Electronic Colloquium on Computational Complexity, Report No. 39 (2025)

Amortized Closure and Its Applications in Lifting for Resolution over Parities

Klim Efremenko*[1] and Dmitry Itsykson†[1,2]

[1]Ben-Gurion University of the Negev, Israel
[2]On leave from Steklov Institute of Mathematics at St. Petersburg

March 31, 2025

Abstract

The notion of closure of a set of linear forms, first introduced by Efremenko, Garlik, and Itsykson [14], has proven instrumental in proving lower bounds on the sizes of regular and bounded-depth Res($\oplus$) refutations [14, 3]. In this work, we present amortized closure, an enhancement that retains the properties of original closure [14] but offers tighter control on its growth. Specifically, adding a new linear form increases the amortized closure by at most one. We explore two applications that highlight the power of this new concept.

Utilizing our newly defined amortized closure, we extend and provide a succinct and elegant proof of the recent lifting theorem by Chattopadhyay and Dvorak [10]. Namely we show that for an unsatisfiable CNF formula φ and a 1-stifling gadget $g\colon \{0,1\}^\ell \to \{0,1\}$, if the lifted formula $\varphi \circ g$ has a tree-like Res($\oplus$) refutation of size 2^d and width w, then φ has a resolution refutation of depth d and width w. The original theorem by Chattopadhyay and Dvorak [10] applies only to the more restrictive class of strongly stifling gadgets.

We further utilize amortized closure to show improved lower bounds for bounded-depth Res($\oplus$), extending the depth beyond that of Alekseev and Itsykson [3]. Our result establishes an exponential lower bound for depth-$\Omega(n \log n)$ Res($\oplus$) refutations of lifted Tseitin formulas, a notable improvement over the existing depth-$\Omega(n \log\log n)$ Res($\oplus$) lower bound.

1 Introduction

Propositional proof complexity investigates proof systems for the language of unsatisfiable CNF formulas, denoted as UNSAT. The fundamental question of whether the complexity classes NP and coNP are distinct is equivalent to asking whether there exists a proof system that can provide polynomial-size proofs for all formulas in UNSAT [12]. A central focus in proof complexity is establishing superpolynomial lower bounds on proof sizes for specific proof systems; a direction often referred to as Cook's program, which aims to separate NP and coNP.

While many exponential-size lower bounds are known for weak proof systems, we lack superpolynomial lower bounds for Frege systems, which include standard propositional proof systems from logic textbooks. A Frege derivation is a sequence of Boolean formulas; each of them is either an axiom or is obtained from the previous by a set of sound and implicationally complete inference rules. Proving Frege lower bounds is often compared to proving Boolean formula/circuit lower bounds for explicit Boolean functions, and both seem intractable. However, progress has been made in restricted settings. An exponential lower bound for

*e-mail: klimefrem@gmail.com. Supported by European Research Council Grant No. 949707.
†e-mail: dmitrits@gmail.com. Supported by European Research Council Grant No. 949707.

ISSN 1433-8092

constant-depth circuits computing parity was proven in the 1980s [16, 1]. Ajtai later used a similar approach to prove a superpolynomial lower bound for bounded-depth Frege systems [2]. Razborov and Smolenski proved lower bounds for constant-depth circuits with $\neg$, $\vee$, $\wedge$, and MOD_p gates in 1987 [23, 21]. The analogous problem of proving a lower bound for constant-depth Frege systems using $\neg$, $\vee$, $\wedge$ and MOD_p gates (denoted $\mathrm{AC}^0[p]$-Frege) is open for all $p > 1$.

This paper is devoted to the study of the propositional proof system resolution over parities (Res($\oplus$)) [19], which is a subsystem of $\mathrm{AC}^0[2]$-Frege. This system extends resolution by incorporating linear algebra over $\mathbb{F}_2$. The proof lines in this proof system are linear clauses, disjunctions of $\mathbb{F}_2$-linear equations; or, equivalently, linear clauses can be treated as negations of $\mathbb{F}_2$-linear systems. A refutation of an unsatisfiable CNF formula φ is a sequence of linear clauses such that the last linear clause in this sequence is an empty clause (i.e., constant false), and every other linear clause is obtained from the previous clauses by the resolution rule or by the weakening rule. The resolution rule allows resolve by a linear form, i.e. allows to derive $(A \vee B)$ from $A \vee f = 0$ and $B \vee f = 1$. The weakening rule allows the deriving of any linear clause that semantically follows from the given. Establishing superpolynomial lower bounds on the size of Res($\oplus$) refutations remains a significant open challenge, representing a crucial step toward proving lower bounds for the more general proof system $\mathrm{AC}^0[2]$-Frege.

1.1 Lifting

Lifting is a highly effective technique for establishing lower bounds by transferring them from weaker to stronger computational models. Recent developments in lifting for fragments of Res($\oplus$) offer promising avenues toward proving a superpolynomial lower bound for general Res($\oplus$). The most relevant lifting results pertaining to Res($\oplus$) are briefly described below.

Chattopadhyay, Mande, Sanyal, and Sherif [11] developed a universal lifting technique for parity decision trees via 1-stifling gadgets, which are characterized by the following property: a gadget $g\colon \{0,1\}^\ell \to \{0,1\}$ is 1-stifling if, for any index $i \in [\ell]$ and any target bit b, there exists an assignment y such that any x agreeing with y on all but ith position yields $g(x) = b$. Their result demonstrates that if a function (or relation) f requires query complexity d, then for any 1-stifling gadget g, the lifted function (or relation) $f \circ g$ requires parity decision trees of size at least 2^d. In the proof complexity settings, this result implies that if a formula φ requires resolution depth d, then for any 1-stifling gadget g, the lifted formula $\varphi \circ g$ requires tree-like Res($\oplus$) size at least 2^d [11]. Independently, Beame and Koroth [5] obtained similar results. Recently, Podolskii and Shekhovostov [20] and Byramji and Impagliazzo [9] extended the results of [11] to randomized parity decision trees.

Lifting techniques are also instrumental in establishing lower bounds for regular Res($\oplus$), a natural fragment of the Res($\oplus$) proof system that is strictly more powerful than its tree-like counterpart. Regular Res($\oplus$) is defined in a manner analogous to regular resolution, inheriting its key restrictions. Bhattacharya, Chattopadhyay, and Dvorak [7] used lifting to prove that regular Res($\oplus$) does not simulate resolution. Subsequently, Alekseev and Itsykson [3] introduced a more general lifting technique. This method transforms formulas with large resolution depth into formulas requiring exponential-size regular Res($\oplus$) refutations.

The depth of any regular Res($\oplus$) refutation is limited to n, the number of variables, and it's known that depth-n Res($\oplus$) is more powerful than regular Res($\oplus$). Alekseev and Itsykson [3] employed their lifting technique to demonstrate an exponential lower bound on the size of Res($\oplus$) refutations restricted to a depth of $cn \log\log n$, where c is a constant and n is the number of variables.

The lifting techniques of Bhattacharya, Chattopadhyay, and Dvorak [7] and Alekseev and Itsykson [3] rely heavily on the concept of closure of a set of linear forms in lifted variables, initially defined by Efremenko, Garlik, and Itsykson [14]. The closure captures the most essential unlifted variables for these linear forms. Based on this, Alekseev and Itsykson [3] developed a game-based lifting technique, which they demonstrated by the following simple and elegant example:

Theorem 1.1 ([3])**.** If a CNF formula φ requires resolution width w, then for every 1-stifling gadget g, the formula $\varphi \circ g$ requires Res($\oplus$) width w.

The proof of Theorem 1.1 proceeds by an explicit transformation of strategies, converting winning strategies from Atserias and Dalmau's [4] resolution-width games into winning strategies for games characterizing the Res($\oplus$) width [18].

Chattopadhyay and Dvorak [10] recently established the following lifting theorem.

Theorem 1.2 ([10])**.** If every resolution refutation of a CNF formula φ of width at most w requires depth at least d, then for every *strongly stifling* gadget g, any tree-like Res($\oplus$) refutation of the formula $\varphi \circ g$ of width at most w has size at least 2^d.

Chattopadhyay and Dvorak [10] uncovered a striking application of this theorem: a supercritical tradeoff for tree-like Res($\oplus$) refutations. This shows that a slight narrowing of width can force a double exponential blow-up in refutation size. Specifically, for a sufficiently small width, the tree-like Res($\oplus$) refutation size can exceed its worst-case upper bound observed in the unrestricted case. This tradeoff is obtained by a straightforward application of Theorem 1.2 alongside Razborov's corresponding tree-like resolution result [22].

Strongly stifling gadgets constitute a more restricted class compared to 1-stifling gadgets, meaning that Theorem 1.2 extends Theorem 1.1 and the results of [11] but only for this smaller class of gadgets. Establishing Theorem 1.2 requires a technically demanding proof, primarily due to the explicit transformation that directly converts a tree-like Res($\oplus$) refutation of the lifted formula into a tree-like resolution refutation of the base formula. The proof of Theorem 1.2 largely mirrors the approach outlined in [11]. However, in the case of bounded width, Chattopadhyay and Dvorak diverge by utilizing forgetting parity decision trees instead of standard parity decision trees. These forgetting trees incorporate forgetting nodes that correspond to weakening rules. The most challenging aspect involves handling these forgetting nodes, for which the authors restrict themselves to strongly stifling gadgets to facilitate the analysis.

1.2 Our contributions

In this work, we contribute to the lifting technique. Namely, we develop the notion of amortized closure of a set of linear forms. This new concept retains all the desirable properties of plain closure but additionally guarantees that the amortized closure increases by at most one when a single linear form is added to the set. The construction of this amortized closure and the proof of its properties (Theorem 1.7) constitute the main technical contribution of our work. We give two nice applications to demonstrate this new concept's power. We believe amortized closure is of independent interest and will find further applications in lifting theorems in proof complexity and Boolean complexity.

As a first application, we prove the following theorem, which extends Theorem 1.2 to the entire class of 1-stifling gadgets, thereby also generalizing Theorem 1.1 and the mentioned result from [11].

Theorem 1.3 (Theorem 4.3)**.** Let φ be an unsatisfiable CNF formula and $g\colon \{0,1\}^\ell \to \{0,1\}$ be a 1-stiffling gadget. Assume that $\varphi \circ g$ has a tree-like Res($\oplus$) refutation of width w and size 2^d. Then φ has a resolution refutation of width w and depth d.

We present a concise and elegant proof of Theorem 1.3, adapting Alekseev and Itsykson's game approach [3] from Theorem 1.1 to amortized closure.

As a second application, we improve depth in the lower bound for bounded-depth Res($\oplus$) refutations established by Alekseev and Itsykson [3]. Specifically, the following theorem implies an exponential lower bound for depth-$cn \log n$ Res($\oplus$) refutations of lifted Tseitin formulas, where n is the number of variables and c is a constant.

Theorem 1.4 (Informal restatement of Corollary 5.6)**.** Let ϕ_n be an unsatisfiable Tseitin formula based on a $\Theta(\log n)$-regular expander with n vertices lifted by the 5-input majority gadget. Then, ϕ_n is a CNF formula with $m = \Theta(n \log n)$ variables and size $\mathrm{poly}(m)$ such that any Res($\oplus$) refutation of ϕ_n has either size at least $2^{\Omega(m/\log m)}$ or depth at least $\Omega(m \log m)$.

The presentation of our results in the introduction starts with the first application. Namely, we begin by detailing the game-based approach of Alekseev and Itsykson [3], and then we explain why its direct application fails to establish Theorem 1.3, emphasizing the necessity of our amortized closure. Then, we present our main contribution, the amortized closure construction, and detail its essential properties. We conclude with the second application: we demonstrate how amortized closure helps to obtain an exponential lower bound for bounded-depth Res($\oplus$) refutations for larger depths.

1.2.1 Bounded-width lifting

Here we present the proof idea of Theorem 1.3. We are going to apply the game approach that was used by Alekseev and Itsykson in the proof of Theorem 1.1. We start with definitions of some basic notions: lifting and closure.

Let $\varphi(y_1, y_2, \ldots, y_m)$ be an unsatisfiable CNF. We call the set of variables $Y = \{y_1, y_2, \ldots, y_m\}$ unlifted. Let $g\colon \{0,1\}^\ell \to \{0,1\}$ be an 1-stifling gadget. The lifted formula $\varphi \circ g$ depends of variables $X = \{x_{i,j} \mid i \in [m], j \in [\ell]\}$, called lifted variables. The formula $\varphi \circ g$ represents in CNF the result of the substitution $\varphi(g(x_{1,1}, \ldots, x_{1,\ell}), \ldots, g(x_{m,1}, \ldots, x_{m,\ell}))$.

