



# Supercritical Size-Width Tree-Like Resolution Trade-Offs for Graph Isomorphism

Christoph Berkholz  

Technische Universität Ilmenau, Germany

Moritz Lichter  

RWTH Aachen University, Germany

Harry Vinall-Smeeth  

Technische Universität Ilmenau, Germany

---

## Abstract

We study the refutation complexity of graph isomorphism in the tree-like resolution calculus. Torán and Wörz [42] showed that there is a resolution refutation of *narrow width*  $k$  for two graphs if and only if they can be distinguished in  $(k + 1)$ -variable first-order logic ( $\text{FO}^{k+1}$ ). While DAG-like narrow width  $k$  resolution refutations have size at most  $n^k$ , tree-like refutations may be much larger. We show that there are graphs of order  $n$ , whose isomorphism can be refuted in narrow width  $k$  but only in tree-like size  $2^{\Omega(n^{k/2})}$ . This is a *supercritical* trade-off where bounding one parameter (the narrow width) causes the other parameter (the size) to grow above its worst case. The size lower bound is super-exponential in the formula size and improves a related supercritical trade-off by Razborov [35]. To prove our result, we develop a new variant of the  $k$ -pebble EF-game for  $\text{FO}^k$  to reason about tree-like refutation size in a similar way as the Prover-Delayer games in proof complexity. We analyze this game on the compressed CFI graphs introduced by Grohe, Lichter, Neuen, and Schweitzer [25]. Using a recent improved *robust* compressed CFI construction of de Rezende, Fleming, Janett, Nordström, and Pang [19], we obtain a similar bound for *width*  $k$  (instead of the stronger but less common *narrow width*) and make the result more robust.

**2012 ACM Subject Classification** Theory of computation  $\rightarrow$  Proof complexity

**Keywords and phrases** Proof complexity, Resolution, Width, Tree-like size, Supercritical trade-off, Lower bound, Finite model theory, CFI graphs

**Digital Object Identifier** 10.4230/LIPIcs.MFCS.2025.18

**Related Version** *Full Version:* <https://doi.org/10.48550/arXiv.2407.17947> [14]

**Funding** *Christoph Berkholz and Harry Vinall-Smeeth:* Funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) - project number 414325841.

*Moritz Lichter:* Funded by the European Union (ERC, SymSim, 101054974). Views and opinions expressed are those of the author(s) and do not necessarily reflect those of the European Union or the ERC. Neither the European Union nor the granting authority can be held responsible for them.

## 1 Introduction

A common theme in proof complexity is the difficulty of refuting a given CNF formula in a particular proof system. There are many variants of this problem depending on the proof system and the notion of difficulty under investigation. We focus on (variants of) resolution, perhaps the most-studied proof system. Here typical measures of difficulty include the minimum width, depth, space, and (tree-like) size over all refutations of the input formula.

By analyzing the proof complexity of formulas that encode natural combinatorial problems, we also gain insights about the inherent complexity of these problems. In this paper, we focus on the graph isomorphism problem, the complexity status of which is still unknown [30]. On the one hand, Babai [4] showed in a breakthrough result that graph isomorphism is



© Christoph Berkholz, Moritz Lichter, and Harry Vinall-Smeeth;  
licensed under Creative Commons License CC-BY 4.0

50th International Symposium on Mathematical Foundations of Computer Science (MFCS 2025).

Editors: Paweł Gawrychowski, Filip Mazowiecki, and Michał Skrzypczak; Article No. 18; pp. 18:1–18:19



Leibniz International Proceedings in Informatics

LIPICs Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

solvable in quasi-polynomial time (see also [26]), which makes it a rare natural candidate for a problem that might be neither NP-complete nor polynomial-time solvable. On the other hand, only relatively weak complexity lower bounds are known [39]. This motivates the study of the hardness of graph isomorphism from other perspectives, such as proof complexity.

In this direction, Torán [40] showed that graph isomorphism is hard for resolution: There are non-isomorphic graphs on  $n$  vertices such that every resolution refutation certifying non-isomorphism has size  $2^{\Omega(n)}$ . Graph isomorphism and the Weisfeiler-Leman algorithm – a well-known algorithm in the context of graph isomorphism – have both been studied in different proof systems, including Sherali-Adams [3, 28], (extended) polynomial calculus [12, 13, 33], sum-of-squares [32], cutting planes [41], and in extensions of resolution with different symmetry rules [36, 41]. We are interested in “tree-like” refutations, which intuitively means that whenever we want to use a clause in a proof step we have to re-derive it. Tree-like resolution corresponds exactly to Boolean decision trees and is closely related to the DPLL algorithm. We will be concerned with “trade-offs” between the *width* – i.e. the maximum number of literals occurring in any clause – and the *size* of tree-like refutations.

Studying trade-offs – i.e. situations where in order for a refutation to be “easy” with respect to one measure, it has to be “hard” with respect to another – is a prominent theme in proof complexity. For example, there are trade-offs between size and space [5, 9], between width and depth, and between width and size [11, 16, 38]. There are two senses in which a trade-off can be particularly strong. Firstly, a trade-off is *robust* if it not only shows that one measure  $A$  has to be large when another measure  $B$  is small, but also that  $B$  can be increased over some (hopefully) wide range without that the bound on  $A$  decreasing. Secondly, a trade-off is *supercritical* if, in case we restrict  $B$ , the measure  $A$  must be larger than the general upper bound on  $A$  (over all formulas) in the case that  $B$  is not restricted.

In fact, one of the first supercritical trade-offs for resolution – proved by Razborov [35] – concerns tree-like size and width: For every  $k = k(n)$ , there are  $k$ -CNF formulas over  $n$  variables that can be refuted in width  $O(k)$ , but such that every tree-like refutation of minimum width requires depth  $n^{\Omega(k)}$  and size  $2^{n^{\Omega(k)}}$ . When the width is unrestricted then, for each unsatisfiable formula over  $n$  variables, there is a tree-like refutation of size at most  $2^n$ . Hence, when bounding the width, the tree-like refutation size increases beyond its worst-case and gets super-exponential in the variable number. This trade-off is not only supercritical but also robust: The lower bounds also hold for width- $k'$  refutations for larger  $k' < n^{1-\varepsilon}/k$ .

One drawback of Razborov’s trade-off is that it is not supercritical if we measure size and width with respect to the formula size rather than the number of variables. While the  $k$ -CNF formula of Razborov uses  $n$  variables, it has size about  $N := n^{\Theta(k)}$ . Thus in terms of the formula size  $N$ , the bound on tree-like resolution size is roughly  $2^N$ . Our first main result concerns *narrow resolution* [21] which extends resolution by an additional rule avoiding side effects caused by large width clauses in the input formula. It is closely related to first-order logic: The width and the depth of *narrow* graph isomorphism refutations correspond to the number of variables and the quantifier depth respectively of first-order formulas distinguishing graphs [41]. We show a supercritical trade-off with respect to formula size between width and size for tree-like narrow resolution applied to graph isomorphism formulas.

► **Theorem 1.** *For all integers  $k \geq 3$  and  $n \in \mathbb{N}$ , there are two non-isomorphic colored graphs  $\mathcal{G}$  and  $\mathcal{H}$  of order  $\Theta(n)$  and color class size 16 such that*

1. *there is a width- $k$  narrow resolution refutation of  $\text{ISO}(\mathcal{G}, \mathcal{H})$ , and*
2. *every width- $k$  tree-like narrow resolution refutation of  $\text{ISO}(\mathcal{G}, \mathcal{H})$  has size  $2^{\Omega(n^{k/2})}$ .*

Narrow resolution is stronger than resolution; in particular, the minimal width of a narrow resolution refutation is at most the minimal width of a (plain) resolution refutation. The formula  $\text{ISO}(\mathcal{G}, \mathcal{H})$ , which encodes graph isomorphism of  $\mathcal{G}$  and  $\mathcal{H}$ , has size  $O(n^4)$  for graphs

of order  $n$ . Thus, Theorem 1 indeed yields a supercritical trade-off between width and tree-like size for narrow resolution *with respect to the formula size*. Building upon very recent work due to de Rezende, Fleming, Janett, Nordström, and Pang [19], who provided a not only supercritical but also robust variant of the trade-off in [25], we can show that Theorem 1 also applies to usual (non-narrow) resolution and the trade-off can be made somewhat robust.

► **Theorem 2.** *For all integers  $k \geq 3$ ,  $1 \leq t \leq \frac{2}{5}k - 1$ , and  $n \in \mathbb{N}$ , there are two colored graphs  $\mathcal{G}$  and  $\mathcal{H}$  of order  $\Theta(n)$  and color class size 16 such that*

1. *there is a width- $(k + 16)$  resolution refutation of  $\text{ISO}(\mathcal{G}, \mathcal{H})$ , and*
2. *every width- $(k + t - 1)$  tree-like resolution refutation of  $\text{ISO}(\mathcal{G}, \mathcal{H})$  has size  $2^{\Omega(n^{k/(t+1)})}$ .*

With this theorem, we address Razborov’s call for supercritical bounds in terms of formula size [35]. Moreover, our trade-off applies to formulas encoding a natural combinatorial problem and is somewhat robust for  $t > 16$  and sufficiently large  $k$ . Since the maximum size of a width  $k$  tree-like refutation is  $2^{O(n^k)}$ , our lower bounds are almost optimal in this range. Our proof utilizes machinery from *finite model theory*: We introduce a new Ehrenfeucht–Fraïssé style game played on two graphs and show that lower bounds for this game imply lower bounds on the tree-like size of narrow resolution refutations of the corresponding graph isomorphism formula.

