs. In Amnon Ta-Shma, editor, *38th Computational Complexity Conference (CCC 2023)*, volume 264 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 36:1–36:21, Dagstuhl, Germany, 2023. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.CCC.2023.36.

11 Klim Efremenko and Dmitry Itsykson. Amortized closure and its applications in lifting for resolution over parities. *Electron. Colloquium Comput. Complex.*, TR25-039, 2025. URL: https://eccc.weizmann.ac.il/report/2025/039.

12 Juan Luis Esteban and Jacobo Torán. Space bounds for resolution. *Information and Computation*, 171(1):84–97, 2001. doi:10.1006/inco.2001.2921.

13 John Fearnley, Paul Goldberg, Alexandros Hollender, and Rahul Savani. The complexity of gradient descent: $\mathsf{CLS} = \mathsf{PPAD} \cap \mathsf{PLS}$. *J. ACM*, 70(1), 2022. doi:10.1145/3568163.

14 Mika Göös, Alexandros Hollender, Siddhartha Jain, Gilbert Maystre, William Pires, Robert Robere, and Ran Tao. Separations in proof complexity and TFNP. *J. ACM*, 71(4), 2024. doi:10.1145/3663758.

15 Armin Haken. The intractability of resolution. *Theoretical Computer Science*, 39:297–308, 1985. Third Conference on Foundations of Software Technology and Theoretical Computer Science. doi:10.1016/0304-3975(85)90144-6.

16 Pavel Hubáček, Erfan Khaniki, and Neil Thapen. TFNP intersections through the lens of feasible disjunction. In Venkatesan Guruswami, editor, *15th Innovations in Theoretical Computer Science Conference (ITCS 2024)*, volume 287 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 63:1–63:24, Dagstuhl, Germany, 2024. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.ITCS.2024.63.

17 Yuhao Li, William Pires, and Robert Robere. Intersection Classes in TFNP and Proof Complexity. In Venkatesan Guruswami, editor, *15th Innovations in Theoretical Computer Science Conference (ITCS 2024)*, volume 287 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 74:1–74:22, Dagstuhl, Germany, 2024. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.ITCS.2024.74.

18 Alexander A. Razborov. Lower bounds for the polynomial calculus. *Computational Complexity*, 7(4):291–324, 1998. doi:10.1007/s000370050013.

A u-wRes and catalytic RevRes are equivalent

To prove our intersection theorems, we consider a more convenient reformulation of the unary Sherali-Adams proof system, which is called *Unary Weighted Resolution*. Informally, this proof system can be viewed as a generalization of Reversible Resolution, where all the clauses are marked with "+" and "−" signs. Unary Weighted Resolution uses the same derivation rules as Reversible Resolution (with respect to the sign of the clause); however, it also uses introduction and elimination rules for pairs of clauses with opposite signs. We define a general notion of weighted systems and show that this notion is equivalent to their catalytic counterparts.

▶ **Definition 32** (Unary Weighted Systems [8]). *Let $\mathcal{R}$ be a collection of strongly sound reversible rules. Let* RevP *be a blackboard proof system based on $\mathcal{R}$. Lines in the proof system* u-wP *are multisets of clauses of* RevP *with* signs*, i.e., they can be* positive *or* negative.

For any CNF formula $\varphi = C_1 \wedge C_2 \wedge \cdots \wedge C_m$ a sequence of multisets of clauses with signs $\mathcal{L}_1, \ldots, \mathcal{L}_t$ is the u-wP *refutation of φ if:*

- *Every clause in $\mathcal{L}_1$ occurs in φ, possibly with multiplicity.*
- *The multiset $\mathcal{L}_t$ contains the empty clause $(\bot, +)$.*
- *All clauses in $\mathcal{L}_t$ are positive (that is, have "+" sign).*
- *For each $i = 1, 2, \ldots, t-1$, the multiset $\mathcal{L}_{i+1}$ is obtained from $\mathcal{L}_i$ with one of the following derivation rules:*
  - *For any rule $(\mathcal{F}, \mathcal{G})$ from $\mathcal{R}$, one can derive $(\mathcal{G}, +)$ from $(\mathcal{F}, +)$ and $(\mathcal{G}, -)$ from $(\mathcal{F}, -)$, where by $(\mathcal{F}, +)$ we denote the multiset of clauses $\{(C_i, +) \mid C_i \in \mathcal{F}\}$.*
  - *We can introduce new clauses with the following rules:*

$$\frac{}{(C,-) \quad (C,+)} \text{ (Sign introduction)} \qquad \frac{(C,-) \quad (C,+)}{} \text{ (Sign elimination)}$$

We define u-wRes as a unary weighted version of RevRes. Following [7], we know that u-wRes is p-equivalent to Unary Sherali-Adams.