Safe sets and closure. Consider the set of $\mathbb{F}_2$-linear forms $F = \{f_1, f_2, \ldots, f_k\}$ in lifted variables and consider their coefficient matrix M_F. The columns of M_F can be splitted on m blocks, where the ith block corresponds to variables $x_{i,1}, x_{i,2}, \ldots, x_{i,\ell}$ with first index i. The set of linear forms F is *safe* [14] if, among the columns of M_F, one can find a basis that includes at most one column for each block. A crucial observation is that if a set of linear forms F is safe, then any satisfiable linear system formed using the linear forms in F for any assignment σ of the unlifted variables admits a solution that respects the assignment σ on the unlifted variables [7, 3]. Indeed, values of variables whose columns are not in the basis can be chosen arbitrarily. Since the gadget is 1-stifling, we can fix its value regardless of the value of the remaining basis variables.

However, F is not necessary to be safe. *A closure* of F is an inclusion-minimal set of blocks such that if we set zeros to all variables from these blocks, the set F becomes safe. For the coefficient matrix, this operation corresponds to the removal of columns corresponding to these blocks. We will identify the closure with the corresponding set of unlifted variables. Bhattacharya, Chattopadhyay, and Dvorak noted that *the closure contains all essential unlifted variables* in the following sense: given a solution α of a linear system Φ in lifted variables, for any unlifted variable y that lies outside a closure of the set of linear forms in Φ, there exists another solution β of Φ such that the assignments induced by α and β on the unlifted variables differ precisely in the value assigned to y.

The following properties of closure were proved by Efremeko, Garlik, and Itsykson [14].

- (Uniqueness) Closure of the set of linear forms F is unique, and it is denoted by $\mathrm{Cl}(F)$;
- (Monotonicity) If $F \subseteq F'$, then $\mathrm{Cl}(F) \subseteq \mathrm{Cl}(F')$;
- (Span invariance) If $\langle F_1 \rangle = \langle F_2 \rangle$, then $\mathrm{Cl}(F_1) = \mathrm{Cl}(F_2)$;
- (Size bound) $|\mathrm{Cl}(F)| \leq \dim\langle F \rangle = \mathrm{rk}\,(M_F)$.

Using the notion of closure, Alekseev and Itsykson [3] define *the correspondence* between linear systems over lifted variables and partial assignments for unlifted variables as follows:

- A system of linear equations Ψ over lifted variables *corresponds* a partial assignment ρ to unlifted variables if ρ is defined on $\mathrm{Cl}(L(\Psi))$ and Ψ has a solution τ such that τ induces on the unlifted variables an assignment that is consistent with ρ, where $L(\Psi)$ denotes the system of linear forms that occur in Ψ. We also say that τ defines the correspondence between Ψ and ρ.

An important property of this correspondence is that if Ψ corresponds ρ and ρ does not falsify any clause of φ, then Ψ does not contradict any clause of $\varphi \circ g$.

This correspondence is in the heart of the proof of Theorem 1.1 since it allows the transformation of a strategy in the game characterizing resolution width of φ to a strategy in the game characterizing Res($\oplus$) width of $\varphi \circ g$.

Let us try to apply this approach directly to the following proposition.

Proposition 1.5. If any resolution refutation of φ of withd w has depth at least d, then for any 1-stifling gadget $g\colon \{0,1\}^\ell \to \{0,1\}$, any Res($\oplus$) refutation of the formula $\varphi \circ g$ of width w has depth at least d.

Proposition 1.5 is weaker than Theorem 1.3 since it says about depth instead of tree-like size. However, in this example, we highlight the problem, explain why the approach described above can not be applied directly, and identify the missing property of closure.

We proceed with the definition of games characterizing depth in bounded-width resolution and bounded-width Res($\oplus$).

A (φ, w)-game for resolution. Consider the following game based on an unsatisfiable CNF formula φ and a natural parameter w. The game has two players: Prover and Adversary. Players save a partial assignment ρ that is initially empty. For every move, Prover can either remove some value from ρ or, if $|\rho| < w$, Prover can choose a variable x and ask Adversary for its value. Adversary chooses $a \in \{0,1\}$ and extends the current assignment ρ by $x := a$. For every move, Adversary earns a coin. The game ends when ρ falsifies a clause of φ. It is known that Adversary has a strategy in the $(\varphi, w+1)$-game that guarantees him to earn at least d coins if and only if any resolution refutation of φ within width w has depth at least d [6].

A (φ, w)-game for Res($\oplus$). Consider an extension of the previous game. This game is also based on a CNF formula φ and a natural parameter w. Now, the players, Prover and Adversary, save a linear system Ψ in variables of φ that is initially empty (i.e. constant true). On every move, Prover can either replace Ψ on its semantical implication or, if the rank of Ψ is less than w, Prover can choose a linear form f and ask Adversary for its value. Adversary chooses $a \in \{0,1\}$ and adds the equation $f = a$ to Ψ. Adversary earns a coin for every move. The game ends when Ψ contradicts a clause of φ. Similarly, one can show Adversary has a strategy in the $(\varphi, w+1)$ game that guarantees him to earn at least d coins if and only if any Res($\oplus$) refutation of φ within width w has depth at least d.

Let us try to prove Proposition 1.5 using these games. Since any resolution refutation of φ of width at most w requires depth at least d, there is an Adversary's strategy in the first $(\varphi, w+1)$-game that guarantees him to earn at least d coins. Using this strategy, we try to construct an Adversary's strategy in the second $(\varphi \circ g, w+1)$-game that will also guarantee the Adversary to earn at least d coins. It will imply that any Res($\oplus$) refutation of $\varphi \circ g$ within width w requires depth at least d.

We will describe an Adversary's strategy in the second $(\varphi \circ g, w+1)$-game using the known Adversary's strategy in the first $(\varphi, w+1)$-game. Describing Adversary's strategy in the second game, we play in parallel in the first game, making moves instead of Prover and using the Adversary's strategy in the first game. We maintain the following invariant: the current system Ψ in the second game corresponds to the current partial assignment ρ in the first game. While this invariant holds, if ρ does not falsify any clause of φ, then Ψ does not contradict any clause of $\varphi \circ g$.

If Prover in the second game changes Ψ to its semantical corollary Ψ', then playing for the Prover in the first game, we restrict ρ to $\mathrm{Cl}(L(\Psi'))$ in the first game. Notice that since Ψ' semantically follows from Ψ, $L(\Psi') \in \langle L(\Psi)\rangle$, hence $\mathrm{Cl}(L(\Psi')) \subseteq \mathrm{Cl}(L(\Psi))$.

If Prover in the second game asks the value of a linear form f, we consider two cases.

- First case: $\mathrm{Cl}(L(\Psi) \cup \{f\}) = \mathrm{Cl}(L(\Psi))$. Let σ be the solution of Ψ that defines the correspondence between Ψ and ρ. Adversary chooses the value $a = f|_\sigma$ and does nothing in the first game. It is easy to see that σ also defines the correspondence between $\Psi \wedge (f = a)$ and ρ; hence, the invariant still holds.

- Second case: $\mathrm{Cl}(L(\Psi) \cup \{f\}) \neq \mathrm{Cl}(L(\Psi))$. In this case, we, playing by Prover in the first game, prolong ρ to variables from $\mathrm{Cl}(L(\Psi) \cup \{f\}) \neq \mathrm{Cl}(L(\Psi))$ (recall that we identify elements of closure with unlifted variables) by asking them one by one. Since we extend ρ to variables out of $\mathrm{Cl}(L(\Psi))$, for the new

value of ρ, there is a solution τ of Ψ such that τ induces an assignment on unlifted variables consistent with ρ. Adversary chooses the value $a = f|_\tau$. Now τ defines the correspondence between $\Psi \wedge (f = a)$ and ρ; hence, the invariant still holds.

Unfortunately, this strategy does not allow us to estimate the number of coins that the Adversary earns in the second game. The problem is that the closure can increase significantly in one step. At this moment, we have spent many coins in the first game while earning only one coin in the second one. Theoretically, it is possible, for example, that on each odd step, Prover in the second game decreases $|\operatorname{Cl}(L(\Psi))|$ on k and on each even step increases $|\operatorname{Cl}(L(\Psi))|$ by k. Then, the Adversary in the second game will earn 1 coin for each pair of two consequent steps while spending k coins in the first game.

To solve this issue, we define *the amortized closure* $\widetilde{\operatorname{Cl}}(F)$ that has all properties of $\operatorname{Cl}(F)$ and also can be increased by at most one by adding a linear form. Using amortized closure in the strategy above instead of plain closure, we can guarantee that every time we spend a coin in the first game, we earn a coin in the second game. Hence, the strategy will guarantee to earn at least d coins, and we will prove Proposition 1.5.

The proof of Theorem 1.3 is very similar to the presented proof idea of Proposition 1.5. To characterize the size of tree-like Res($\oplus$) refutations, we use width-bounded Prover-Delayer games instead of Prover-Adversary games for Res($\oplus$).

1.2.2 Amortized closure

Before defining amortized closure, consider an example where the closure increases more than by one by adding just one linear form.

Example 1.6. Let $m = 3$ and $\ell = 2$. Consider linear forms: $f_1 = x_{3,2}, f_2 = x_{1,2}, f_3 = x_{2,2} + x_{3,1}, f_4 = x_{2,1}$. The coefficient matrix of $F = \{f_1, f_2, f_3, f_4\}$ is the following:

$$M_F = \begin{pmatrix} 00 & 00 & 01 \\ 01 & 00 & 00 \\ 00 & 01 & 10 \\ 00 & 10 & 00 \end{pmatrix}$$

- We claim that $\operatorname{Cl}(f_1, f_2, f_3) = \emptyset$. Indeed, the submatrix of M_F formed by the first three rows contains a basis from the columns $x_{1,2}, x_{2,2}$, and $x_{3,2}$. Hence, $\{f_1, f_2, f_3\}$ is safe and, thus, $\operatorname{Cl}(f_1, f_2, f_3) = \emptyset$.
- Let us show that $\operatorname{Cl}(f_1, f_2, f_3, f_4) = \{2, 3\}$. Indeed, if we remove both the second and third blocks, the resulting matrix will have the basis consisting of only column $x_{1,2}$. The rank of M_F is 4, which is greater than the number of blocks. If we remove only the second or only the third block, the rank of the obtained matrix will be 3, which is also greater than the number of remaining blocks. Hence, $\operatorname{Cl}(f_1, f_2, f_3, f_4) = \{2, 3\}$.

Let F be a set of linear forms with coefficient matrix M_F. We say that a subset of blocks $A \subseteq [m]$ is coverable with respect to M_F if one can choose $|A|$ linearly independent columns from matrix A such that every block from A contains one chosen column. Consider the following order $\preceq$ on the subsets of $[m]$: $A \preceq B$, if $\sum_{i \in A} 2^i \leq \sum_{i \in B} 2^i$. An *amortized closure* of F is the $\preceq$-maximal coverable with respect to M_F subset of $[m]$. We denote the amortized closure of F by $\widetilde{\operatorname{Cl}}(F)$.

In Example 1.6, $\widetilde{\operatorname{Cl}}(f_1) = \{3\}, \widetilde{\operatorname{Cl}}(f_1, f_2) = \{1, 3\}, \widetilde{\operatorname{Cl}}(f_1, f_2, f_3) = \{1, 2, 3\}$ and $\widetilde{\operatorname{Cl}}(f_1, f_2, f_3, f_4) = \{1, 2, 3\}$.

The uniqueness of amortized closure trivially follows from the definition. We establish other properties in the following theorem:

Theorem 1.7. Amortized closure has the following properties.