**Razborov’s Trade-Off and Weisfeiler-Leman.** To prove his trade-off, Razborov used a compression technique, known as *hardness condensation* [15, 35], that is based on *xorification* and variable reuse and converts large but hard formulas into smaller ones that are still hard. Xorification is a well-known technique which replaces every variable in a formula by an XOR of fresh variables. Xorification, or variable substitution in general, has found many applications in proof complexity (see e.g. [6, 8–10]). Razborov’s compression technique was adapted to the Weisfeiler-Leman (WL) algorithm – an important algorithm in the field of graph isomorphism [4, 23, 27]. The algorithm, parameterized by a dimension  $k$ , is a graph isomorphism heuristic, that is, whenever it distinguishes two graphs they are not isomorphic but, for every  $k$ , it fails to distinguish all non-isomorphic graphs [17]. Of particular interest is the number of iterations needed by the  $k$ -dimensional WL-algorithm to distinguish two graphs; this almost corresponds to the quantifier depth needed in  $(k + 1)$ -variable first-order logic with counting to distinguish them. Berkholz and Nordström [15] adapted Razborov’s compression technique to construct  $k$ -ary relational structures for which the  $k$ -dimensional WL-algorithm requires  $n^{\Omega(k/\log k)}$  iterations; here the best known upper bound is  $O(n^{k-1}/\log n)$  [24]. From the perspective of trade-offs, first-order logic (without a bound on the variables) requires at most quantifier depth  $n$  to distinguish all non-isomorphic graphs, which means this trade-off is also supercritical. The lower bound was recently improved to  $n^{\Omega(k)}$  [24].

The trade-offs described above have a common drawback: They are supercritical with respect to the number of variables and the number of vertices of the structures, respectively, but not with respect to the formula size or the size of the structure (in terms of the number of tuples in the  $k$ -ary relations). The common reason is that hardness condensation turns 3-CNF formulas into  $k$ -CNF formulas and 3-ary structures into  $k$ -ary ones. But recently, Grohe, Lichter, Neuen, and Schweitzer [25] introduced a powerful new compression technique for the so-called Cai-Fürer-Immerman (CFI) graphs [17] to prove a lower bound of  $\Omega(n^{k/2})$  for the iteration number of the  $k$ -dimensional WL-algorithm on graphs of order  $n$ . The bound not only improves the known ones, it is also a bound on graphs and, as graphs have size  $O(n^2)$ , the lower bound is supercritical with respect to the structure size. The inspiration for this paper was to see if this new technique yields analogous proof complexity results.

**Our Techniques and New Games.** Tree-like refutations can be (almost) exponentially larger than their non-tree-like counterparts [7]. The usual tool to prove width- $k$  tree-like size lower bounds is the Prover-Delayer game [34]. Prover maintains a partial assignment to at most  $k$  variables. In each round, Prover forgets one variable and asks Delayer for an assignment to another one. Delayer can either give such an assignment or allow Prover to set it; in the latter case Delayer scores a point. Prover wants to find an inconsistent partial assignment and Delayer wants to gain as many points as possible. If Delayer has a strategy to score  $p$  points, then every width- $k$  tree-like refutation has size at least  $2^p$ . On xorified formulas, where each variable  $v$  is replaced with an XOR of  $v_0$  and  $v_1$ , Delayer can always gain a point when Prover queries  $v_0$  or  $v_1$  so long as the other one is not already assigned. This leads to tree-like size lower bounds exponential in the depth of a refutation [43].

However, the xorification of a graph isomorphism formula is not necessarily a graph isomorphism formula. Since we are interested in such formulas, our idea is to instead apply xorification on the level of graphs. We show that twins in a graph, i.e., vertices with the same neighborhood, can play the role of XORs in a formula: When we isomorphically map a pair of twins in one graph to a pair of twins in the other graph, the image of the first twin can be chosen arbitrary. We consider *twinned graphs*, where every vertex is replaced by a pair of twins. Ultimately, we want to show that the narrow tree-like refutation size of a twinned graph is exponential in the refutation depth of the original graph. Unfortunately, there seems to be no generic argument for this. To show that this is indeed the case for the graphs we consider, we introduce a variant of the Prover-Delayer game suited for narrow resolution. Then we use techniques from finite model theory to show lower bounds for this game. For other examples of finite-model-theoretic techniques in proof complexity see, e.g. [1, 11, 22].

We cannot reuse the correspondence between width- $(k-1)$  narrow resolution and  $k$ -variable first-order logic [42], or equivalently the  $k$ -pebble game [29], because we care about tree-like size, not only about width and depth. The issue is that assigning a variable to one or to zero in graph isomorphism formulas is not symmetric: In terms of isomorphisms, fixing the image of a vertex is usually more restrictive than forbidding a single vertex as the image of another vertex. We introduce a new pebble game, called the  *$k$ -pebble game with blocking*, which captures this difference between one and zero assignments. Round lower bounds in the pebble game with blocking imply exponential size lower bounds for tree-like resolution.

Another game is involved in this lower bound. The hardness of uncompressed CFI graphs for  $k$ -variable first-order logic is captured by the  $k$ -Cops and Robber game [25, 37], which forgets about the CFI construction and instead considers the simpler underlying *base graphs*. For compressed CFI graphs, this game was modified to the compressed  $k$ -Cops and Robber game [25]. To obtain lower bounds for the  $k$ -pebble game with blocking, we have to introduce a blocking mechanism to the compressed  $k$ -Cops and Robber game. Via all these games, we obtain the  $2^{\Omega(n^{k/2})}$  narrow width- $k$  tree-like size lower bound in Theorem 1.

**From Narrow to Plain Resolution.** We lift Theorem 1 to (non-narrow) resolution. Since lower bounds for narrow resolution imply lower bounds for resolution, transferring the lower bounds is trivial. But it is unclear whether the relevant isomorphism formula can be refuted in (non-narrow) width  $k$ . By increasing the width by the maximal color class size of these graphs (which is 16), we can simulate the narrow resolution refutation by a plain resolution refutation. But now the lower bound from Theorem 1 does not apply anymore. At this point, the aforementioned result from [19] comes to hand: The compression of the CFI graphs get modified to obtain, for every fixed  $t < k$ , graphs whose isomorphism formula can be refuted in narrow width  $k$  but every narrow width  $k+t$  refutation has depth at least  $\Omega(n^{k/(t+1)})$ . So the

lower bound is robust within the range from  $k$  to  $k + t - 1$ . This construction can be seen as an interpolation between the original compression [25] with round lower bound  $\Omega(n^{k/2})$  and the linear round lower bound  $\Omega(n)$  by Fürer [20]; both appear as special cases for  $t = 1$  and  $t = k$ . Our approach with twinned graphs also applies to the improved construction implying a narrow width- $(k + t)$  tree-like size lower bound of  $2^{\Omega(n^{k/(t-1)})}$ , but we need to restrict the range of  $t$  even further. For  $k$  large enough and  $t > 16$  we can actually refute isomorphism of the graphs in (non-narrow) width  $k + t$  and finally obtain a supercritical trade-off between width and tree-like size for resolution with respect to formula size (Theorem 2).

**Further Related Work.** How the robust compressed CFI construction [19] yields a supercritical width-depth trade-off for resolution was presented at the Oberwolfach workshop *Proof Complexity and Beyond* [2]. The resulting preprint [19] also contains a trade-off for tree-like resolution. A key difference is that our trade-off applies to graph-isomorphism formulas. Also, different techniques are used. We cannot apply hardness condensation techniques to graph isomorphism formulas but apply a form of xorification on the level of graphs and analyze them using model theoretic techniques. In contrast, the trade-off of [19] is obtained via xorification; the parameters obtained are within a constant factor of one-another.