▶ **Definition 33** (Unary Sherali-Adams). *Unary Sherali–Adams refutes unsatisfiable sets of polynomial equations $\{a_i(x) = 0 \colon i \in [m]\}$ with integer coefficients $a_i \in \mathbb{Z}[x]$,* written in unary notation. *A CNF contradiction F can be translated into this language by encoding each clause, say, $C \coloneqq (x_1 \vee \neg x_2 \vee x_3)$, as the equation $\overline{x}_1 x_2 \overline{x}_3 = 0$, and by enforcing each variable x_i to take boolean values with the equation $x_i^2 - x_i = 0$. A* uSA *refutation of $\{a_i(x) = 0\}$ is a polynomial identity of the form*

$$\sum_{i \in [m]} p_i(x) \cdot a_i(x) + \sum_{j \in [n]} q_j(x) \cdot (x_j^2 - x_j) + \sum_{j \in [n]} r_j(x)(x_j + \overline{x}_j - 1) + J(x) = c,$$

where $c \in \mathbb{N}$ is a positive constant, $p_i, q_j, r_j \in \mathbb{Z}[x]$ are polynomials, and J is a conical junta: a nonnegative linear combination of terms, that is, $J(x) = \sum_j t_j(x)$, where each t_j is a conjunction of literals; for example, $t_j(x) = x_1 \overline{x}_2 x_3$. The size of the uSA *refutation is the sum of the magnitudes of all coefficients of the monomials appearing in p_i, a_i, q_j, r_j and t_j.*

CatP and u-wP are p-equivalent

To simplify the proofs and give an additional intuition about the nature of u-wP, we prove the following fact:

▶ **Lemma 34.** *The following are equivalent for any unsatisfiable CNF $\varphi = C_1 \wedge C_2 \wedge \cdots \wedge C_n$ and fixed S and w:*

1. *There exists a refutation of size S and width w for φ in* u-wP.
2. *There exists a sequence of (not necessarily distinct) clauses $D_1, \ldots, D_k$, such that there is a* RevP *derivation of size $\Theta(S)$ and width w, which starts with $D_1, D_2, \ldots, D_k, C_{\alpha_1}, C_{\alpha_2}, \ldots, C_{\alpha_t}$ and ends in a state $\mathcal{L}$ such that*

$$D_1, D_2, \ldots, D_k, \bot \subseteq \mathcal{L}.$$

This lemma in fact shows that u-wP and CatP are p-equivalent.

Proof of Lemma 34. First, we show that $2 \Rightarrow 1$. To construct a u-wP derivation of size $\Theta(S)$, we first introduce the clauses D_i with the minus sign:

$$\frac{}{(D_1,-) \quad (D_1,+)} \quad \frac{}{(D_2,-) \quad (D_2,+)} \quad \cdots \quad \frac{}{(D_k,-) \quad (D_k,+)}$$

Now, using the clauses $(D_i, +)$ with positive signs and the clauses C_{α_j}, we repeat the RevP-derivation to obtain the sequence of states

$$\mathcal{L}'_j = \mathcal{L}_j \cup \bigcup_{i=1}^{k} (D_i, -),$$

where $\mathcal{L}_j$ are the states of RevP refutation, interpreted as clauses with positive signs and

$$(D_1, +), (D_2, +), \ldots, (D_k, +), (\bot, +) \in \mathcal{L}_t.$$

Thus, we can contract $(D_i, -)$ and $(D_i, +)$ in $\mathcal{L}'$ for each $i \in [k]$. This operation will generate a state $\mathcal{L}''$ such that $(\bot, +) \in \mathcal{L}''$ and the rest of the clauses from $\mathcal{L}''$ have are positive.

Next, we show $1 \Rightarrow 2$. First, observe that we can transform u-wP refutation to one of size $\Theta(S)$, in which the following holds:

(i) We introduce all negative clauses at the very beginning of the refutation.

(ii) We apply cut and weakening rules only to positive clauses.