1. (Size bound) $|\widetilde{\operatorname{Cl}}(F)| \leq \dim\langle F \rangle$ (Lemma 2.10);
2. (Span invariance) If $\langle F \rangle = \langle H \rangle$, then $\widetilde{\operatorname{Cl}}(F) = \widetilde{\operatorname{Cl}}(H)$ (Lemma 2.11);

3. (Relation between closures)
   (a) $\mathrm{Cl}(F) \subseteq \widetilde{\mathrm{Cl}}(F)$ (Lemma 2.15);
   (b) If $\mathrm{Cl}(F \cup \{f\}) \neq \mathrm{Cl}(F)$, then $\widetilde{\mathrm{Cl}}(F \cup \{f\}) = \widetilde{\mathrm{Cl}}(F)$ (Lemma 2.17);
4. (Continuity) $\widetilde{\mathrm{Cl}}(F) \subseteq \widetilde{\mathrm{Cl}}(F \cup \{f\})$ and $|\widetilde{\mathrm{Cl}}(F \cup \{f\})| \leq |\widetilde{\mathrm{Cl}}(F)| + 1$ (Theorem 2.18);
5. (Monotonicity) If $F \subseteq \langle H \rangle$, then $\widetilde{\mathrm{Cl}}(F) \subseteq \widetilde{\mathrm{Cl}}(H)$ (Corollary 2.19);

Since the amortized closure contains the plain closure, the amortized closure also *contains all essential unlifted variables*, i.e. linear systems do not restrict values of unlifted variables out of the amortized closure. The most technically involved part is the proof of continuity of amortized closure.

1.2.3 Lower bound for depth-$cn \log n$ Res($\oplus$)

Alekseev and Itsykson [3] have recently proved that every Res($\oplus$) refutation of lifted Tseitin formulas either has size at least $2^{\Omega(n/\log n)}$ or depth at least $\Omega(n \log \log n)$, where n is the number of variables. Our Theorem 1.4 is the improvement of this result, and its proof is basically built on the proof by Alekseev and Itsykson [3]. To explain our contribution, we start by presenting the idea of the former result. This tradeoff was proved for the lifted formulas $\varphi \circ g$, where $g : \{0,1\}^\ell \to \{0,1\}$ is a 2-stifling gadget (for example, g can be the ℓ-input majority for $\ell \geq 5$; see Section 3.2 for definition) and φ satisfies rather strong conditions. Namely, there exists a set of partial assignments $\mathcal{A}$ to variables of φ and integer numbers t and p such that the following conditions hold.

1. Any assignment from $\mathcal{A}$ does not falsify a clause of φ.
2. For any assignment $\sigma \in \mathcal{A}$, for any $\rho \subseteq \sigma$, $\rho \in \mathcal{A}$.
3. Any Res($\oplus$) refutation Π of $\varphi \circ g$ satisfies the following *random-walk* property.
   - We say that a linear clause C in the lifted variables is $\mathcal{A}$-good if the system $\neg C$ corresponds to some assignment from $\mathcal{A}$; i.e. there exists a solution σ of $\neg C$ that induces on $\mathrm{Cl}(L(C))$ an assignment from $\mathcal{A}$, where $L(C)$ denotes the set of linear forms that appear in C.
   - Consider arbitrary $\mathcal{A}$-good clause C_0 from Π such that $|\mathrm{Cl}(L(C_0))| \leq t/2$. Let $\rho_0 \in \mathcal{A}$ correspond to $\neg C_0$. Let τ be a random solution of $\neg C_0$ among all solutions inducing the partial assignment ρ_0 on unlifted variables. We make $t/2$ steps in Π starting in C_0, and on each step, we move from the current linear clause to a premise of the rule falsified by τ (we count only steps corresponding to resolution rules and do not count weakening rules). Then, with probability at least 2^{-p}, this walk finishes in an $\mathcal{A}$-good clause.

Fortunately, Tseitin formulas meet these conditions for appropriate $\mathcal{A}, p$, and t [3].

Assume that there is a Res($\oplus$) refutation Π of $\varphi \circ g$ of size less than 2^s, where s is some parameter. The following argument was used in [3] to prove that Π has a large depth. Let C_0 be the empty clause from a Π; C_0 is $\mathcal{A}$-good for trivial reasons. By the random-walk property on the distance $t/2$ from C_1, there is an $\mathcal{A}$-good clause C_1. If $|\mathrm{Cl}(L(C_1))| \leq t/2$, then by the random walk property on the distance $t/2$ from C_0, there is an $\mathcal{A}$-good clause C_2, and so on. Let we finish this process at $\mathcal{A}$-good clause C_k such that $|\mathrm{Cl}(L(C_k))| > t/2$. Then we get that the depth of Π is at least $kt/2$. We have to show that k can be sufficiently large, for this we have to use that the size of Π is less than 2^s.

To bound k from below, Alekseev and Itsykson [3] estimate the rank of $\neg C_{i+1}$ in comparison to the rank $\neg C_i$. Namely, the size upper bound on Π together with the random-walk property imply that one can choose C_{i+1} such that $\mathrm{rk}(\neg C_{i+1}) \leq \mathrm{rk}(\neg C_i)(\ell+1) + p + s$. Since the estimated value of the rank can be increased in at least $(\ell+1)$ times by one step, in this approach $k \leq \log_{(\ell+1)} \frac{t}{2(p+s)} + 1$. The total depth that can be achieved by this approach is at most $O(t \log \frac{t}{p+s})$.

Our improvement. Instead of estimating rank, we suggest estimating the size of the amortized closure $|\widetilde{\mathrm{Cl}}(\neg C_i)|$. We prove the following lemma.

Lemma 1.8 (Lemma 5.1)**.** Let Φ and Ψ be two linear systems in the lifted variables $X = \{x_{i,j} \mid i \in [m], j \in [\ell]\}$. Let π be a partial assignment defined on $\{x_{i,j} \mid i \in [\mathrm{Cl}(L(\Phi))], j \in [\ell]\}$. Let Σ consist of all solutions σ of Φ such that σ extends π. Assume that $\Sigma \neq \emptyset$. Let τ be a random element of Σ. Then $\Pr[\tau \text{ satisfies } \Psi] \leq 2^{|\widetilde{\mathrm{Cl}}(L(\Phi))|-|\widetilde{\mathrm{Cl}}(L(\Psi))|}$.

Lemma 1.8, the upper bound $|\Pi| < 2^s$ and the random-walk property imply that on the distance $t/2$ from C_i one can find an $\mathcal{A}$-good C_{i+1} such that $|\widetilde{\mathrm{Cl}}(L(C_{i+1})| \leq |\widetilde{\mathrm{Cl}}(L(C_i)| + p + s$. So we can achieve $k = \lceil \frac{t}{2(p+s)} \rceil$ and depth at least $\Omega\left(\frac{t^2}{p+s}\right)$. This is sufficient to establish Theorem 1.4.

Notice that there is a potential way to improve k by improving the upper bound on p in the random-walk property and taking smaller s.

1.3 Discussion about closures

- The concept of closure proves helpful when addressing problems with an underlying lifted structure. In such cases, the closure of a set of linear forms effectively captures the most essential unlifted variables. Furthermore, when the lifting involves a 1-stifling gadget, the set of linear forms imposes no constraints on variables outside the closure.
- Plain closure is monotone but not necessarily continuous. Amortized closure, containing plain closure, is both monotone and continuous. For the best results, using both is recommended: plain closure more accurately identifies essential unlifted variables, while amortized closure allows for more convenient estimations.
- While (as shown by [11]) closure is not required for parity decision trees (i.e., for tree-like Res($\oplus$)), where essential unlifted variables can be captured iteratively along a path, closure (both plain and amortized) provides a key advantage in dag-like proofs: path-independence. This invariance is why closure is necessary for lower bounds in regular and bounded-depth Res($\oplus$). Furthermore, our first application shows that even for tree-like Res($\oplus$) in bounded-width settings, amortized closure can give better results, as in our case, it applies to a broader class of gadgets.
- A limitation of using closure is that variables within the closure are not necessarily indeed constrained by the linear forms. It seems to be one of the primary obstacles preventing us from applying a bottleneck argument to unrestricted Res($\oplus$).

1.4 Further research

We identify the following questions as interesting directions for further investigation.

- Prove a supercritical tradeoff between the size and depth of dag-like Res($\oplus$) refutations. Specifically, provide an example of a family of formulas with a polynomial-size Res($\oplus$) refutation, yet every such refutation has a depth that exceeds the number of variables. While numerous supercritical tradeoffs between the size and depth exist for resolution [15, 8, 13, 17], all use the width-size relationship, which remains unknown for Res($\oplus$). Thus, the question requires some additional ideas.
- Prove a superpolynomial lower bound for Res($\oplus$) refutations of depth $n^{1+\epsilon}$ for some $\epsilon > 0$. As we noticed above, improving the success probability in the random-walk theorem from [3] is sufficient for further depth improvement.
- Prove a lifting theorem that translates lower bounds on resolution width to lower bounds on the size of Res($\oplus$) refutations with depth at most n. The lifted Tseitin formula is the only known example of a lower bound for bounded-depth Res($\oplus$). Such a lifting theorem will provide a method for generating many such examples.

2 Closure and amortized closure

In this section, we give preliminaries about closure, provide a definition of amortized closure, and prove its main properties.

Throughout the paper, we use the notation $\langle S \rangle$ to denote the span of the set of vectors S from some vector space.

2.1 Safe and dangerous sets of linear forms

We consider the set of propositional variables $X = \{x_{i,j} \mid i \in [m], j \in [\ell]\}$. The variables from X are divided into m blocks by the value of the first index. The variables $x_{i,1}, x_{i,2}, \ldots, x_{i,\ell}$ form the ith block, for $i \in [m]$.

Consider sets of linear forms using variables from X over the field $\mathbb{F}_2$. The *support* of a linear form $f = x_{i_1,j_1} + x_{i_2,j_2} + \cdots + x_{i_k,j_k}$ is the set $\{i_1, i_2, \ldots, i_k\}$ of blocks of variables that appear in f with non-zero coefficients. We denote the support by $\mathrm{supp}(f)$. The support of a set of linear forms F is the union of the supports of all linear forms in this set. We denote it by $\mathrm{supp}(F)$. We say that a linearly independent set of linear forms F is *dangerous* if $|F| > |\mathrm{supp}(F)|$. We say that a set of linear forms F is *safe* if $\langle F \rangle$ does not contain a dangerous set. If F is linearly dependent but $\langle F \rangle$ contains a dangerous set, instead of saying that F is dangerous, we say it is not safe.

Every linear form corresponds to a vector of its coefficients indexed by the variables from the set X. Given a list of linear forms $f_1, f_2, \ldots, f_k$, one may consider their coefficient matrix of size $k \times |X|$ in which the i-th row coincides with the coefficient vector of f_i.

Theorem 2.1 ([14])**.** Let $f_1, f_2, \ldots, f_k$ be linearly independent linear forms and let M be their coefficient matrix. Then, the following conditions are equivalent.

(1) The set of linear forms $f_1, f_2, \ldots, f_k$ is safe.

(2) One can choose k blocks and one variable from each of these blocks such that the columns of M corresponding to the k chosen variables are linearly independent. (Since $\mathrm{rk}(M) = k$ the chosen set of columns forms the basis.)

2.2 Closure

Let $S \subseteq [m]$ be a set of blocks; for a linear form f we denote by $f[\backslash S]$ a linear form obtained from f by substituting 0 for all variables with support in S. For a set of linear forms F we will use the notation $F[\backslash S] = \{f[\backslash S] \mid f \in F\}$.

A *closure* of a set of linear forms F is any inclusion-wise minimal set $S \subseteq [m]$ such that $F[\backslash S]$ is safe.

Lemma 2.2 (Uniqueness [14])**.** For any F, its closure is unique.

We denote the closure of F by $\mathrm{Cl}(F)$.

Lemma 2.3 (Monotonicity [14])**.** If $F_1 \subseteq F_2$, then $\mathrm{Cl}(F_1) \subseteq \mathrm{Cl}(F_2)$.

Lemma 2.4 (Span invariance [14])**.** $\mathrm{Cl}(F) = \mathrm{Cl}(\langle F \rangle)$.

Lemma 2.5 (Size bound [14])**.** $|\mathrm{Cl}(F)| + \dim\langle F[\setminus \mathrm{Cl}(F)]\rangle \leq \dim\langle F\rangle$, and hence $|\mathrm{Cl}(F)| \leq \dim\langle F\rangle$.

A set of linear forms F is *minimally dangerous* if it is dangerous, and $\langle F \rangle$ does not contain a dangerous set with strictly smaller support than the support of F. Recall that a dangerous set is necessarily linearly independent.

Consider the following algorithm:

Algorithm 2.6. Input: a set of linear forms F.

1. $S \leftarrow \emptyset$;

2. While $\langle F[\setminus S]\rangle$ contains dangerous sets:
   (a) Find a minimally dangerous set in $\langle F[\setminus S]\rangle$. Let T be its support.
   (b) $S \leftarrow S \cup T$.
3. Return S.