## 2 Preliminaries

**Graphs.** An (*undirected*) graph  $\mathcal{G}$  is a tuple  $(V, E)$  where  $V$  is a finite set of *vertices* and  $E \subseteq \binom{V}{2}$  is a set of *edges*. The vertex set of  $\mathcal{G}$  is denoted by  $V_{\mathcal{G}}$  and the edge set of  $\mathcal{G}$  by  $E_{\mathcal{G}}$ . For  $W \subseteq V_{\mathcal{G}}$ , the *subgraph of  $\mathcal{G}$  induced by  $W$*  is denoted by  $\mathcal{G}[W]$ . The *distance* between two vertices  $u, v \in V_{\mathcal{G}}$  is the number of edges in a shortest path between  $u$  and  $v$  in  $\mathcal{G}$ . The distance between  $U, W \subseteq V_{\mathcal{G}}$  is the minimal distance of all  $u \in U$  and  $v \in W$ . We will sometimes consider directed graphs, where the set of edges is a subset of  $V_{\mathcal{G}}^2$ , but we mention this explicitly. A directed graph is *acyclic*, if it does not contain a (directed) cycle. A *source* (or *sink*) is a vertex without incoming (or outgoing) edges. A *colored* graph  $\mathcal{G}$  is a tuple  $(V, E, \chi)$  such that  $(V, E)$  is a graph and  $\chi$  is a map  $V \rightarrow \mathbb{N}$ . We interpret  $\chi$  as a vertex coloring of  $\mathcal{G}$  and denote it by  $\chi_{\mathcal{G}}$ . The *color class* of  $u \in V_{\mathcal{G}}$  is the set  $\chi_{\mathcal{G}}^{-1}(\chi_{\mathcal{G}}(u))$  of vertices of the same color as  $u$ . The *color class size* of  $\mathcal{G}$  is the maximal cardinality of its color classes. The graph  $\mathcal{G}$  is *ordered* if  $\chi$  is injective. We can see every graph as a colored graph in which every vertex is colored 0. An *isomorphism* of colored graphs  $\mathcal{G}$  and  $\mathcal{H}$  is a bijection  $f: V_{\mathcal{G}} \rightarrow V_{\mathcal{H}}$  such that, for all  $u, v \in V_{\mathcal{G}}$ , we have  $\chi_{\mathcal{G}}(u) = \chi_{\mathcal{H}}(f(u))$ , and  $\{u, v\} \in E_{\mathcal{G}}$  if and only if  $\{f(u), f(v)\} \in E_{\mathcal{H}}$ . If there is such an isomorphism,  $\mathcal{G}$  and  $\mathcal{H}$  are *isomorphic*.

**Resolution.** A *literal* is a proposition variable  $x$  or its negation  $\bar{x} := \neg x$ . We set  $\neg \bar{x} = x$ . A *clause*  $C$  is a finite set of literals  $\{\lambda_1, \dots, \lambda_k\}$ . We may write clauses as disjunctions, e.g.,  $C = (\lambda_1 \vee \dots \vee \lambda_k)$ . A *CNF formula*  $F$  is a finite set of clauses  $\{C_1, \dots, C_m\}$ , which we may write as a conjunction  $F = (C_1 \wedge \dots \wedge C_m)$ . The set of *variables occurring* in a clause  $C$  is  $\text{var}(C)$  and for a CNF formula  $F$  it is  $\text{var}(F) := \bigcup_{C \in F} \text{var}(C)$ . A (*partial*) *assignment* for a CNF formula  $F$  is a (partial) map  $\sigma: \text{var}(F) \rightarrow \{0, 1\}$ . The *domain* of  $\sigma$  is  $\text{dom}(\sigma)$ . The *size* of  $\sigma$  is  $|\text{dom}(\sigma)|$ . The assignment  $\sigma$  *violates* a clause  $C \in F$  if  $\text{var}(C) \subseteq \text{dom}(\sigma)$  and  $\sigma$  satisfies no literal in  $C$ . For a variable  $x \in \text{var}(F)$  and a Boolean value  $\delta \in \{0, 1\}$ , let  $\sigma[x \mapsto \delta]$  be the assignment with domain  $\text{dom}(\sigma) \cup \{x\}$  derived from  $\sigma$  that sets  $x$  to  $\delta$ , i.e.,  $\sigma[x \mapsto \delta](x) = \delta$  and  $\sigma[x \mapsto \delta](y) = \sigma(y)$  for all  $y \in \text{dom}(\sigma) \setminus \{x\}$ . For partial assignments  $\sigma$  and  $\sigma'$ , we write  $\sigma' \subseteq \sigma$  if  $\text{dom}(\sigma') \subseteq \text{dom}(\sigma)$  and  $\sigma'(x) = \sigma(x)$  for all  $x \in \text{dom}(\sigma')$ . For  $k \in \mathbb{N}$ , we write  $[k] := \{1, \dots, k\}$ . We now introduce the proof systems studied in this paper.

► **Definition 3** (Narrow Resolution [21]). A narrow resolution derivation  $\pi$  of a clause  $D$  from a CNF formula  $F$  is a directed acyclic graph  $\pi = (V, E)$  whose vertices are labeled with clauses,  $D$  is the label of a source of  $\pi$ , and all sinks of  $\pi$  are labeled with clauses in  $F$ . Moreover, for every vertex  $v \in V$ , its clause  $C$  is derived from the clauses  $C_1, \dots, C_\ell$  labeling the vertices, to which  $v$  has an outgoing edge, by one of the following three rules.

1. **Axiom Rule:**  $\ell = 0$  and  $C \in F$ .
2. **Resolution Rule:**  $\ell = 2$  and  $C_1 = A \vee x$ ,  $C_2 = B \vee \bar{x}$ , and  $C = A \vee B$ .
3. **Narrow Resolution Rule:**  $\ell \geq 2$  and, up to reordering,  $C_\ell = (A \vee \lambda_1 \vee \dots \vee \lambda_{\ell-1}) \in F$  is an axiom,  $C = (A \vee A_1 \vee \dots \vee A_{\ell-1})$ , and  $C_i = (A_i \vee \bar{\lambda}_i)$  for all  $i \in [\ell - 1]$ .

A *resolution derivation* is a narrow resolution derivation using only Rules 1 and 2. The derivation  $\pi$  is *tree-like* if  $\pi$  is a tree. In this case we call the unique source the *root* and the sinks *leaves*. The *size*  $|\pi|$  of the derivation  $\pi$  is the number of vertices  $|V|$ . The *depth* of  $\pi$  is the length of the longest directed path in it. The *width* of a clause  $C$  is its number of literals. The *width* of a derivation  $w(\pi)$  is the maximal width of all clauses in  $\pi$ . The *narrow width* of a derivation  $w^*(\pi)$  is the maximal number of literals among all those clauses in  $\pi$  that are not axioms. A *k-narrow* derivation is a narrow resolution derivation of narrow width at most  $k$ . A derivation of the empty clause from  $F$  is a *refutation* of  $F$ .

### 3 A Prover-Delayer Game for Tree-Like Narrow Resolution

In this section, we introduce a game that allows us to prove lower bounds on the size of  $k$ -narrow tree-like refutations of *graph isomorphism formulas*. We now introduce these formulas. Let  $\mathcal{G}$  and  $\mathcal{H}$  be  $n$ -vertex colored graphs; following [42], we define a CNF formula  $\text{ISO}(\mathcal{G}, \mathcal{H})$  whose solutions correspond to isomorphisms  $\mathcal{G} \rightarrow \mathcal{H}$ . For all vertices  $u \in V_{\mathcal{G}}$  and  $v \in V_{\mathcal{H}}$ , we add a propositional variable  $x_{u,v}$ . The variables  $x_{u,v}$  have the intended meaning that  $u$  is mapped to  $v$ . The CNF formula  $\text{ISO}(\mathcal{G}, \mathcal{H})$  contains three types of clause.

- **Color Clauses:** for each vertex  $u \in V_{\mathcal{G}}$ , let  $W_u := \chi_{\mathcal{H}}^{-1}(\chi_{\mathcal{G}}(u))$  be the vertices of  $\mathcal{H}$  with the same color as  $u$ . Add the clause  $\bigvee_{v \in W_u} x_{u,v}$  to encode that  $u$  is mapped to a vertex of the same color. For each  $v \in V_{\mathcal{H}}$ , let  $W_v := \chi_{\mathcal{G}}^{-1}(\chi_{\mathcal{H}}(v))$  and add the clause  $\bigvee_{u \in W_v} x_{u,v}$ .
- **Bijection Clauses:** For all  $u \in V_{\mathcal{G}}$  and distinct  $v, w \in V_{\mathcal{H}}$ , we add the clause  $(\neg x_{u,v} \vee \neg x_{u,w})$  to encode that an isomorphism is a function. For all distinct  $u, v \in V_{\mathcal{G}}$  and  $w \in V_{\mathcal{H}}$ , we add the clause  $(\neg x_{u,w} \vee \neg x_{v,w})$  to encode injectivity of the desired isomorphism.
- **Edge Clauses:** for all  $u, u' \in V_{\mathcal{G}}$  and  $v, v' \in V_{\mathcal{H}}$  with  $u \neq u'$  such that  $\{u, u'\} \in E_{\mathcal{G}}$  if and only if  $\{v, v'\} \notin E_{\mathcal{H}}$ , we include the clause  $\neg x_{u,v} \vee \neg x_{u',v'}$  to encode the edge relation.

The formula  $\text{ISO}(\mathcal{G}, \mathcal{H})$  has  $O(n^2)$  variables,  $O(n^4)$  clauses, width equal to the maximal color class size of  $\mathcal{G}$  and  $\mathcal{H}$  (unless every vertex gets a unique color; in this case the width is two), and is satisfiable if and only if  $\mathcal{G}$  is isomorphic to  $\mathcal{H}$ .