Indeed, to get the second property, we consider the application of any rule $(\mathcal{F}, \mathcal{G}) \in \mathcal{R}$ for negative clauses, and show that we can replace it with an application of the reversed rule for positive clauses in the following way:

$$\dfrac{(\mathcal{F}, -) \quad \dfrac{\dfrac{}{(\mathcal{G}, +)} \quad (\mathcal{G}, -)}{(\mathcal{F}, +)} \quad (\mathcal{G}, -)}{(\mathcal{G}, -)} \quad \begin{array}{l} \text{(Sign introduction)} \\ (\mathcal{G}, \mathcal{F})\text{-rule} \\ \text{(Sign elimination)} \end{array}$$

This operation allows us to get rid of one application of this rule to the cut rule for the minus clauses.

After getting rid of all applications of derivation rules for minus clauses, we only apply introduction/elimination rules for minus clauses. Thus, we can apply all the introduction rules in the beginning, and postpone all the applications of elimination rules to the very end.

By considering all negative clauses as *catalyst* $D_1, \ldots, D_k$, and all positive clauses as regular clauses, we get a RevRes derivation of size $\Theta(S)$, which starts with $D_1, D_2, \ldots, D_k, (C_1, \alpha_1), \ldots, (C_k, \alpha_k)$ and ends with a state $\mathcal{L}$ such that

$$D_1, D_2, \ldots, D_k, \bot \subseteq \mathcal{L}.$$ ◀

B Algebraic intersection theorem

We start with the definitions of proof systems from [17].

▶ **Definition 35** (Nullstellensatz over $\mathbb{F}_q$)**.** *Let $q \geq 2$ be a positive integer (not necessarily prime) and consider the ring $\mathbb{Z}_q$. Given a CNF $\varphi = C_1 \wedge \ldots \wedge C_m$ over variables $x_1, \ldots, x_n$, a generalized Nullstellensatz refutation of φ over $\mathbb{Z}_q$ is given by a list of polynomials $p_i, q_j, r_j \in \mathbb{Z}_q[x_1, \ldots, x_n]$ such that:*

$$\sum_{j \in [m]} p_j(x)\overline{C}_j(x) + \sum_{j \in [n]} q_j(x) \cdot (x_j^2 - x_j) + \sum_{j \in [n]} r_j(x)(x_j + \overline{x}_j - 1) \equiv c \pmod{q},$$

where $\overline{C}_j$ is the natural translation of clauses from φ, c is a constant from $\mathbb{Z}_q$, which is not equal to 0. We denote this proof system as NS_q^*. The size of a NS_q^* refutation is the total number of monomials in p_i, q_j, r_j.

▶ **Definition 36** ($\mathbb{F}_q$-Sherali-Adams). *Let $\varphi = C_1 \wedge \ldots \wedge C_m$ be a CNF over variables $x_1, \ldots, x_n$. A q-Sherali-Adams (SA_q) refutation of φ is a unary Sherali-Adams refutation, with the further constraints that $1 \leq c \leq q-1$ and the conical junta J can be written as $q \cdot J'$.*

We want to prove the following intersection theorem:

▶ **Theorem 37.** $\mathrm{NS}_q \curlywedge \mathrm{uSA}$ *is p-equivalent to* SA_q.

Proof. To show that $\mathrm{NS}_q \curlywedge \mathrm{uSA}$ is p-equivalent to SA_q, we observe the following. Let

$$\sum p_j h_j \equiv c_0 \pmod{q}$$

be a NS_q refutation of $\{h_j = 0\}$ where $1 \leq c_0 \leq q-1$ and

$$\sum f_j h_j = c + J(x)$$

be a uSA refutation of the same system. Then the NS_q refutation can be naturally transformed into the following equation of $\mathrm{poly}(S)$ size in the unary encoding of the following form:

$$\sum p'_j h_j = c_0 + q \cdot R(x),$$

where $p_j, R \in \mathbb{Z}[x]$. Now, for each monomial t in the RHS with a negative sign, we add to both sides of the equation the following polynomial:

$$q \cdot t \cdot \sum f_j h_j = q \cdot t \cdot (c + J(x)).$$

This operation will give us an equation of size $\mathrm{poly}(S)$ of the form

$$\sum p''_j h_j = c_0 + q \cdot R'(x),$$

where all the monomials in $R'(x)$ have a positive sign. This is a SA_q refutation since $1 \leq c_0 \leq q-1$. ◀