Lemma 2.7 ([14])**.** Algorithm 2.6 computes $\mathrm{Cl}(F)$ regardless on choosing T on Step 2a.

Corollary 2.8. If F contains a minimally dangerous set with support $T \subseteq [m]$, then $\mathrm{Cl}(F) = T \cup \mathrm{Cl}(F[\setminus T])$.

2.3 Amortized closure and its properties

Let $V_1, V_2, \ldots, V_m$ be sets of vectors from some linear space over a field $\mathbb{F}$.

We say that a subset $A \subseteq [m]$ is *coverable* with respect to $V_1, V_2, \ldots, V_m$ if for every $i \in A$ there is $v_i \in V_i$ such the set $\{v_i \mid i \in A\}$ is linearly independent.

The following extension of the well-known Hall's matching theorem was proved by Welsh in 1971.

Theorem 2.9 ([24])**.** A set $A \subseteq [n]$ is coverable with respect to $V_1, V_2, \ldots, V_m$ if and only if for every $B \subseteq A$ the dimension of $\langle \cup_{i \in B} V_i \rangle$ is at least $|B|$.

We consider the following order $\preceq$ on the subsets of $[m]$: for any $A, B \subseteq [m]$, $A \preceq B$, if and only if $\sum_{i \in A} 2^i \leq \sum_{i \in B} 2^i$. We also define the strict order $A \prec B$, if and only if $A \preceq B$ and $A \neq B$.

Let $X = \{x_{i,j} \mid i \in [m], j \in [\ell]\}$ be the set of propositional variables and $F = \{f_1, f_2, \ldots, f_n\}$ be a set of $\mathbb{F}_2$-linear forms with variables from X. Consider a coefficient matrix of F: its columns correspond to X, and for all $i \in [n]$ ith row is the coefficient vector of f_i. For every $i \in [m]$, let V_i consist of matrix columns corresponding to variables with support $\{i\}$.

An *amortized* closure of F, denoted by $\widetilde{\mathrm{Cl}}(F)$, is the $\preceq$-maximal subset of $[m]$ that is coverable with respect to $V_1, V_2, \ldots, V_m$. It is easy to see that $\widetilde{\mathrm{Cl}}(F)$ does not depend on the permutation of rows in the coefficient matrix of F.

Lemma 2.10 (Size bound)**.** $|\widetilde{\mathrm{Cl}}(F)| \leq \dim\langle F\rangle$.

Proof. $|\widetilde{\mathrm{Cl}}(F)|$ is at most the rank of a coefficient matrix of F that equals $\dim\langle F\rangle$. □

Lemma 2.11 (Span invariance)**.** If $\langle F_1\rangle = \langle F_2\rangle$, then $\widetilde{\mathrm{Cl}}(F_1) = \widetilde{\mathrm{Cl}}(F_2)$.

Proof. It is well-known that for every finite set of vectors U from some linear space over $\mathbb{F}_2$ and for every basis of $\langle U\rangle$ one can obtain this basis from U by a sequence of the following to operations: 1) adding one vector to another; 2) removing zero.

Since $\langle F_1\rangle = \langle F_2\rangle$, we can choose the common basis in them. Thus, it is sufficient to verify that $\widetilde{\mathrm{Cl}}(\{f_1, f_2, \ldots, f_n\}) = \widetilde{\mathrm{Cl}}(\{f_1 + f_2, f_1, \ldots, f_n\})$ and $\widetilde{\mathrm{Cl}}(F \cup \{0\}) = \widetilde{\mathrm{Cl}}(F)$. Both these properties straightforwardly follow from the definition of amortized closure. □

We call a subset $T \subseteq [m]$ *important* for a set of linear forms F if there exists a safe linearly independent set of linear forms $\{h_1, h_2, \ldots, h_k\} \subseteq \langle F\rangle$ with support T such that $k = |T|$.

Proposition 2.12. If $\langle F\rangle$ contains a minimal dangerous set with support T, then T is important.

Proof. Let $\{h_1, h_2, \ldots, h_k, h_{k+1}\}$ be a minimal dangerous set with support T. The minimality implies that the set $h_1, h_2, \ldots, h_k$ is safe. The support of $\{h_1, h_2, \ldots, h_k\}$ equals T, since if it is less than T, this set would be dangerous. Hence, T is important. □

Lemma 2.13. Let T be important for F. Then $\widetilde{\mathrm{Cl}}(F) = T \cup \widetilde{\mathrm{Cl}}(F[\setminus T])$.

Proof. Since $\widetilde{\mathrm{Cl}}(F)$ is coverable, $\widetilde{\mathrm{Cl}}(F) \setminus T$ is also coverable. We know that $\widetilde{\mathrm{Cl}}(F[\setminus T]) \cap T = \emptyset$. Hence, $\widetilde{\mathrm{Cl}}(F) \setminus T \preceq \widetilde{\mathrm{Cl}}(F[\setminus T])$. Thus, $\widetilde{\mathrm{Cl}}(F) \preceq T \cup \widetilde{\mathrm{Cl}}(F[\setminus T])$.

We will show that for every $i \in T$, one can choose one column corresponding to a variable with support i such that all chosen columns are linearly independent and each of them does not belong to the linear space of columns corresponding to variables with support out of T. It will imply that $T \cup \widetilde{\mathrm{Cl}}(F[\setminus T])$ is also coverable and, thus, $\widetilde{\mathrm{Cl}}(F) = T \cup \widetilde{\mathrm{Cl}}(F[\setminus T])$.

Since T is important, there exists a linear independent and safe set $H = \{h_1, h_2, \ldots, h_k\} \in \langle F \rangle$ with support T of size k. Let us choose a basis F_1 in $\langle F \rangle$ that continues H. By Lemma 2.11, $\widetilde{\mathrm{Cl}}(F_1) = \widetilde{\mathrm{Cl}}(F)$. Consider the coefficient matrix M_H of H. Since H is safe and linearly independent, Theorem 2.1 implies that for every $i \in T$, one can choose a column u_i of M_H corresponding to a variable with support i such that all these columns are linearly independent. M_H is a submatrix of the coefficient matrix M_{F_1} of F_1. Let for $i \in T$, v_i be the collumn in M_{F_1} corresponding to u_i. $\{v_i \mid i \in T\}$ are also linearly imndependent since for all $i \in T$, u_i is the prefix of v_i. Notice that all columns of M_{F_1} corresponding to variables with support out of T have zeros in the first k coordinates, hence for all $i \in T$, v_i does not belong to the linear span of all columns of M_{F_1} with columns with support out of T. □

Lemma 2.14. If $F \subseteq G$, then $\widetilde{\mathrm{Cl}}(G) = \mathrm{Cl}(F) \cup \widetilde{\mathrm{Cl}}(G[\setminus \mathrm{Cl}(F)])$.

Proof. Consider the execution of Algorithm 2.6 on F. Let $T_1, T_2, \ldots, T_s$ be the minimally dangerous sets found by the algorithm. Then $\mathrm{Cl}(F) = T_1 \cup T_2 \cup \ldots T_s$.

By Proposition 2.12, T_1 is important for F, hence it is important for G. Then, by Lemma 2.13, $\widetilde{\mathrm{Cl}}(G) = T_1 \cup \widetilde{\mathrm{Cl}}(G[\setminus T_1])$. By Proposition 2.12, T_2 is important for $F[\setminus T_1]$, hence it is important for $G[\setminus T_1]$. Then, by Lemma 2.13, $\widetilde{\mathrm{Cl}}(G) = T_1 \cup T_2 \cup \widetilde{\mathrm{Cl}}(G[\setminus (T_1 \cup T_2)])$. Continue this reasoning s times we get that $\widetilde{\mathrm{Cl}}(G) = T_1 \cup T_2 \cup \cdots \cup T_s \cup \widetilde{\mathrm{Cl}}(G[\setminus (T_1 \cup T_2 \cup \cdots \cup T_s)]) = \mathrm{Cl}(F) \cup \widetilde{\mathrm{Cl}}(G[\setminus \mathrm{Cl}(F)])$. □

Lemma 2.15. $\mathrm{Cl}(F) \subseteq \widetilde{\mathrm{Cl}}(F)$

Proof. Follows from Lemma 2.14 applied to $G = F$. □

Lemma 2.16. If F is safe and for a linear form f, $F \cup \{f\}$ is not safe, then $\widetilde{\mathrm{Cl}}(F) = \widetilde{\mathrm{Cl}}(F \cup \{f\})$.

Proof. Since $F \cup \{f\}$ is not safe, $\langle F \cup \{f\} \rangle$ contains a minimally dangerous set $H = \{h_1, h_2, \ldots, h_{k+1}\}$ with support T of size k. Assume that H contains the maximal possible number of elements from $\langle F \rangle$. It is easy to see that the number of such elements should be k. Indeed, this number should be less than $k+1$ since F is safe; if H contains two elements from $f + \langle F \rangle$, we can change one of them to their sums, and this increases the number of elements from $\langle F \rangle$. Let $h_1, h_2, \ldots, h_k \in \langle F \rangle$ and $h_{k+1} \in f + \langle F \rangle$. Since F is safe, the support of $h_1, h_2, \ldots, h_k$ is also T. Hence, T is important, thus

$$\widetilde{\mathrm{Cl}}(F \cup f) \overset{\text{(Lem. 2.11)}}{=} \widetilde{\mathrm{Cl}}(F \cup \{h_{k+1}\}) \overset{\text{(Lem. 2.13)}}{=} T \cup \widetilde{\mathrm{Cl}}((F \cup \{h_{k+1}\})[\setminus T]) \overset{\text{(Lem. 2.11)}}{=}$$
$$T \cup \widetilde{\mathrm{Cl}}(F[\setminus T]) \overset{\text{(Lem. 2.13)}}{=} \widetilde{\mathrm{Cl}}(F).$$

□

The following Lemma extends Lemma 2.16.

Lemma 2.17. If $\mathrm{Cl}(F \cup \{f\}) \subsetneq \mathrm{Cl}(F)$, then $\widetilde{\mathrm{Cl}}(F \cup \{f\}) = \widetilde{\mathrm{Cl}}(F)$.

Proof. Consider the execution of Algorithm 2.6 on F. Let $T_1, T_2, \ldots, T_s$ be the minimally dangerous sets found by the algorithm. Then $\mathrm{Cl}(F) = T_1 \cup T_2 \cup \ldots T_s$. Notice that we can construct the closure of $F \cup \{f\}$ using the algorithm starting from the same sets $T_1, T_2, \ldots, T_s$. By multiple applications of Lemma 2.8, we get that $\mathrm{Cl}(F \cup \{f\}) = \mathrm{Cl}(F) \cup \mathrm{Cl}(F \cup \{f\}[\setminus \mathrm{Cl}(F)])$. By the definition of closure, $F[\setminus \mathrm{Cl}(F)])$ is

safe; since $\mathrm{Cl}(F \cup \{f\}) \neq \mathrm{Cl}(F)$, the set of linear forms $(F \cup \{f\})[\setminus \mathrm{Cl}(F)])$ is not safe. By Lemma 2.16, $\widetilde{\mathrm{Cl}}(F \cup \{f\})[\setminus \mathrm{Cl}(F)] = \widetilde{\mathrm{Cl}}(F)[\setminus \mathrm{Cl}(F)]$.

By Lemma 2.14 we get $\widetilde{\mathrm{Cl}}(F \cup \{f\}) = \widetilde{\mathrm{Cl}}((F \cup \{f\})[\setminus \mathrm{Cl}(F)]) \cup \mathrm{Cl}(F)$ and $\widetilde{\mathrm{Cl}}(F) = \widetilde{\mathrm{Cl}}(F[\setminus \mathrm{Cl}(F)]) \cup \mathrm{Cl}(F)$. Finally,

$$\widetilde{\mathrm{Cl}}(F \cup \{f\}) = \widetilde{\mathrm{Cl}}((F \cup \{f\})[\setminus \mathrm{Cl}(F)]) \cup \mathrm{Cl}(F) = \widetilde{\mathrm{Cl}}(F[\setminus \mathrm{Cl}(F)]) \cup \mathrm{Cl}(F) = \widetilde{\mathrm{Cl}}(F).$$

□

Theorem 2.18 (Continuity)**.** $\widetilde{\mathrm{Cl}}(F) \subseteq \widetilde{\mathrm{Cl}}(F \cup \{f\})$ and $|\widetilde{\mathrm{Cl}}(F \cup \{f\}) \setminus \widetilde{\mathrm{Cl}}(F)| \leq 1$.