**The  $k$ -Narrow Prover-Delayer Game.** Let  $\mathcal{G}$  and  $\mathcal{H}$  be non-isomorphic colored graphs. The  $k$ -narrow Prover-Delayer game on  $\mathcal{G}, \mathcal{H}$  is played by two players, Prover and Delayer, who construct partial assignments for  $\text{ISO}(\mathcal{G}, \mathcal{H})$  as follows. The game begins with the empty assignment  $\sigma_0 = \emptyset$ . Let  $\sigma_{t-1}$  be the assignment after the  $(t-1)$ -th round. In round  $t$ , Prover chooses  $\sigma \subseteq \sigma_{t-1}$  with  $|\text{dom}(\sigma)| \leq k-1$  and makes one of the following kinds of moves.

1. **Resolution Move:** Prover chooses a variable  $x \notin \text{dom}(\sigma)$ . Delayer chooses a response.
  - a. **Committal Response:** Delayer responds with  $\delta \in \{0, 1\}$  and sets  $\sigma_t := \sigma[x \mapsto \delta]$ .
  - b. **Point Response:** Delayer gets a point; Prover picks  $\delta \in \{0, 1\}$  and sets  $\sigma_t := \sigma[x \mapsto \delta]$ .

2. *Narrow Move*: Prover chooses a color clause  $C$  from  $\text{ISO}(\mathcal{G}, \mathcal{H})$ . Again Delayer chooses one of two response types.
  - a. *Committal Response*: Delayer chooses some  $x \in C \setminus \sigma^{-1}(0)$  and sets  $\sigma_t := \sigma[x \mapsto 1]$ .
  - b. *Point Response*: Delayer chooses distinct  $x, y \in C \setminus \sigma^{-1}(0)$  and gets a point; Prover chooses  $z \in \{x, y\}$  and sets  $\sigma_t := \sigma[z \mapsto 1]$ .

If the assignment  $\sigma_t$  violates a clause of  $\text{ISO}(\mathcal{G}, \mathcal{H})$ , the game ends and *Prover wins*. Otherwise, the game continues in round  $t + 1$ . *Prover has an  $r$ -point strategy* if, no matter how Delayer plays, Prover can always win the game while limiting Delayer to at most  $r$  points. If Prover does *not* have an  $r$ -point strategy, then *Delayer has an  $(r + 1)$ -point strategy*. It will be useful to start the  $k$ -narrow Prover-Delayer game on  $\mathcal{G}, \mathcal{H}$  from assignments  $\sigma \neq \emptyset$ . In this case, the game starts at  $\sigma_0 = \sigma$ . By constructing strategies for Delayer, the game can be used to show tree-like size lower bound for resolution refutations of graph isomorphism formulas.

► **Lemma 4.** *For all  $k \geq 1$ , colored graphs  $\mathcal{G}, \mathcal{H}$ , and  $k$ -narrow tree-like refutations  $\pi$  of  $\text{ISO}(\mathcal{G}, \mathcal{H})$ , Prover has a  $(\lceil \log(|\pi|) \rceil)$ -point strategy in the  $(k + 1)$ -narrow Prover-Delayer game on  $\mathcal{G}, \mathcal{H}$ .*

**Proof Sketch.** Prover follows  $\pi$  starting at the empty clause at the root. If a resolution rule is applied to a variable  $x$ , then Prover makes a resolution move for  $x$ . Similarly, Prover follows narrow resolution moves. If Delayer makes a committal response, Prover moves to the corresponding child in  $\pi$ . If Delayer makes a point response, Prover moves to the child with the smallest subtree “below it”, at least halving the size of the subtree at the current position. Prover wins if a leaf is reached, so Delayer can score at most  $\lceil \log(|\pi|) \rceil$  points. ◀

**The  $k$ -pebble Game and Narrow Resolution.** We next recall the connection between  $(k - 1)$ -narrow resolution refutations and the  $k$ -variable fragment of first order logic [42]. For an integer  $k$ , we write  $\mathcal{L}_k$  for the set of first order formulas using at most  $k$  *distinct* variables. We denote the set of  $\mathcal{L}_k$ -formulas with quantifier depth at most  $r$  by  $\mathcal{L}_{k,r}$ . If two graphs  $\mathcal{G}$  and  $\mathcal{H}$  satisfy the same sentences of  $\mathcal{L}_k$  or  $\mathcal{L}_{k,r}$ , the graphs are  $\mathcal{L}_k$ -equivalent or  $\mathcal{L}_{k,r}$ -equivalent, respectively, and we write  $\mathcal{G} \simeq^k \mathcal{H}$  or  $\mathcal{G} \simeq^{k,r} \mathcal{H}$ , respectively.

These equivalences are characterized by the following game: Let  $\mathcal{G}$  and  $\mathcal{H}$  be (colored) graphs and  $k, r \in \mathbb{N}$ . The  $r$ -round  $k$ -pebble game on  $\mathcal{G}, \mathcal{H}$  is played by two players, Spoiler and Duplicator. A *position* of the game is a pair  $(\alpha, \beta)$  of partial assignments  $\alpha : [k] \rightarrow V_{\mathcal{G}}$  and  $\beta : [k] \rightarrow V_{\mathcal{H}}$  such that  $\text{dom}(\alpha) = \text{dom}(\beta)$ . These maps define positions of up to  $k$  pebble pairs on  $\mathcal{G}$  and  $\mathcal{H}$ . Duplicator aims to show that  $\mathcal{G}$  and  $\mathcal{H}$  are isomorphic; Spoiler tries to show they are not. Initially, no pebbles are placed. Let  $(\alpha_t, \beta_t)$  be the position at the end of round  $t < r$ . At the beginning of round  $t + 1$ , Spoiler picks one of the graphs, say  $\mathcal{G}$ , and  $i \in [k]$ . The  $i$ -th pebble pair is picked up and Spoiler places the  $i$ -th pebble for  $\mathcal{G}$  on some  $u \in V_{\mathcal{G}}$  yielding the map  $\alpha_{t+1}$ . Duplicator responds by placing the  $i$ -th pebble for  $\mathcal{H}$  on a vertex of  $\mathcal{H}$  yielding  $\beta_{t+1}$ . If  $(\alpha_{t+1}, \beta_{t+1})$  does *not induce a partial isomorphism*, meaning that  $\alpha(i) \mapsto \beta(i)$  is not an isomorphism of the induced subgraphs  $\mathcal{G}[\{\alpha(i) \mid i \in \text{dom}(\alpha)\}]$  and  $\mathcal{H}[\{\beta(i) \mid i \in \text{dom}(\beta)\}]$ , then *Spoiler wins*. Otherwise, if  $t + 1 < r$ , the play continues in the next round. If  $t + 1 = r$ , then *Duplicator wins*. A player (Spoiler or Duplicator) has a *winning strategy*, if they can win independently of the moves of the other player.

► **Theorem 5** ([29, 42]). *Let  $k, r \in \mathbb{N}$ . The following are equivalent:*

1.  $\mathcal{G} \not\simeq^{k,r} \mathcal{H}$ , i.e.,  $\mathcal{G}$  and  $\mathcal{H}$  are not  $\mathcal{L}_{k,r}$ -equivalent.
2. Spoiler has a winning strategy in the  $r$ -round  $k$ -pebble game on  $\mathcal{G}, \mathcal{H}$ .
3. There is a  $(k - 1)$ -narrow resolution refutation of  $\text{ISO}(\mathcal{G}, \mathcal{H})$  of depth at most  $r$ .

It will sometimes be convenient to start the game from position  $(\alpha_0, \beta_0) \neq (\emptyset, \emptyset)$ ; nothing else in the rules of the games changes in this case. Similarly, we may sometimes not specify the number of rounds in advance; in this case the game only ends if Spoiler wins.

#### 4 Twinned Graphs and Pebble Games

In this section, we introduce the *twinned graph* construction, which we described on a high-level in the introduction. This will allow us to transfer lower bounds on the  $k$ -pebble game with blocking to lower bounds on the  $k$ -narrow Prover-Delayer game (and therefore to lower bounds on  $(k-1)$ -narrow tree like refutation size).

Given a colored graph  $\mathcal{G}$ , we define a new colored graph as follows. For each vertex  $u \in V_{\mathcal{G}}$ , set  $\mathcal{X}_{\mathcal{G}}(u) := \{u_0, u_1\}$ , where  $u_0$  and  $u_1$  are fresh vertices; intuitively these are copies of  $u$ . We define the *twinned graph*  $\mathcal{X}(\mathcal{G})$  with vertex set  $V_{\mathcal{X}(\mathcal{G})} := \bigcup_{u \in V_{\mathcal{G}}} \mathcal{X}_{\mathcal{G}}(u)$  and edge set

$$E_{\mathcal{X}(\mathcal{G})} := \{ \{x, y\} \mid x \in \mathcal{X}_{\mathcal{G}}(u), y \in \mathcal{X}_{\mathcal{G}}(v), \{u, v\} \in E_{\mathcal{G}} \} \cup \{ \mathcal{X}_{\mathcal{G}}(u) \mid u \in V_{\mathcal{G}} \}.$$

We give  $u_0$  and  $u_1$  the same color in  $\mathcal{X}(\mathcal{G})$  as  $u$  has in  $\mathcal{G}$ . For notational convenience, we define  $\hat{u}_0 := u_1$  and  $\hat{u}_1 := u_0$ . Moreover, we define  $\mathcal{X}_{\mathcal{G}}^{-1}(u_i) := u$  for  $i \in \{0, 1\}$ .