We will prove Theorem 2.18 in Subsection 2.4.

Corollary 2.19 (Monotonicity)**.** If $F_1 \subseteq \langle F \rangle$, then $\widetilde{\mathrm{Cl}}(F_1) \subseteq \widetilde{\mathrm{Cl}}(F)$.

Proof. By Theorem 2.18, $\widetilde{\mathrm{Cl}}(F_1) \subseteq \widetilde{\mathrm{Cl}}(F_1 \cup F)$ and by Lemma 2.11, $\widetilde{\mathrm{Cl}}(F_1 \cup F) = \widetilde{\mathrm{Cl}}(F)$. □

2.4 Amortized closure is continues (proof of Theorem 2.18).

Let L and L' be vector spaces over a field $\mathbb{F}$ let $e \in L'$ be such that $e \notin L$ and $L' = \langle L \cup \{e\} \rangle$. Let π denote the projection from L' to L.

The following theorem implies Theorem 2.18.

Theorem 2.20. Let $V'_1, V'_2, \ldots, V'_m$ be sets of vectors from L'. Let for every $i \in [m]$, $V_i = \{\pi(v) \mid v \in V'_i\}$.

Let $T \subseteq [m]$ be $\preceq$-maximal coverable set with respect to $V'_1, V'_2, \ldots, V'_m$. Let $S \subseteq [m]$ be $\preceq$-maximal coverable set with respect to $V_1, V_2, \ldots, V_m$. Then $S \subseteq T$ and $|T \setminus S| \leq 1$.

Proof. For every $i \in T$ we choose $u'_i \in V'_i$ such that the set $\{u'_i \mid i \in T\}$ is linearly independent. For $i \in T$ we denote $u_i := \pi(u'_i)$. For every $i \in S$ we choose $v_i \in V_i$ such that the set $\{v_i \mid i \in S\}$ is linearly independent. Let for $i \in S$, v'_i be an element of V'_i such that $\pi(v'_i) = v_i$.

Notice that the set $\{v'_i \mid i \in S\}$ is also linearly independent, hence S is coverable with respect to $V'_1, V'_2, \ldots, V'_m$. By maximality of T, $S \preceq T$. If $S = T$, then the theorem holds; hence, assume that $S \prec T$ (strictly less). Let us denote $t := \max(T \setminus S)$.

The theorem holds if $S \cup \{t\} = T$. So, we assume that $S \cup \{t\} \neq T$.

Claim 2.21. $S \cup \{t\}$ is coverable with respect to $V'_1, V'_2, \ldots, V'_m$.

Proof. We will maintain the set of vectors $\{w'_i \mid i \in S \cup \{t\}\}$ that satisfies the following properties:

1. If $i \in S$ and $i < t$, then $w'_i = v'_i$;
2. $w'_t = u'_t$;
3. If $i \in S$ and $i > t$, then either $w'_i = v'_i$, or $w'_i = u'_i$;
4. The inequality $\dim\langle\{w_i \mid i \in S \cup \{t\}\}\rangle \geq |S|$ holds, where for all $i \in S \cup \{t\}$, $w_i = \pi(w'_i)$.

Initially assume that for all $i \in S$ and $i \neq t$, $w'_i := v'_i$ and $w'_t = u'_t$. In other words the set $\{w'_i \mid i \in S \cup \{t\}\}$ initially equals $\{v'_i \mid i \in S\} \cup \{u'_t\}$. It is easy to verify that all properties above are satisfied.

While the set of vectors $\{w'_i \mid i \in S \cup \{t\}\}$ is not linearly independent, we apply to this set some operation that will guarantee the satisfaction of all properties. We describe this operation below.

Since $\dim\{w_i \mid i \in S \cup \{t\}\} \geq |S|$, we also have that $\dim\{w'_i \mid i \in S \cup \{t\}\} \geq |S|$. Since $\{w'_i \mid i \in S \cup \{t\}\}$ is not linearly independent, $\dim\langle\{w'_i \mid i \in S \cup \{t\}\}\rangle = |S|$. Thus, there exists a unique non-empty set $I \subseteq S \cup \{t\}$ and non-zero elements $\{\alpha_i \in \mathbb{F}\}_{i \in I}$ such that $\sum_{i \in I} \alpha_i w'_i = 0$; and, thus, $\sum_{i \in I} \alpha_i w_i = 0$.

We claim that for all $j \in I$, $j \geq t$. Indeed, assume that for some $j \in I$, $j < t$, Then $\langle\{w_i \mid i \in S \cup \{t\} \setminus \{j\}\}\rangle$ contains $\langle\{w_i \mid i \in S \cup \{t\}\}\rangle$ whose dimension is at least $|S|$, thus $S \cup \{t\} \setminus \{j\}$ is coverable with respect to $V_1, \ldots, V_n$, but $S \prec S \cup \{t\} \setminus \{j\}$; contradiction with the maximality of S.

It is impossible to have $w'_i = u'_i$ for all $i \in I$ since all u'_i are linearly independent. Thus, there exists $k \in I$ such that $w'_k = v'_k \neq u'_k$. Since $k \in I$, $\{w_i \mid i \in S \cup \{t\}\} \in \langle \{w_i \mid i \in S \cup \{t\} \setminus \{k\}\rangle$, by the dimension argument we get that the set $\{w_i \mid i \in S \cup \{t\} \setminus \{k\}\}$ is linearly independent. Let us change values $w'_k := u'_k$ (and, correspondingly, $w_k := u_k$). Note that $\dim\langle \{w_i \mid i \in S \cup \{t\}\}\rangle \geq \dim\langle \{w_i \mid i \in S \cup \{t\} \setminus \{k\}\}\rangle = |S|$, hence all the properties are satisfied for new values of w'_i.

We can't apply this operation infinitely since the value $|\{i \in S \mid i > t, w'_i \neq u'_i\}|$ is decreased on every step. Hence, at some moment, we can't apply the operation, which means that $\{w'_i \mid i \in S \cup \{t\}\}$ is linearly independent and, thus, $S \cup \{t\}$ is coverable with respect to $V'_1, V'_2, \ldots, V'_m$. □

Consider the set $\{u_i \mid i \in T\}$. Since $\{u'_i \mid i \in T\} \in \langle \{u_i \mid i \in T\} \cup \{e\}\rangle$, $\dim\langle \{u_i \mid i \in T\}\rangle \geq |T| - 1$.

If $\dim\langle \{u_i \mid i \in T\}\rangle = |T|$, the set $\{u_i \mid i \in T\}$ is linearly independent, we get a contradiction with maximality of S since $S \prec T$. Thus, $\dim\langle \{u_i \mid i \in T\}\rangle = |T| - 1$. Let us fix some $\ell \in T$ such that u_ℓ is in the span of u_i for $i \in T \setminus \{\ell\}$. In this case $\{u_i \mid i \in T \setminus \{\ell\}\}$ is linearly independent, thus $T \setminus \{\ell\}$ is coverable with respect to $V_1, \ldots, V_m$.

Claim 2.22. $t \leq \ell$

Proof. The set $T \setminus \{\ell\}$ is coverable with respect to $V_1, \ldots, V_m$. Since S is the maximal coverable, $T \setminus \{\ell\} \preceq S$. It implies that $t \leq \ell$. □

Claim 2.23. $t \neq \ell$

Proof. Assume that $t = \ell$. By Claim 2.21 the set $S \cup \{\ell\}$ is coverable with respect to $V'_1, \ldots, V'_n$. Then $S \cup \{\ell\} \preceq T$. Since $S \cup \{\ell\} = S \cup \{t\} \neq T$, $S \cup \{\ell\} \prec T$. Let $h = \max(T \setminus (S \cup \{\ell\})$. It is straightforward that $h < t = \ell$. By the definition of h we get that $S \prec \{i \in T \mid i \geq h, i \neq \ell\}$, but the set $\{u_i \mid i \in T, i \geq h, i \neq \ell\}$ is linearly independent since it is a subset of $\{u_i \mid i \in T \setminus \{\ell\}\}$. This contradicts the maximality of S. □

The last two claims imply $t < \ell$.

Claim 2.21 implies that $S \cup \{t\} \preceq T$. If $S \cup \{t\} \neq T$, then $S \cup \{t\} \prec T$. Let $t' = \max(T \setminus (S \cup \{t\})$.

Let $J = (\{t' + 1, \ldots, m\} \setminus \{t, \ell\}) \cap T$. The set $J \cup \{t', t\}$ is coverable with respect to $V_1, V_2, \ldots, V_m$ since $\{u_j \mid j \in T \setminus \{\ell\}\}$ is linearly independent. The set $J \cup \{\ell\}$ is coverable with respect to $V_1, V_2, \ldots, V_m$ since v_i for $i \in S$ are linearly independent and $t < \ell$. The sets $J \cup \{\ell, t\}$ and $J \cup \{\ell, t'\}$ are not coverable with respect to $V_1, V_2, \ldots, V_m$ since it would contradict maximality of S. The following lemma (Lemma 2.24) implies that such a situation is impossible. We get a contradiction with our assumption that the theorem does not hold. □

Lemma 2.24. Let $J \subseteq [m]$, t, t' and ℓ be different elements from $[m] \setminus J$. Assume that $J \cup \{\ell\}$ is coverable with respect to $V_1, V_2, \ldots, V_m$ but $J \cup \{\ell, t\}$ and $J \cup \{\ell, t'\}$ are not coverable. Then $J \cup \{t', t\}$ is not coverable.

Proof. Asume for a sake of contradiction that $J \cup \{t', t\}$ is coverable.

For any set $A \subseteq [m]$ we will use the notation $U(A) := \langle \bigcup_{i \in A} V_i \rangle$.

By Theorem 2.9 since $J \cup \{\ell, t\}$ is not coverable, there exists $A \subseteq J \cup \{\ell, t\}$ such that $\dim U(A) < |A|$. Since $J \cup \{\ell\}$ and $J \cup \{t', t\}$ are coverable, both ℓ and t belong A. Let us denote $A' := A \setminus \{\ell, t\}$.

Since $J \cup \{t', t\}$ is coverable, $\dim U(A' \cup \{t\}) \geq |A'| + 1$. Since $J \cup \{\ell\}$ is coverable, $\dim U(A' \cup \{\ell\}) \geq |A'| + 1$. But we know that $\dim U(A' \cup \{t, \ell\}) \leq |A|' + 1$, hence $\dim U(A' \cup \{t\}) = \dim U(A' \cup \{\ell\}) = \dim U(A' \cup \{t, \ell\}) = |A'| + 1$. The last equality implies that $V_\ell \subseteq U(A' \cup \{t\})$ and $V_t \subseteq U(A' \cup \{\ell\})$.

Analogously using that $J \cup \{\ell, t'\}$ is not coverable we get that there exists $B' \subseteq [m] \setminus \{\ell, t'\}$ such that $\dim U(B' \cup \{t'\}) = \dim U(B' \cup \{\ell\}) = \dim U(B' \cup \{t', \ell\}) = |B'| + 1$. This equality implies that $V_\ell \subseteq U(B' \cup \{t'\})$ and $V_{t'} \subseteq U(B' \cup \{\ell\})$.

By our assumption, the set $J \cup \{t', t\}$ is coverable. So, we may estimate

$$|A' \cup B'| + 2 \le \dim U(A' \cup B' \cup \{t, t'\}) \le \dim U(A' \cup B' \cup \{t, t', \ell\}) =$$
$$\dim U(A' \cup B' \cup \{t', \ell\}) = \dim U(A' \cup B' \cup \{\ell\}) =$$
$$\dim U(A' \cup \{\ell\}) + \dim U(B' \cup \{\ell\}) - \dim U((A' \cap B') \cup \{\ell\}) \le$$
$$|A'| + 1 + |B'| + 1 - (|A' \cap B'| + 1) = |A' \cup B'| + 1,$$

and get a contradiction. In the first equality, we explore that $V_t \subseteq U(A' \cup \{\ell\})$. In the second equality we explore that $V_{t'} \subseteq U(B' \cup \{\ell\})$. In the third equality we use that $\dim\langle X \cup Y\rangle = \dim\langle X\rangle + \dim\langle Y\rangle - \dim(\langle X\rangle \cap \langle Y\rangle)$. In the last inequality we used the known values of $\dim U(A' \cup \{\ell\})$ and $\dim U(B' \cup \ell)$ and that $J \cup \{\ell\}$ is coverable. □

3 Preliminary knowledge on resolution over parities and lifting

3.1 Resolution and resolution over parities

Here and after, all scalars are from the field $\mathbb{F}_2$. Let X be a set of variables that take values in $\mathbb{F}_2$. A linear form in variables from X is a homogeneous linear polynomial over $\mathbb{F}_2$ in variables from X or, in other words, a polynomial $\sum_i^n x_i a_i$, where $x_i \in X$ is a variable and $a_i \in \mathbb{F}_2$ for all $i \in [n]$. A linear equation is an equality $f = a$, where f is a linear form and $a \in \mathbb{F}_2$.