We first show that – under a mild condition – if there is a  $k$ -narrow refutation of  $\text{ISO}(\mathcal{G}, \mathcal{H})$ , then there is a  $k$ -narrow refutation of  $\text{ISO}(\mathcal{X}(\mathcal{G}), \mathcal{X}(\mathcal{H}))$ . To state the condition, we need the following notion. Two distinct vertices  $u, v \in V_{\mathcal{G}}$  are *twins* if for every  $w \in V_{\mathcal{G}} \setminus \{u, v\}$ , we have that  $\{u, w\} \in E_{\mathcal{G}}$  if and only if  $\{v, w\} \in E_{\mathcal{G}}$ . That is, the neighborhoods of  $u$  and  $v$  in  $\mathcal{G}$  are, apart from  $u$  and  $v$  themselves, identical. Twins  $u$  and  $v$  are *connected twins* if  $\{u, v\} \in E_{\mathcal{G}}$ . Note that if  $\mathcal{G}$  has no connected twins, then  $\mathcal{X}(\mathcal{G})$  has exactly one pair of connected twins for each vertex in  $\mathcal{G}$ . This leads to the following observation.

► **Lemma 6.** *Let  $k \geq 3$  and  $\mathcal{G}$  and  $\mathcal{H}$  be colored graphs that do not have connected twins. If  $\mathcal{G} \not\preceq^{k,r} \mathcal{H}$ , then  $\mathcal{X}(\mathcal{G}) \not\preceq^{k,r+1} \mathcal{X}(\mathcal{H})$ .*

By applying Theorem 5 we obtain the following corollary.

► **Corollary 7.** *Let  $k \geq 2$  and  $\mathcal{G}$  and  $\mathcal{H}$  be colored graphs that have no connected twins. If there exists a  $k$ -narrow refutation of  $\text{ISO}(\mathcal{G}, \mathcal{H})$  of depth  $d$ , then there exists a  $k$ -narrow refutation of  $\text{ISO}(\mathcal{X}(\mathcal{G}), \mathcal{X}(\mathcal{H}))$  of depth  $d+1$ .*

It turns out that Prover-Delayer lower bounds on our twinned graphs are implied by round lower bounds for certain pebble games on the original graphs. The normal  $k$ -pebble game is the wrong tool for this task; intuitively, the reason is the asymmetry between setting a variable of a graph isomorphism formula to zero or one.

**The  $k$ -Pebble Game with Blocking.** Let  $\mathcal{G}$  and  $\mathcal{H}$  be colored graphs and  $k, r \in \mathbb{N}$ . We define the  $r$ -round  $k$ -pebble game with blocking on  $\mathcal{G}$  and  $\mathcal{H}$  as follows. The game is played in rounds by Spoiler and Duplicator. A position in the game is a triple  $(\alpha, \beta, c)$  of partial maps  $\alpha : [k] \rightarrow V_{\mathcal{G}}$ ,  $\beta : [k] \rightarrow V_{\mathcal{H}}$ , and  $c : [k] \rightarrow \{\text{regular}, \text{blocking}\}$  with  $\text{dom}(\alpha) = \text{dom}(\beta) = \text{dom}(c)$ . The first two maps give the positions of the pebbles and  $c$  marks each pair of pebbles as either *regular* or *blocking*. Regular pebbles (possibly) define partial isomorphisms as before, but blocking ones forbid certain ones as follows.

► **Definition 8 (Partial Isomorphism with Blocking).** *Let  $(\alpha, \beta, c)$  be a position in the  $r$ -round  $k$ -pebble game with blocking on  $\mathcal{G}$  and  $\mathcal{H}$ ,  $R := c^{-1}(\text{regular})$ , and  $B := c^{-1}(\text{blocking})$ . Then  $(\alpha, \beta, c)$  induces a partial isomorphism with blocking if  $(\alpha|_R, \beta|_R)$  induces a partial isomorphism and if every regular pebble respects every blocking pebble. Formally, this means that for every  $p \in B$  and  $q \in R$ , we have  $(\alpha(p), \beta(p)) \neq (\alpha(q), \beta(q))$ .*

In the initial position  $(\alpha_0, \beta_0, c_0)$ , all maps are empty. Let  $(\alpha_t, \beta_t, c_t)$  be the position after the  $t$ -th round. At the beginning of the  $(t+1)$ -th round, Spoiler can make either a *regular move* or a *blocking move*. A regular move works in the same way as a move in the  $k$ -pebble game; the pebble pair moved in this turn is then marked **regular**. For a blocking move, Spoiler picks  $p \in [k]$  and places the  $p$ -th pebble in  $\mathcal{G}$  on some vertex  $u \in V_{\mathcal{G}}$  and in  $\mathcal{H}$  on some vertex  $v \in V_{\mathcal{H}}$ . Duplicator next decides how to mark this pair. If Duplicator chooses **regular**, then the round ends. If instead Duplicator chooses **blocking**, then the round continues and Spoiler can again choose to make either a regular or a blocking move. If  $(\alpha_{t+1}, \beta_{t+1}, c_{t+1})$  does *not* induce a partial isomorphism with blocking, then *Spoiler wins* and the game ends. Otherwise if  $t+1 < r$ , the game continues in round  $t+2$ . If  $t+1 = r$ , then *Duplicator wins*.

We write  $\mathcal{G} \simeq_{\mathcal{B}}^{k,r} \mathcal{H}$  if Duplicator has a winning strategy in the  $r$ -round  $k$ -pebble game with blocking. If  $\mathcal{G} \simeq_{\mathcal{B}}^{k,r} \mathcal{H}$  for all  $r \in \mathbb{N}$ , then we write  $\mathcal{G} \simeq_{\mathcal{B}}^k \mathcal{H}$ . As for the  $k$ -pebble game, it will also be convenient to consider variants of the  $k$ -pebble game with blocking where we start from arbitrary positions or do not specify the number of rounds in advance. Note that while in the (non-blocking)  $k$ -pebble game it never makes sense for Spoiler to place a pebble on an already pebbled vertex, this is not the case in the  $k$ -pebble game with blocking.

**Spoiler and Duplicator meet Prover and Delayer.** We end the section by connecting the  $k$ -pebble game with blocking to the  $k$ -narrow Prover-Delayer game via the following lemma.

► **Lemma 9.** *Let  $\mathcal{G}$  and  $\mathcal{H}$  be colored graphs and  $k \geq 2$  an integer. If  $\mathcal{G} \simeq_{\mathcal{B}}^{k,r} \mathcal{H}$ , then Delayer has an  $r$ -point strategy in the  $k$ -narrow Prover-Delayer game on  $\mathcal{X}(\mathcal{G}), \mathcal{X}(\mathcal{H})$ .*

**Proof Sketch.** In the  $k$ -narrow Prover-Delayer game on  $\mathcal{X}(\mathcal{G}), \mathcal{X}(\mathcal{H})$ , Delayer simulates positions of the  $k$ -pebble game with blocking on  $\mathcal{G}, \mathcal{H}$ . Intuitively, whenever a **regular** pebble pair is placed on vertices  $u$  and  $v$  (and there is not already a pebble pair on  $u$  and  $v$ ), Delayer should score a point since it “does not matter” whether we map  $u_0$  to  $v_0$  or to  $v_1$ . As the round counter of the  $k$ -pebble game with blocking only advances when a pebble pair is marked as **regular**, filling in the details is relatively straightforward. ◀

Lemmas 4 and 9 finally connect the pebble game with blocking to tree-like refutation size.

► **Theorem 10.** *Let  $k \geq 1$ , and  $r \in \mathbb{N}$  and  $\mathcal{G}$  and  $\mathcal{H}$  be colored graphs. If  $\mathcal{G} \simeq_{\mathcal{B}}^{k+1,r} \mathcal{H}$ , then every  $k$ -narrow tree-like refutation of  $\text{ISO}(\mathcal{X}(\mathcal{G}), \mathcal{X}(\mathcal{H}))$  has size at least  $2^r$ .*

## 5 Compressing CFI Graphs

By what we have seen so far (Corollary 7 and Theorem 10), to prove Theorem 1 it suffices to show that Duplicator can survive a large number of rounds in the  $k$ -pebble game with blocking on suitably chosen colored graphs  $\mathcal{G}, \mathcal{H}$ . In this section, we describe a framework which allows us to construct such graphs.

Concretely, we recall a recent approach to construct pairs of graphs that require quantifier depth  $\Omega(n^{k/2})$  to be distinguished in  $k$ -variable first order logic  $\mathcal{L}_k$  (and also with counting) [25]. The key idea is a novel compression technique of the so-called Cai-Fürer-Immerman (CFI) graphs [17] and a concrete compression construction for CFI graphs over grids. Having introduced this construction, we give a method for proving lower bounds for the  $k$ -pebble game with blocking on compressed CFI graphs. To do this, we first recall a variant of the Cops and Robber game, which can be used to derive lower bounds on the  $k$ -pebble game on compressed CFI graphs, and then extend this game with an appropriate notion of blocking.

**CFI Graphs.** Let  $\mathcal{G} = (V_{\mathcal{G}}, E_{\mathcal{G}})$  be a connected ordered graph, called a *base graph*, and  $f: E_{\mathcal{G}} \rightarrow \mathbb{F}_2$  be a function, where  $\mathbb{F}_2$  is the two-element field. From  $\mathcal{G}$  and  $f$  we derive the colored CFI graph  $\text{CFI}(\mathcal{G}, f)$ : Vertices of  $\mathcal{G}$  are called *base vertices*. Every base vertex of  $\mathcal{G}$  is replaced by a *CFI gadget* and gadgets of adjacent vertices are connected. The vertices of the CFI gadget for a degree  $d$  base vertex  $u \in V_{\mathcal{G}}$  are the pairs  $(u, \bar{a})$  for all  $d$ -tuples  $\bar{a} = (a_1, \dots, a_d) \in \mathbb{F}_2^d$  with  $\sum_{i=1}^d a_i = 0$ . The vertex  $(u, \bar{a})$  has *origin*  $u$ . Vertices inherit the color of their origin. Since every vertex of the base graph has a unique color, the vertices of each gadget form a color class of the CFI graph. For all adjacent base vertices  $u, v \in V_{\mathcal{G}}$ , we add the following edges between the gadgets for  $u$  and  $v$ : Let  $u$  be the  $i$ -th neighbor of  $v$  and  $v$  be the  $j$ -th neighbor of  $u$  according to the order on  $V_{\mathcal{G}}$ . There is an edge between vertices  $(u, \bar{a})$  and  $(v, \bar{b})$  if and only if  $a_i + b_j = f(\{u, v\})$ , where  $a_i$  is the  $i$ -th entry of  $\bar{a}$  and  $b_j$  is the  $j$ -th entry of  $\bar{b}$ . See Figure 1 for an example. We say that two functions  $f, g: E_{\mathcal{G}} \rightarrow \mathbb{F}_2$  *twist an edge*  $e \in E_{\mathcal{G}}$  or the edge  $e \in E_{\mathcal{G}}$  is *twisted by  $f$  and  $g$*  if  $f(e) \neq g(e)$ . It is known that  $\text{CFI}(\mathcal{G}, f) \not\cong \text{CFI}(\mathcal{G}, g)$  if and only if  $f$  and  $g$  twist an odd number of edges [17].

**Compressing CFI Graphs.** CFI graphs are a well-studied tool to derive lower bounds for  $k$ -variable logic with counting or other logics, see e.g. [15, 17, 18, 20, 31]. This construction and its generalizations have also been used to derive proof complexity lower bounds on graph isomorphism in various proof systems [12, 13, 32, 36, 40, 41]. We now discuss the method of *compressing CFI graphs* [25]. The goal is to reduce the size of the resulting graph while essentially preserving the hardness of it. The main idea is to identify the gadgets of certain base vertices. The hardness of the resulting compressed CFI graphs heavily depends on which gadgets get identified and can be analyzed using a variant of the Cops and Robber game. We now present this framework.

► **Definition 11 (Graph Compression).** An equivalence relation  $\equiv$  on  $V_{\mathcal{G}}$  is a  $\mathcal{G}$ -compression if for all  $u, u', v, v' \in V_{\mathcal{G}}$  it satisfies the following two conditions:

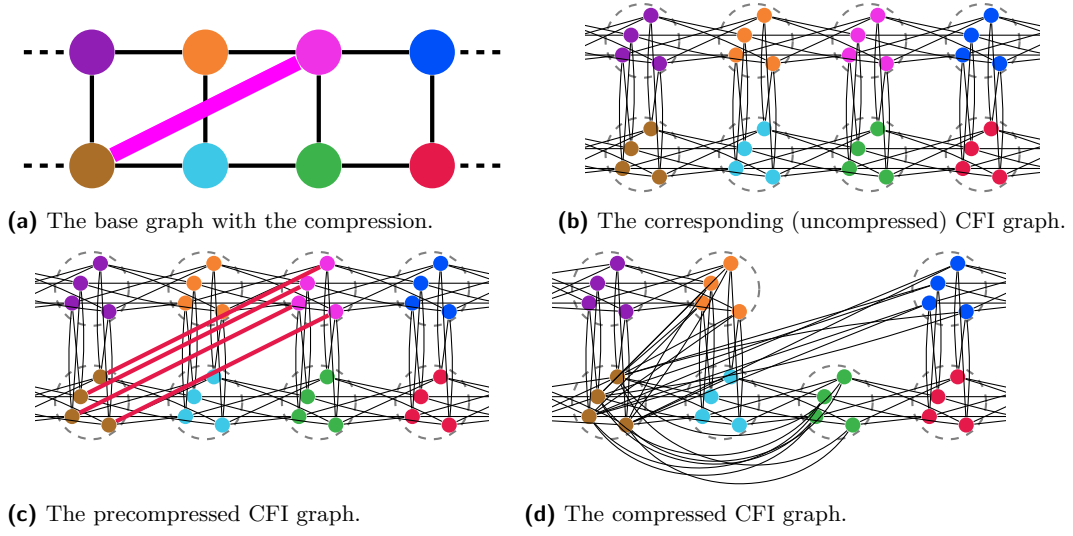
1. If  $u \equiv v$ , then  $u$  and  $v$  are non-adjacent and of the same degree.
2. If  $\{u, v\}, \{u', v'\} \in E_{\mathcal{G}}$ ,  $u \equiv u'$ ,  $v \equiv v'$ , and  $u$  is the  $i$ -th neighbor of  $v$  (according to the order on  $V_{\mathcal{G}}$ ), then  $u'$  is the  $i$ -th neighbor of  $v'$ .

Let  $\equiv \subseteq V_{\mathcal{G}}^2$  be a  $\mathcal{G}$ -compression. It induces an equivalence relation on  $\text{CFI}(\mathcal{G}, f)$  (independently of the function  $f: E \rightarrow \mathbb{F}_2$ ), which we also denote by  $\equiv$ , via  $(u, \bar{a}) \equiv (v, \bar{b})$  if and only if  $u \equiv v$  and  $\bar{a} = \bar{b}$ . Contracting all  $\equiv$ -equivalence classes in  $\text{CFI}(\mathcal{G}, f)$  into a single vertex yields the colored graph  $\text{CFI}(\mathcal{G}, f)/\equiv$ : the vertices of  $\text{CFI}(\mathcal{G}, f)/\equiv$  are the  $\equiv$ -equivalence classes  $u/\equiv := \{w \in V_{\text{CFI}(\mathcal{G}, f)} \mid w \equiv u\}$ , and  $u/\equiv$  and  $v/\equiv$  are adjacent if there are  $u' \equiv u$  and  $v' \equiv v$  such that  $u'$  and  $v'$  are adjacent in  $\text{CFI}(\mathcal{G}, f)$ . Observe that  $\text{CFI}(\mathcal{G}, f)/\equiv$  is loop-free by the condition on  $\equiv$  that equivalent vertices of  $\mathcal{G}$  are non-adjacent. The color of a  $\equiv$ -equivalence class in  $\text{CFI}(\mathcal{G}, f)/\equiv$  is the minimal color of one of its members in  $\text{CFI}(\mathcal{G}, f)$ . To obtain reasonable graphs,  $f$  has to be compatible with the compression  $\equiv$  in the following sense.

► **Definition 12 (Compressible).** A function  $f: E_{\mathcal{G}} \rightarrow \mathbb{F}_2$  is  $\equiv$ -compressible if  $f(\{u, v\}) = f(\{u', v'\})$  for all vertices  $u, v, u', v' \in V_{\mathcal{G}}$  such that  $\{u, v\}, \{u', v'\} \in E_{\mathcal{G}}$ ,  $u \equiv u'$ , and  $v \equiv v'$ .

► **Definition 13 (Compressed CFI).** For a  $\mathcal{G}$ -compression  $\equiv$  and a  $\equiv$ -compressible function  $f: E_{\mathcal{G}} \rightarrow \mathbb{F}_2$ , the graph  $(\text{CFI}(\mathcal{G}, f), \equiv)$  expanding the colored graph  $\text{CFI}(\mathcal{G}, f)$  with  $\equiv$  is a precompressed CFI graph, and the colored graph  $\text{CFI}(\mathcal{G}, f)/\equiv$  is a compressed CFI graph.

Precompressed CFI graphs can also be seen as edge-colored graphs that use two colors for the edges – one for the regular edges and one for the equivalence relation. An example is shown in Figure 1. The round number of the bijective  $k$ -pebble game (a variant of the  $k$ -pebble



■ **Figure 1** Compressed CFI graphs for a grid of height 2 as base graph, a very simple compression, which only identifies two base vertices, and the function that assigns 0 to all edges. The compression on the base graph and the induced one on the precompressed CFI graph is drawn in magenta.

game that characterizes equivalence of  $k$ -variable first order logic with counting quantifiers) on precompressed and compressed CFI graphs are almost equal [25]. The corresponding statement for the  $k$ -pebble game with blocking is proved similarly.