A *linear clause* is a disjunction of linear equations: $\bigvee_{i=1}^t (f_i = a_i)$. Notice that over $\mathbb{F}_2$ a linear clause $\bigvee_{i=1}^t (f_i = a_i)$ may be represented as the negation of a linear system: $\neg \bigwedge_{i=1}^t (f_i = a_i + 1)$.

For a linear clause C we denote by $L(C)$ the set of linear forms that appear in C; i.e. $L\left(\bigvee_{i=1}^t (f_i = a_i)\right) = \{f_1, f_2, \ldots, f_t\}$. The same notation we use for linear systems: if Ψ is a $\mathbb{F}_2$-linear system, $L(\Psi)$ denotes the set of all linear forms from Ψ.

Let φ be an unsatisfiable CNF formula. A refutation of φ in the proof system Res($\oplus$) [19] is a sequence of linear clauses $C_1, C_2, \ldots, C_s$ such that C_s is the empty clause (i.e., identically false) and for every $i \in [s]$ the clause C_i is either a clause of φ or is obtained from previous clauses by one of the following inference rules:

- *Resolution rule* allows us to derive from linear clauses $C \vee (f = a)$ and $D \vee (f = a+1)$ the linear clause $C \vee D$.
- *Weakening rule* allows us to derive from a linear clause C an arbitrary linear clause D in the variables of φ that semantically follows from C (i.e., any assignment satisfying C also satisfies D).

The *width* (sometimes the term rank is used for the same notion) of a Res($\oplus$) refutation is the maximal rank of the negation of a linear clause from the refutation.

A Res($\oplus$) refutation of φ is a *tree-like* if it can be arranged as a tree, where leaves correspond clauses of φ and any clause in the interior node is obtained by a rule from the clauses in its children.

The *depth* of a Res($\oplus$) refutation is the maximal number of resolution rules applied on a path between a clause of the initial formula and the empty clause.

A resolution refutation of a formula φ is a special case of a Res($\oplus$) refutation, where all linear clauses are plain (i.e., disjunctions of literals). For resolution refutations, we also use the notions of *width* and *depth* that correspond to the same notions in Res($\oplus$) refutations.

3.2 Lifting of formulas via gadget

For every CNF formula Φ with variables $Y = \{y_1, y_2, \ldots, y_m\}$ and every Boolean function $g\colon \{0,1\}^\ell \to \{0,1\}$ we define a CNF formula $\Phi \circ g$ with variables $X = \{x_{i,j} \mid i \in [m], j \in [\ell]\}$ representing

$\Phi(g(x_{1,1}, x_{1,2}, \ldots, x_{1,\ell}), g(x_{2,1}, x_{2,2}, \ldots, x_{2,\ell}), \ldots, g(x_{m,1}, x_{m,2}, \ldots, x_{m,\ell}))$ (i.e. we substitute to every variable of Φ the function g applied to ℓ fresh variables). Let $\Phi = \bigwedge_{i \in I} C_i$, where C_i is a clause for all $i \in I$. For every $i \in [m]$ we denote by $y_i \circ g$ the cannonical CNF formula representing $g(x_{i,1}, x_{i,2}, \ldots, x_{i,\ell})$ which has ℓ variables in every clause and by $(\neg y_i) \circ g$ the cannonical CNF formula representing $\neg g(x_{i,1}, x_{i,2}, \ldots, x_{i,\ell})$ which has ℓ variables in every clause. Let $C_i = l_{i,1} \vee l_{i,2} \vee \cdots \vee l_{i,n_i}$, where l_i is a literal. Then we denote by $C_i \circ g$ a CNF formula that represents $l_{i,1} \circ g \vee l_{i,2} \circ g \vee \cdots \vee l_{i,n_i} \circ g$ as follows: $C_i \circ g$ consists of all clauses of the form $D_1 \vee D_2 \vee \cdots \vee D_{n_i}$, where D_j is a clause of $l_{i,j} \circ g$ for all $j \in [m_i]$. And $\Phi \circ g := \bigwedge_{i \in I} C_i \circ g$.

We refer to $\Phi \circ g$ as a formula Φ *lifted with a gadget* g. We refer to the set $Y = \{y_1, y_2, \ldots, y_m\}$ as a set of *unlifted* variables and to the set $X = \{x_{i,j} \mid i \in [m], j \in [\ell]\}$ as a set of *lifted* variables.

Sometimes, we will identify subsets of $[m]$ with corresponding subsets of Y. It is especially convenient to use such correspondence for the notions of support, closure, and amortized closure. So, we will assume that the support and the (amortized) closure of the set of linear forms over lifted variables is the set of unlifted variables.

A partial assignment ρ to the set of variables X is called block-respectful if, for every i, ρ either assigns values to all variables with support i or does not assign values to any of them.

Suppose that ρ is a block-respectful partial assignment. Then we define by $\hat{\rho}$ the partial assignment on the set of variables Y such that $\hat{\rho}(y_i) = g(\rho(x_{i,1}, x_{i,2}, \ldots, x_{i,\ell}))$ (here we assume that if the right-hand side is undefined, then the left-hand side is also undefined).

Let $k < \ell$. A gadget (i.e. Boolean function) $g : \{0,1\}^\ell \to \{0,1\}$ is called *k-stifling* [11] if for every $A \subset [\ell]$ of size k for every $c \in \{0,1\}$ there exists $a \in \{0,1\}^\ell$ such that for every $b \in \{0,1\}^\ell$ if a and b agree on set of indices $[\ell] \setminus A$, then $g(b) = c$.

Lemma 3.1 ([7], [3])**.** Let Ψ be a satisfiable linear system in the lifted variables X. Let $g\colon \{0,1\}^\ell \to \{0,1\}$ be a 1-stifling gadget. Suppose

- σ is a full assignment to lifted variables X satisfying Ψ.
- π is a full assignment to unlifted variables Y such that $\pi|_{\mathrm{Cl}(L(\Psi))} = \hat{\sigma}|_{\mathrm{Cl}(L(\Psi))}$.

Then there exists a full assignment τ to the lifted variables X such that τ satisfies Ψ and

$$\hat{\tau} = \pi.$$

Lemma 3.2 ([3])**.** Let Ψ be a satisfiable linear system in the lifted variables X. Let $g\colon \{0,1\}^\ell \to \{0,1\}$ be a 1-stifling gadget. Suppose there exists a full assignment σ to lifted variables X satisfying Ψ such that $\hat{\sigma}|_{\mathrm{Cl}(L(\Psi))}$ does not falsify any clause of φ. Then, Ψ does not contradict any clause of $\varphi \circ g$.

4 Bounded-width lifting theorem

In this section, we present our first application of amortized closure. Namely, we give an easy proof of the lifting theorem that extends Theorem 1.2 recently obtained by Chattopadhyay and Dvorak [10]. In Subsection 4.1, we define bounded-width games characterizing resolution depth and tree-like Res($\oplus$) size. In Subsection 4.2, we state and prove our lifting theorem.

4.1 Bounded-width games for resolution and resolution over parities

Consider the following bounded-width Prover-Adversary game [6, 15]. The game is defined for an unsatisfiable CNF formula φ and integer parameter $w \geq 1$. During the game, players save a partial assignment ρ. Initially, ρ is empty. Every her move, Prover has several possibilities: 1) Forget: change ρ to ρ' if $\rho' \subseteq \rho$; 2) Query: if $|\rho| < w$, Prover can choose a variable x not from domain of ρ and Adversary chooses $a \in \{0,1\}$ and changes $\rho := \rho \cup \{x := a\}$. For every move, Adversary earns a coin. The game ends if ρ falsifies a clause of φ.

Lemma 4.1 (Lemma 6 from [6])**.** An unsatisfiable CNF formula φ has resolution refutation of width w and depth d if and only if Prover has a strategy in the game for φ with the parameter $w+1$ that guarantees that Adversary earns at most d coins for any his behavior.

Now, we introduce a bounded-width Res($\oplus$)-Prover-Delayer game. This game is also defined on an unsatisfiable formula φ and a parameter w. The players save a linear system Ψ, which is initially empty. Prover has several possibilities for every her move: 1) Forget: change the system Ψ to any system Ψ' such that Ψ semantically implies Ψ'. 2)Query: if $\mathrm{rk}(\Psi) < w$, Prover can choose a linear form f. Delayer can either choose a value $a \in \{0,1\}$ and change Ψ to $\Psi \wedge (f = a)$ or report $*$, in the second case Prover chooses $a \in \{0,1\}$ by herself and update Ψ to $\Psi \wedge (f = a)$. Delayer earns a coin for each answer $*$. The game ends if the system Ψ contradicts a clause of φ.

Lemma 4.2. If Delayer has a strategy in the game defined for an unsatisfiable formula φ with parameter $w+1$ that guarantees him to earn at least d coins, then the size of any tree-like Res($\oplus$) refutation of φ of width at most w has size at least 2^d.

Proof. Consider a tree-like Res($\oplus$) refutation Π of φ with width at most w. For a node v of the proof tree, we denote by C_v a linear clause that labels v. Based on Delayer's strategy, we define a random path from the root to a leaf of Π. We start a path in the root of the proof tree that corresponds to an empty clause. To define a path we will play the bounded-width game on the formula φ. The linear system in the game always equals the negation of the current clause. At the root, we have the empty linear system.

If a current node u has only one child v (i.e., it corresponds to the weakening rule), we move to this child v. Since C_v semantically implies C_u, $\neg C_u$ semantically implies $\neg C_v$. In the game, we change a linear system $\neg C_u$ to its semantical implication $\neg C_v$. It is easy to see that $\mathrm{rk}(\neg C_v) \le \mathrm{rk}(\neg C_u)$.

Assume that C_u results from the resolution rule applied to C_{u_0} and C_{u_1}, and f_u is the resolved linear form. In this case $C_{u_0} = (f_u = 0) \vee D_0$ and $C_{u_1} = (f_u = 1) \vee D_1$ and $C_u = D_0 \vee D_1$. Prover asks for the value of the linear form f_u. It is a legal step since $\mathrm{rk}(\neg C_u) \le w$. If Delayer answers $*$, we choose $a \in \{0,1\}^*$ at random. Otherwise, $a \in \{0,1\}$ is the value chosen by Delayer. We move to u_{1-a}. In the game, we first get a linear system $(f_u = a) \vee \neg C_u$ and then change it to its semantical implication $\neg C_{1-a}$. With probability 1 we finish the path in a leaf ℓ of the proof tree. C_ℓ is a clause of φ, and thus $\neg C_\ell$ contradicts a clause of φ. By the property of Delayer's strategy, Delayer earns at least d coins at that moment. Thus, for every leaf, the probability that the path finishes in this leaf is at most 2^{-d}. Hence the number of leaves in the proof tree is at least 2^d. □

4.2 Proof of lifting theorem

Theorem 4.3. Let φ be an unsatisfiable CNF formula and $g\colon \{0,1\}^\ell \to \{0,1\}$ be a 1-stiffling gadget. Assume that $\varphi \circ g$ has a tree-like Res($\oplus$) refutation of rank w and size 2^d. Then φ has a resolution refutation of width w and depth d.

Proof. Proof by contradiction. Assume that φ does not have a resolution refutation of width w and depth d. Then, by Lemma 4.1, there is a strategy of Adversary in the first game for the formula φ and the parameter $w+1$ that guarantees him to earn at least $d+1$ coins. Using this strategy, we construct the strategy of Delayer in the second game for the formula $\varphi \circ g$ and the parameter $w+1$.

Let Ψ denote the current linear system in the second game; Ψ is a linear system in the lifted variables. Let ρ denote the current partial assignment in the first game; it assigns values to unlifted variables. We maintain the following invariant: ρ is defined on $\widetilde{\mathrm{Cl}}(L(\Psi))$ and Ψ has a solution π such that $\hat{\pi}$ coincides with ρ on $\widetilde{\mathrm{Cl}}(L(\Phi))$. Initially, Ψ is the empty system, ρ is the empty assignment, and the invariant holds for any π. Consider Prover's different types of moves in the second game.

First, assume that Prover makes a query and chooses a linear form f.

1. If $\widetilde{\mathrm{Cl}}(L(\Psi) \cup \{f\}) = \widetilde{\mathrm{Cl}}(L(\Psi))$. Delayer chooses a equals the value of f on π. The values ρ and π remain unchanged.

2. If $\widetilde{\mathrm{Cl}}(L(\Psi) \cup \{f\}) \neq \widetilde{\mathrm{Cl}}(L(\Psi))$, then by Theorem 2.18, $\widetilde{\mathrm{Cl}}(L(\Psi) \cup \{f\}) = \widetilde{\mathrm{Cl}}(L(\Psi)) \cup \{j\}$ for some $j \notin \widetilde{\mathrm{Cl}}(L(\Psi))$. Delayer reports $*$. We ask the value of the variable y_j in the first game and let a_j be the answer. We update $\rho := \rho \cup \{y_j := a_j\}$. Let Prover choose a value $a \in \{0,1\}$ in the second game. By Lemma 2.17, $\mathrm{Cl}(L(\Psi) \cup \{f\}) = \mathrm{Cl}(L(\Psi))$. Since $\mathrm{Cl}(L(\Psi) \cup \{f\}) = \mathrm{Cl}(L(\Psi)) \subseteq \widetilde{\mathrm{Cl}}(L(\Psi))$, Lemma 3.1 implies that there is a solution τ of $\Psi \wedge (f = a)$ such that $\hat{\tau}$ coincide with ρ on $\widetilde{\mathrm{Cl}}(L(\Psi))$. We update $\pi := \tau$.

Now assume that Prover forgets, i.e. she changes Ψ to Ψ', where Ψ semantically implies Ψ'. Then we restrict ρ on the set of variables $\widetilde{\mathrm{Cl}}(L(\Psi))$. Since $L(\Psi') \subseteq \langle L(\Psi) \rangle$, by Corollary 2.19 $\widetilde{\mathrm{Cl}}(L(\Psi')) \subseteq \widetilde{\mathrm{Cl}}(L(\Psi))$.

Assume that the invariant holds and ρ does not falsify any clause of φ. By Lemma 2.15, $\mathrm{Cl}(L(\Psi)) \subseteq \widetilde{\mathrm{Cl}}(L(\Psi))$, hence by Lemma 3.2, Ψ does not contradict a clause of $\varphi \circ g$.

In the first game, Adversary can earn at least $d+1$ coins. By the construction of the strategy, each time Adversary earns a coin, Delayer also earns a coin. Hence, Delayer, using the described strategy, can earn at least $d+1$ coins. And by Lemma 4.2, this contradicts the assumption of the theorem. □

5 Lower bound for depth-$\Omega(n \log n)$ Res($\oplus$)

In this section, we describe how to prove an exponential lower for depth-$\Omega(n \log n)$ Res($\oplus$). In Subsection 5.1, we present the key lemma utilizing the notion of amortized closure that we will use to improve the result by [3]. In Subsections 5.2 and 5.3, we describe how to modify the proof by [3] to improve it using the key lemma.

5.1 Key lemma

Lemma 5.1. Let Φ and Ψ be two linear systems in variables $X = \{x_{i,j} \mid i \in [m], j \in [\ell]\}$. Let π be a partial assignment defined on $\{x_{i,j} \mid i \in [\mathrm{Cl}(L(\Phi))], j \in [\ell]\}$. Let Σ consist of all solutions σ of Φ such that σ extends π. Assume that $\Sigma \neq \emptyset$. Let τ be a random element of Σ. Then $\Pr[\tau \text{ satisfies } \Psi] \leq 2^{|\widetilde{\mathrm{Cl}}(L(\Phi))| - |\widetilde{\mathrm{Cl}}(L(\Psi))|}$.

Proof. By the definition of the closure, the set of linear form $L(\Phi|_\pi)$ is safe. Hence, by Theorem 2.1, there exists a basis in the set of columns of the matrix of $\Phi|_\pi$ such that for every block, the basis contains at most one column corresponding to this block. Let $Z \subseteq X$ be the set of variables corresponding to the basis elements. Since $\Sigma \neq \emptyset$, the system $\Phi|_\pi$ is satisfiable. Hence, the system $\Phi|_\pi$ can be equivalently rewritten as the system of $|Z|$ equations, each of them linearly expresses the corresponding variable from Z from variables $X \setminus Z \setminus \mathrm{Dom}(\pi)$. Let us denote this representation by Φ'_π.

A random solution of $\Phi|_\pi$ has the following structure: we take at random values of all variables $X \setminus Z \setminus \mathrm{Dom}(\pi)$, and, then the values of variables from Z are uniquely determined by the system Φ'_π. Thus, the following statement holds.

Claim 5.2. Let H be a satisfiable linear system in the variables $X \setminus Z \setminus \mathrm{Dom}(\pi)$. Then $\Pr[\tau \text{ satisfies } H] = 2^{-\mathrm{rk}(H)}$.

Let Π be the following linear system: $\bigwedge_{j \in [\ell], i \in [\mathrm{Cl}(L(\Phi))]} x_{i,j} = \pi(x_{i,j})$.

Notice that the linear system $\Phi \wedge \Pi$ is semantically equivalent to the system $\Phi|_\pi \wedge \Pi$ that is equivalent to the system $\Phi'_\pi \wedge \Pi$.

The system $\Pi \wedge \Phi'_\pi$ sets variables from $\mathrm{Dom}(\pi)$ to constants and expresses the variables from Z from the variables $X \setminus Z \setminus \mathrm{Dom}(\pi)$. Let Ψ' denote the linear system Ψ where we substitute for all variables from $\mathrm{Dom}(\pi) \cup Z$ their expressions given by the system $\Pi \wedge \Phi'_\pi$. So Ψ' is a linear system in the variables $X \setminus Z \setminus \mathrm{Dom}(\pi)$.

Let Ψ'' be the maximal set of linearly independent equations from Ψ'.

$$\Pr[\tau \text{ satisfies } \Psi] = \Pr[\tau \text{ satisfies } \Psi \wedge \Pi \wedge \Phi'_\pi] = \Pr[\tau \text{ satisfies } \Psi' \wedge \Pi \wedge \Phi'_\pi] = \Pr[\tau \text{ satisfies } \Psi'' \wedge \Pi \wedge \Phi'_\pi] = \Pr[\tau \text{ satisfies } \Psi''] \overset{\text{(Claim 5.2)}}{=} 2^{-\mathrm{rk}(\Psi'')}$$

$$|\widetilde{\mathrm{Cl}}(L(\Psi))| \overset{\text{(Cor. 2.19)}}{\leq} |\widetilde{\mathrm{Cl}}(L(\Pi \wedge \Phi'_\pi \wedge \Psi))| \overset{\text{(Lem. 2.11)}}{=} |\widetilde{\mathrm{Cl}}(L(\Pi \wedge \Phi'_\pi \wedge \Psi''))| \overset{\text{(Cor. 2.19)}}{\leq}$$

$$|\widetilde{\mathrm{Cl}}(L(\Pi \wedge \Phi \wedge \Psi''))| \overset{\text{(Lem. 2.14)}}{=} |\,\mathrm{Cl}(L(\Phi))| + |\widetilde{\mathrm{Cl}}\,(L(\Pi[\setminus \mathrm{Cl}(L(\Phi))]) \cup L(\Phi[\setminus \mathrm{Cl}(L(\Phi))]) \cup L(\Psi''[\setminus \mathrm{Cl}(L(\Phi))]))\,| =$$

$$|\,\mathrm{Cl}(L(\Phi))| + |\widetilde{\mathrm{Cl}}(L(\Phi[\setminus \mathrm{Cl}(L(\Phi))]) \cup L(\Psi''))| \overset{\text{(Th. 2.18)}}{\leq}$$

$$|\,\mathrm{Cl}(L(\Phi))| + |\widetilde{\mathrm{Cl}}(L(\Phi)[\setminus \mathrm{Cl}(L(\Phi))])| + \mathrm{rk}(\Psi'') \overset{\text{(Lem. 2.14)}}{=} |\widetilde{\mathrm{Cl}}(L(\Phi))| + \mathrm{rk}(\Psi'').$$

So we get, $\Pr[\tau \text{ satisfies } \Psi] = 2^{-\mathrm{rk}(\Psi'')} \leq 2^{|\widetilde{\mathrm{Cl}}(L(\Phi))| - |\widetilde{\mathrm{Cl}}(L(\Psi))|}$.

□

5.2 Random-walk theorem

The main technical tool used in [3] in proving the lower bound for bounded-depth Res($\oplus$) is the random-walk theorem.

Let φ be a CNF formula and $\mathcal{A}$ be a set consisting of partial assignments for variables of φ. We assume that $\mathcal{A}$ has two properties:

- $\mathcal{A}$ is closed under restrictions: if for every $\rho \in \mathcal{A}$ for every $\sigma \subseteq \rho$, $\sigma \in \mathcal{A}$.
- For every $\sigma \in \mathcal{A}$, σ does not falsify any clause of φ.

$(\varphi, \mathcal{A})$-games of Prover and Delayer with starting position $\rho_0 \in \mathcal{A}$. In this game, two players, Prover and Delayer, maintain a partial assignment ρ for variables of φ that initially equals ρ_0. On every move, Prover chooses a variable x, and Delayer has two options:

- Delayer can earn a *white* coin and reports $*$. Then, Prover chooses a Boolean value a of x.
- Delayer can earn a *white* coin and pay a *black* coin to choose a Boolean value a of x by himself.

The current assignment ρ is updated: $\rho := \rho \cup \{x := a\}$. The game ends when $\rho \notin \mathcal{A}$.

Delayer's strategy is called *linearly described* if Delayer can see only the set of requested variables and he does not know the values of the variables chosen by Prover and even by himself before. When he chooses a value by himself, he chooses a $\mathbb{F}_2$-affine function from the values of previous variables, and the result of this function is used as a value chosen by Delayer. For a more detailed definition of linearly described strategies, we refer to [3].

Theorem 5.3 (Theorem 4.3 from [3])**.** Let φ be an unsatisfiable CNF formula. Let $\mathcal{A}$ be a set of partial assignments for $\mathrm{Vars}(\varphi)$ such that $\mathcal{A}$ is closed under restrictions and for any $\sigma \in \mathcal{A}$, σ does not falsify any clause of φ. Assume that in the $(\varphi, \mathcal{A})$-game, Delayer has a linearly described strategy with start position $\rho_0 \in \mathcal{A}$ that guarantees him to earn w white coins while paying at most c black coins. Let $g\colon \{0,1\}^\ell \to \{0,1\}$ be a 2-stifling gadget. Consider a Res($\oplus$) refutation of $\varphi \circ g$.Let C_0 be a linear clause from this refutation. Assume that $\mathrm{Cl}(L(C_0)) = \mathrm{Dom}(\rho_0)$ and there is a solution τ of $\neg C_0$ such that $\hat{\tau}$ extends ρ_0. Let Σ be the set of all full assigmnets π such that π satisfies $\neg C_0$ and $\hat{\pi}$ extends ρ_0. Let t be integer number such that $t \leq w - |\widetilde{\mathrm{Cl}}(L(C_0))| + |\rho_0|$. Consider a random full assignment $\sigma \in \Sigma$ and make t steps in the refutation from C_0 according to σ: each time we go from a linear clause to its premise falsifying by σ, and we count only applications of resolution rules (if we reach an initial clause earlier than in t steps, we stay there). Assume that we stop in a node labeled with a linear clause C. Then $\hat{\sigma}|_{\mathrm{Cl}(L(C))} \in \mathcal{A}$ with probability at least $2^{-c(\ell-1)}$.

The only difference between Theorem 5.3 and Theorem 4.3 from [3] is that the inequality $t \le w - |\widetilde{\mathrm{Cl}}(L(C_0))| + |\rho_0|$ that was slightly stronger $t \le w - |\mathrm{rk}(\neg C_0)| + |\rho_0|$ in Theorem 4.3 from [3]. It is easy to see that the proof from [3] works with the weaker inequality as well. This is because this inequality was only used to show that if a linear system F has type $\neg C_0 \wedge H$, where H consists of at most t equations, then $|\,\mathrm{Cl}(L(F))| \le w + |\rho_0|$. Using the weaker inequality $|\,\mathrm{Cl}(L(F))|$ can be estimated as follows: $|\,\mathrm{Cl}(L(F))| \overset{\text{(Lem. 2.15)}}{\le} |\widetilde{\mathrm{Cl}}(L(F))| \overset{\text{(Th. 2.18)}}{\le} |\widetilde{\mathrm{Cl}}(L(C_0)| + t \le w + |\rho_0|$.