► **Lemma 14.** Let  $k \geq 3$ ,  $r \in \mathbb{N}$ ,  $\equiv$  be a  $\mathcal{G}$ -compression, and  $f, g : E_{\mathcal{G}} \rightarrow \mathbb{F}_2$  be  $\equiv$ -compressible.

1.  $\text{CFI}(\mathcal{G}, f) \not\equiv_{\mathcal{B}}^{k,r} \text{CFI}(\mathcal{G}, g)$  implies  $(\text{CFI}(\mathcal{G}, f), \equiv) \not\equiv_{\mathcal{B}}^{k,r} (\text{CFI}(\mathcal{G}, g), \equiv)$ .
2.  $(\text{CFI}(\mathcal{G}, f), \equiv) \not\equiv_{\mathcal{B}}^{k,r} (\text{CFI}(\mathcal{G}, g), \equiv)$  implies  $\text{CFI}(\mathcal{G}, f) / \equiv \not\equiv_{\mathcal{B}}^{k,r} \text{CFI}(\mathcal{G}, g) / \equiv$ .
3.  $\text{CFI}(\mathcal{G}, f) / \equiv \not\equiv_{\mathcal{B}}^{k,r} \text{CFI}(\mathcal{G}, g) / \equiv$  implies  $(\text{CFI}(\mathcal{G}, f), \equiv) \not\equiv_{\mathcal{B}}^{k,r+2} (\text{CFI}(\mathcal{G}, g), \equiv)$ .

**The Compressed Cops and Robber Game.** The ability of the bijective  $k$ -pebble game to distinguish non-isomorphic CFI graphs is captured by the  $k$ -Cops and Robber game [25, 37]. A variant of this game – the compressed  $k$ -Cops and Robber game – provides lower bounds for compressed CFI graphs. To see this, we consider isomorphisms of CFI graphs. These always twist an even number of edges and can be described in terms of paths in the base graphs by twistings (defined below). Moreover, if these paths are compatible with the compression, they induce isomorphisms of compressed CFI graphs. For ordered base graphs, these twistings correspond one-to-one with isomorphisms of the (compressed) CFI graphs.

► **Definition 15 (Twisting).** A set  $T \subseteq \{(u, v) \mid \{u, v\} \in E\}$  is called a  $\mathcal{G}$ -twisting if, for every  $u \in V$ , the set  $T \cap (\{u\} \times V)$  is of even size. The twisting  $T$

- twists an edge  $\{u, v\} \in E$  if the set  $T$  contains exactly one of  $(u, v)$  and  $(v, u)$  and
- fixes a vertex  $u \in V$  if  $T \cap (\{u\} \times V) = \emptyset$ .

To obtain a reasonable notion of twistings for isomorphisms of compressed CFI graphs, the twistings have to be compatible with the compression. For more details on (compressed) CFI graphs, their isomorphisms, and twistings, we refer to the original paper [25].

► **Definition 16 (Compressible Twisting).** For a  $\mathcal{G}$ -compression  $\equiv$ , a  $\mathcal{G}$ -twisting  $T$  is called  $\equiv$ -compressible if the following holds for all  $u, u' \in V$  with  $u \equiv u'$ : Let  $u$  and  $u'$  be of degree  $d$ . Then for every  $i \in [d]$ , we have  $(u, v_i) \in T$  if and only if  $(u', v'_i) \in T$ , where  $v_i$  is the  $i$ -th neighbor of  $u$  and  $v'_i$  is the  $i$ -th neighbor of  $u'$  (according to the order on  $\mathcal{G}$ ).

The *compressed  $k$ -Cops and Robber game* [25] is played on a base graph  $\mathcal{G}$  and a  $\mathcal{G}$ -compression  $\equiv$ . The Cops Player places cops on up to  $k$   $\equiv$ -equivalence classes and the robber is placed on one edge of  $\mathcal{G}$ . Initially, only the robber is placed. The game proceeds in rounds:

1. The Cops Player picks up a cop and announces a new  $\equiv$ -equivalence class  $C$  for this cop.
2. The robber moves. To move from the current edge  $e_1$  to another edge  $e_2$ , the robber has to provide a  $\equiv$ -compressible  $\mathcal{G}$ -twisting that only twists the edges  $e_1$  and  $e_2$  and that fixes every vertex contained in a cop-occupied  $\equiv$ -equivalence class.
3. The cop that was picked up in Step 1 is placed on  $C$ . The next round starts.

The robber is *caught* if the two endpoints of the robber-occupied edge are contained in cop-occupied  $\equiv$ -classes. The cops have a winning strategy in  $r$  rounds, if they can catch the robber in  $r$  rounds independently of the moves of the robber. Similarly, the robber has a *strategy for the first  $r$  rounds* if the robber can avoid being caught for  $r$  rounds independently of the moves of the Cops Player. The winner of the compressed game depends on the initial position of the robber. This game yields lower bounds for the (bijective)  $k$ -pebble game:

► **Lemma 17** ([25]). *Let  $\equiv$  be a  $\mathcal{G}$ -compression and suppose  $f, g : E_{\mathcal{G}} \rightarrow \mathbb{F}_2$  only twist a single edge  $e$ . If the robber, initially placed on the edge  $e$ , has a strategy for the first  $r$  rounds in the compressed  $k$ -Cops and Robber game on  $\mathcal{G}$  and  $\equiv$ , then  $(\text{CFI}(\mathcal{G}, f), \equiv) \simeq^{k,r} (\text{CFI}(\mathcal{G}, g), \equiv)$ .*

**Introducing Roadblocks for Cops.** To obtain lower bounds for the  $k$ -pebble game with blocking, we add “roadblocks” to the compressed Cops and Robber game and prove a blocking analogue of Lemma 17. Let  $\mathcal{G}$  be an ordered graph. A *roadblock for a vertex  $u \in V_{\mathcal{G}}$*  is a nonempty set  $N \subseteq \{(u, v) \mid \{u, v\} \in E_{\mathcal{G}}\}$  of (directed) edges incident to  $u$  of even size. A  $\mathcal{G}$ -twisting  $T$  *avoids a roadblock  $N$*  for a vertex  $u$  if  $T \cap \{u\} \times V_{\mathcal{G}} \neq N$ . In particular,  $T$  may contain a strict superset or subset of  $N$ . If  $T$  does not avoid  $N$ , then  $T$  *uses  $N$* . A *roadblock for a  $\equiv$ -equivalence class  $C$*  is a nonempty set  $N \subseteq [d]$  of even size, where  $d$  is the unique degree of the vertices in  $C$ . A  $\mathcal{G}$ -twisting  $T$  *avoids the roadblock  $N$  on  $C$*  if, for every vertex  $u \in C$ , the twisting  $T$  avoids the roadblock  $N_u := \{(u, v_i) \mid i \in N\}$  for  $u$ , where  $v_i$  denotes the  $i$ -th neighbor of  $u$ . If  $T$  is  $\equiv$ -compressible and does not avoid  $N$ , then  $T$  *uses  $N_u$*  for every vertex  $u \in C$ ; we say that  $T$  *uses  $N$* . Let  $M \subseteq [d]$  be the set of all  $i \in [d]$  such that  $T$  contains the edge to the  $i$ -th neighbor of some and, since  $T$  is  $\equiv$ -compressible, of every  $u \in C$ . We write  $T(N)$  for the symmetric difference of  $N$  and  $M$ .

The *compressed and blocking  $k$ -Cops and Robber game* is played on a base graph  $\mathcal{G}$  and a  $\mathcal{G}$ -compression  $\equiv$ . The Cops Player controls cops and roadblocks. The total number of cops and roadblocks is  $k$  but the number of each may vary during the game. Cops and roadblocks are placed on  $\equiv$ -equivalence classes and the robber is located on an edge. Initially, only the robber is placed. A round of the game proceeds as follows: The Cops Player picks up a cop or a roadblock and can choose to play a cop move or a blocking move.

1. A *cop move* proceeds similarly to the non-blocking game. First, the Cops Player announces a  $\equiv$ -equivalence class  $C$ . Next, the robber moves. To move from an edge  $e_1$  to another edge  $e_2$ , the robber provides a  $\equiv$ -compressible  $\mathcal{G}$ -twisting  $T$  that only twists the edges  $e_1$  and  $e_2$ , fixes every vertex contained in a cop-occupied  $\equiv$ -equivalence class, and avoids every roadblock. Afterwards, a cop is placed on the announced class  $C$ .
2. For a *blocking move*, the Cops Player announces a  $\equiv$ -equivalence class  $C$  and a roadblock  $N$  for  $C$ . Next, the robber moves with a  $\equiv$ -compressible  $\mathcal{G}$ -twisting  $T$  as in the cop move. If  $T$  uses  $N$ , then a cop is placed on  $C$ . Otherwise, the roadblock  $N$  is placed on  $C$ .
3. The existing roadblocks are updated. If a roadblock  $N'$  is placed on a class  $C'$ , then it is replaced by the roadblock  $T(N')$  on  $C'$ . Because in both a cop and a blocking move  $T$  avoids all roadblocks,  $T(N')$  will always be a nonempty set. If a roadblock was placed in this move, the Cops Player can again choose to play either a cop or a blocking move without increasing the round counter.