5.3 Size vs depth tradeoff

Theorem 5.4. [cf. Theorem 8.1 from [3]] Let φ be an unsatisfiable CNF formula. Let $\mathcal{A}$ be a set of partial assignments for $\mathrm{Vars}(\varphi)$ such that for any $\sigma \in \mathcal{A}$, σ does not falsify any clause of φ and $\mathcal{A}$ is closed under restrictions (i.e., if $\rho \in \mathcal{A}$ and $\tau \subseteq \rho$, then $\tau \in \mathcal{A}$). Assume that there are integers t and c such that for every $\rho \in \mathcal{A}$ such that $|\rho| < t$, in the $(\varphi, \mathcal{A})$-game with start position ρ there is a linearly described strategy of Delayer that guarantees him to earn at least $t - |\rho|$ white coins while paying at most c black coins. Let $g\colon \{0,1\}^\ell \to \{0,1\}$ be a 2-stifling gadget. Then any $\mathrm{Res}(\oplus)$ refutation of $\varphi \circ g$ has either size at least 2^c or depth at least $\frac{t^2}{4c\ell}$.

Proof. We say that a linear clause C in lifted variables is $\mathcal{A}$-good if there is a solution τ of $\neg C$ such that $\hat{\tau}|_{\mathrm{Cl}(L(C))} \in \mathcal{A}$.

Consider a $\mathrm{Res}(\oplus)$ refutation of $\varphi \circ g$ and denote is by Π.

Claim 5.5. Assume that Π contains an $\mathcal{A}$-good linear clause C_0 such that $|\widetilde{\mathrm{Cl}}(L(C_0))| \le r$, where $r < t$. Let $S_{t-r}(C_0)$ denote the set of all $\mathcal{A}$-good clauses C such that there is a path from C_0 to C of length $t-r$ in the branching program associated with Π. Assume that for every $C \in S_{t-r}(C_0)$, $|\widetilde{\mathrm{Cl}}(L(C))| \ge r + c\ell$ holds. Then, the size of the refutation Π is at least 2^c.

Proof. Since C_0 is $\mathcal{A}$-good, there is a solution τ_0 of $\neg C_0$ such that $\hat{\tau}_0|_{\mathrm{Cl}(L(C))} \in \mathcal{A}$. Let us denote $\rho_0 := \hat{\tau}_0|_{\mathrm{Cl}(L(C_0))}$. Then $|\rho_0| = |\,\mathrm{Cl}(L(C_0))| \le |\widetilde{\mathrm{Cl}}(L(C_0))| \le r$. By the conditions of the theorem, there is a linearly described strategy of Delayer in the $(\varphi, \mathcal{A})$-game with starting position ρ_0 that guarantees him to earn $t - |\rho_0|$ white coins while paying at most c black coins.

Let Σ be the set of all assignments π such that π satisfies $\neg C_0$ and $\hat{\pi}|_{\mathrm{Cl}(L(C_0))} = \rho_0$. Since $\tau_0 \in \Sigma$, $\Sigma \neq \emptyset$.

Consider a random assignment $\sigma \in \Sigma$ and make $t - r$ steps in the linear branching program from C_0 according to σ. Notice that $t - r \le (t - |\rho_0|) + |\rho_0| - |\widetilde{\mathrm{Cl}}(L(C_0))|$. Let C be the linear clause at the end of the path. By Theorem 5.3, with probability at least $2^{-(\ell-1)c}$, C is $\mathcal{A}$-good. By Lemma 3.2, C is not a clause of $\phi \circ g$, hence, $C \in S_{t-r}(C_0)$. Thus, $|\widetilde{\mathrm{Cl}}(L(C))| \ge r + c\ell$.

If Ψ is a satisfiable linear system such that $|\widetilde{\mathrm{Cl}}(\Psi)| \ge r + c\ell$, then by Lemma 5.1, $\Pr[\sigma \text{ satisfies } \Psi] \le 2^{-c\ell}$. Hence, the refutation contains at least 2^c clauses C such that $|\widetilde{\mathrm{Cl}}(L(C)) \ge r + c\ell$. □

Let D_0 denote the empty clause from Π. If for every $\mathcal{A}$-good clause C such that there is a path from D_0 to C of length t, $|\widetilde{\mathrm{Cl}}(L(C))| \ge c\ell$, then by Claim 5.5, the size of the refutation Π is at least 2^c. Otherwise, there is an $\mathcal{A}$-good clause D_1 such that there is a path from D_0 to D_1 of length t and $|\widetilde{\mathrm{Cl}}(L(D_1))| \le c\ell$. Let $k := \lceil \frac{t}{2c\ell} \rceil$, then $c\ell(k-1) \le t/2$. We repeat the same reasoning $k-1$ more times for all i from 1 to $k-1$ maintaining invariant $|\widetilde{\mathrm{Cl}}(L(D_i))| \le c\ell i$: if for every $\mathcal{A}$-good clause C such that there is a path from D_i to C of length $t - c\ell i$, $|\widetilde{\mathrm{Cl}}(L(C))| \ge c\ell(i+1)$, then by Claim 5.5, the size of Π is at least 2^c. Otherwise, there is an $\mathcal{A}$-good clause D_{i+1} such that there is a path from D_i to D_{i+1} of length $t - c\ell i$ and $|\widetilde{\mathrm{Cl}}(L(D_{i+1}))| \le c\ell(i+1)$.

So we get that either the size of refutation is at least 2^c or depth is at least the length of the path from D_0 to D_1, from D_1 to D_2, etc, from D_{k-1} to D_k which is at least $kt/2 \ge \frac{t^2}{4cl}$. □

Corollary 5.6 (cf. Corollary 8.3 from [3])**.** Let $\mathrm{T}(G,c)$ be an unsatisfiable Tseitin formula based on a spectral (n,d,α)-expander. Then, any $\mathrm{Res}(\oplus)$ refutation of $\mathrm{T}(G,c) \circ Maj_5$ has either size at least 2^n or depth at least $\frac{n}{20} \cdot \left\lfloor d \cdot \frac{(1-\alpha)}{8} \right\rfloor^2$.

In particular, if $d = \Theta(\log n)$ and $\alpha < 1$ is a constant, then $\mathrm{T}(G,c) \circ Maj_5$ is a formula with $m = 5dn/2$ variables and of size $\mathrm{poly}(m)$. And any $\mathrm{Res}(\oplus)$ refutation of $\mathrm{T}(G,c) \circ Maj_5$ has either size at least $2^{\Omega(m/\log m)}$ or depth at least $\Omega(m \log m)$.

Proof. The proof repeats the proof of Corollary 8.3 from [3] where the application of Theorem 8.1 from [3] is substituted by the application of Theorem 5.4. □

Acknowledgments. The authors thank Yaroslav Alekseev and Alexander Knop for fruitful discussions.

References

[1] M. Ajtai. $\sum_1^1$-formulae on finite structures. *Annals of Pure and Applied Logic*, 24(1):1–48, 1983.

[2] Miklós Ajtai. The complexity of the pigeonhole principle. *Combinatorica*, 14(4):417–433, 1994.

[3] Yaroslav Alekseev and Dmitry Itsykson. Lifting to bounded-depth and regular resolutions over parities via games. *Electron. Colloquium Comput. Complex.*, TR24-128, Revision 1, 2024. To appear in proceedings of STOC 2025.

[4] Albert Atserias and Víctor Dalmau. A combinatorial characterization of resolution width. *Journal of Computer and System Sciences*, 74(3):323–334, 2008. Computational Complexity 2003.

[5] Paul Beame and Sajin Koroth. On Disperser/Lifting Properties of the Index and Inner-Product Functions. In Yael Tauman Kalai, editor, *14th Innovations in Theoretical Computer Science Conference (ITCS 2023)*, volume 251 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 14:1–14:17, Dagstuhl, Germany, 2023. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

[6] Christoph Berkholz. On the complexity of finding narrow proofs. In *53rd Annual IEEE Symposium on Foundations of Computer Science, FOCS 2012, New Brunswick, NJ, USA, October 20-23, 2012*, pages 351–360. IEEE Computer Society, 2012.

[7] 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.

[8] Sam Buss and Neil Thapen. A simple supercritical tradeoff between size and height in resolution. *Electron. Colloquium Comput. Complex.*, TR24-001, 2024.

[9] Farzan Byramji and Russell Impagliazzo. Lifting to randomized parity decision trees. *Electron. Colloquium Comput. Complex.*, TR24-202, 2024.

[10] Arkadev Chattopadhyay and Pavel Dvorak. Super-critical trade-offs in resolution over parities via lifting. *Electron. Colloquium Comput. Complex.*, TR24-132, 2024.

[11] Arkadev Chattopadhyay, Nikhil S. Mande, Swagato Sanyal, and Suhail Sherif. Lifting to parity decision trees via stifling. In Yael Tauman Kalai, editor, *14th Innovations in Theoretical Computer Science Conference, ITCS 2023, January 10-13, 2023, MIT, Cambridge, Massachusetts, USA*, volume 251 of *LIPIcs*, pages 33:1–33:20. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2023.

[12] Stephen A. Cook and Robert A. Reckhow. The relative efficiency of propositional proof systems. *The Journal of Symbolic Logic*, 44(1):36–50, March 1979.

[13] Susanna F. de Rezende, Noah Fleming, Duri Andrea Janett, Jakob Nordström, and Shuo Pang. Truly supercritical trade-offs for resolution, cutting planes, monotone circuits, and weisfeiler-leman. *Electron. Colloquium Comput. Complex.*, TR24-185, 2024.

[14] Klim Efremenko, Michal Garlík, and Dmitry Itsykson. Lower bounds for regular resolution over parities. In Bojan Mohar, Igor Shinkar, and Ryan O'Donnell, editors, *Proceedings of the 56th Annual ACM Symposium on Theory of Computing, STOC 2024, Vancouver, BC, Canada, June 24-28, 2024*, pages 640–651. ACM, 2024. The full version is available as ECCC technical report TR23-187.

[15] Noah Fleming, Toniann Pitassi, and Robert Robere. Extremely deep proofs. In Mark Braverman, editor, *13th Innovations in Theoretical Computer Science Conference, ITCS 2022, January 31 - February 3, 2022, Berkeley, CA, USA*, volume 215 of *LIPIcs*, pages 70:1–70:23. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022.

[16] Merrick Furst, James B. Saxe, and Michael Sipser. Parity, circuits, and the polynomial-time hierarchy. *22nd Annual Symposium on Foundations of Computer Science (sfcs 1981)*, pages 260 – 270, 1981.

[17] Mika Göös, Gilbert Maystre, Kilian Risse, and Dmitry Sokolov. Supercritical tradeoffs for monotone circuits. *Electron. Colloquium Comput. Complex.*, TR24-186, 2024.

[18] Svyatoslav Gryaznov, Sergei Ovcharov, and Artur Riazanov. Resolution over linear equations: Combinatorial games for tree-like size and space. *ACM Trans. Comput. Theory*, jul 2024. Just Accepted.

[19] Dmitry Itsykson and Dmitry Sokolov. Resolution over linear equations modulo two. *Ann. Pure Appl. Log.*, 171(1), 2020.

[20] Vladimir Podolskii and Alexander Shekhovtsov. Randomized lifting to semi-structured communication complexity via linear diversity. *Electron. Colloquium Comput. Complex.*, TR24-199, 2024.

[21] A. A. Razborov. "lower bounds on the size of bounded depth circuits over a complete basis with logical addition. *Mat. Zametki*, 41:598–607, 1987.

[22] Alexander A. Razborov. A new kind of tradeoffs in propositional proof complexity. *J. ACM*, 63(2):16:1–16:14, 2016.

[23] Roman Smolensky. Algebraic methods in the theory of lower bounds for boolean circuit complexity. In *Proceedings of the 19th Annual ACM Symposium on Theory of Computing, 1987, New York, New York, USA*, pages 77–82, 1987.

[24] D.J.A. Welsh. Generalized versions of Hall's theorem. *Journal of Combinatorial Theory, Series B*, 10(2):95–101, 1971.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il