The notion of the robber being caught or having a strategy for the first  $r$  round is the same as in the non-blocking game. As in the non-blocking game, the starting edge of the robber is important. The following lemma is proved similarly to Lemma 17.

► **Lemma 18.** *Suppose  $\equiv$  is a  $\mathcal{G}$ -compression and  $f, g : E_{\mathcal{G}} \rightarrow \mathbb{F}_2$  only twist a single edge  $e$ . If the robber, initially placed on the edge  $e$ , has a strategy for the first  $r$  rounds in the compressed and blocking  $k$ -Cops and Robber game on  $\mathcal{G}$  and  $\equiv$ , then  $(\text{CFI}(\mathcal{G}, f), \equiv) \simeq_{\mathcal{B}}^{k,r} (\text{CFI}(\mathcal{G}, g), \equiv)$ .*

The  $\equiv$ -compressible twistings of the robber induce isomorphisms of the compressed CFI graphs, which respect all currently placed pebbles. These are used to move the twisted edge (“the robber”) away from the pebbles. Cops correspond to **regular** pebble pairs and roadblocks to **blocking** ones. The case distinction in Point 2 whether a cop roadblock is placed ensures that in a blocking move in the pebble game with blocking the pebble pair gets marked as **regular** or **blocking** consistently with the current isomorphism. Updating the roadblocks in Point 3 corresponds to applying the isomorphism induced by the twisting  $T$  to them.

## 6 The Super-Linear Lower Bound with Roadblocks

We now present and analyze the robust compressed CFI construction of [19]. This work shows that the robber can survive for a large number of rounds in the compressed Cops and Robber game for certain compressions. This section shows that the robber also has a strategy for a large number of rounds in the game with roadblocks. By Lemma 18 and Theorem 10, such a result implies a lower bound on tree-like refutation size for graph isomorphism formulas.

### 6.1 Compressing Cylindrical Grids

Fix an integer  $k \geq 3$  and a sufficiently large integer  $w$ . Set  $f(k) := 4k$ . Let  $p_1, \dots, p_k$  be pairwise coprime numbers such that  $\frac{w}{2} \leq p_i \leq w$  for every  $i \in [k]$ . For all sufficiently large  $w$ , such numbers exist [25]. Set  $J := f(k) \cdot p_1 \cdot \dots \cdot p_k$ . Let  $\mathcal{C}$  be the  $k \times J$  cylindrical grid, that is, the  $k \times J$  grid, in which we also connect the top and bottom row. The vertices of  $\mathcal{C}$  are pairs  $(i, j)$  for all  $i \in [k]$  and  $j \in [J]$ . They are ordered lexicographically. We think of the first component as the row index and the second component as the column index. We refer to the first  $f(k)$  columns as the *left end* of  $\mathcal{C}$ , and to the last  $f(k)$  columns as the *right end* of  $\mathcal{C}$ . We use addition on row indices in a modulo-like manner, e.g., the  $(k+1)$ -th row is the first one and  $p_{k+1} = p_1$ . For each  $t \in [k-1]$ , we define the following equivalence  $\equiv^t$  via:

$$(i, j) \equiv^t (i', j') \iff i = i'; f(k) < j, j' \leq J - f(k); \text{ and } j - j' \text{ is divisible by } f(k)p_i \cdot \dots \cdot p_{i+t}.$$

These equivalences are  $\mathcal{C}$ -compressions [19]. Note that the vertices in the left or the right end of  $\mathcal{C}$  are in singleton  $\equiv^t$ -equivalence classes. The vertices in between are identified periodically, but the period is different in every row. It is not hard to show that there are  $\Theta(w^{t+1})$   $\equiv^t$ -equivalence classes. Together with the fact that CFI gadgets for degree 4 base vertices have 8 vertices, this implies the next lemma:

► **Lemma 19.** *For all  $t \in [k-1]$  and  $\equiv^t$ -compressible  $f : E_{\mathcal{C}} \rightarrow \mathbb{F}_2$ , the graph  $\text{CFI}(\mathcal{C}, f) / \equiv^t$  has order  $\Theta(w^{t+1})$  (where  $k$  and  $t$  are seen as constants) and color class size 8.*

While the order of the graphs is  $\Theta(w^{t+1})$ , the robber has a strategy for  $\Omega(w^k)$  rounds:

► **Theorem 20** ([19]). *For every  $t \in [k-1]$ , consider the compressed  $(k+t)$ -Cops and Robber game played on  $\mathcal{C}$  and  $\equiv^t$ . If the robber is initially placed on an edge on the left or right end of  $\mathcal{C}$ , then the robber has a strategy for the first  $\Omega(J) = \Omega(w^k)$  rounds.*

Unfortunately, this theorem does not lift to the game with roadblocks; in order to lift it, we investigate the strategy of the robber in more detail: The robber is always located in either the left or right end of the grid. On uncompressed grids of height  $k$ , the optimal strategy of the Cops Player with at most  $2k$  cops is to separate the left from the right end of grid using the cops and to move this separator slowly towards the robber (by at most a constant number of columns in each round). So the robber can avoid getting caught for a number of rounds linear in the length of the grid: when a newly announced cop is about to form a separator, the robber moves to the end furthest from the separator. In the compressed game, the strategy is similar. However, the suitable notion of a separator and the analysis of the situations in which the robber can move from the one end of the grid to the other are more complicated. We now describe them on an informal level to illustrate the central ideas. For formal details and more explanations, we refer to the original works [19, 25].

To move the robber from one end of the grid to the other, we use  $\equiv^t$ -compressible  $\mathcal{C}$ -twistings that twist exactly two edges, one in the first and one in the last column. Such twistings are called *t-end-to-end twistings* and are obtained from  $\ell$ -periodic paths [25]. Intuitively, these are paths from the first to the last column in the grid  $\mathcal{C}$ , which repeat every  $\ell$  columns. This means that an  $\ell$ -periodic path is defined by a path in columns 0 to  $\ell - 1$  repeating every  $\ell$  columns. If  $\ell$  is the greatest common divisor of the compression periods of all the rows used by the path, then the path induces a *t-end-to-end twisting*:

► **Lemma 21** ([19, 25]). *Let  $t \in [k - 1]$ ,  $\pi = (u_1, \dots, u_m)$  be an  $\ell$ -periodic path, and  $I \subseteq [k]$  be the set of all rows of which  $\pi$  contains vertices. If  $\ell = \gcd\{f(k)p_i \cdot \dots \cdot p_{i+t} \mid i \in I\}$ , then  $\pi$  induces the  $\equiv^t$ -compressible  $\mathcal{C}$ -twisting  $\{(u_i, u_{i-1}), (u_i, u_{i+1}) \mid 1 < i < m\}$ .*

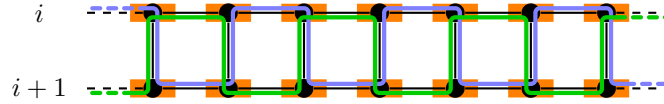
We now turn to a suitable notion of “a separator” for the compressed grid. Let  $W$  be a set of  $\equiv^t$ -equivalence classes. A *t-virtual cordon* [19] for  $W$  is a separator  $S \subseteq V_{\mathcal{C}}$  that separates the left from the right end of the grid  $\mathcal{C}$  and satisfies additional conditions on the vertices that  $S$  is allowed to contain. For example, if  $W$  contains only one class of row  $i$ , then  $S$  may only contain a single vertex from that class. A set  $W$  is *t-critical*, if there is a *t-virtual cordon* for  $W$  and there is no periodic path satisfying the conditions of Lemma 21 that avoids all vertices of the classes in  $W$  (and actually even more). Intuitively, for *t-critical* sets the robber cannot move between both ends. For non-*t-critical* sets of size at most  $k + t - 1$  (so in situations where at least one cop is picked up), this is always possible using periodic paths.

► **Lemma 22** ([19]). *Let  $t \in [k - 1]$  and let  $W$  be a set of at most  $k + t - 1$  many  $\equiv^t$ -equivalence classes. If  $W$  is not *t-critical*, then there is a *t-end-to-end-twisting* avoiding all classes in  $W$ .*

The minimal distance of the robber to an inclusion-wise minimal *t-virtual cordon* for  $W$  measures the distance between the robber and the cops. When an announced cop will make the position *t-critical*, the robber moves to the end to which this distance is larger. This distance decreases by at most a constant in each round [19]. So, the robber still has a strategy for a number of rounds linear in the grid length. Since the compressed CFI graphs are much smaller, we get a much better bound for the  $k$ -pebble game on the compressed CFI graphs.

## 6.2 Cops do not Benefit From Roadblocks

We now show that for the  $\mathcal{C}$ -compressions of the previous section, the Cops Player does not benefit from roadblocks. This means that, although blocking moves possibly allow the Cops Player to make multiple moves per round, the number of rounds the robber can avoid getting caught does not change asymptotically compared to the game without roadblocks. Note that converting a roadblock to a cop only makes it harder for the robber to move. To see this,



■ **Figure 2** The two 2-periodic paths (in blue and in green) constructed in the proof of Lemma 23. Edges in and between rows  $i$  and  $i + 1$  in the cylindrical grid are drawn in black. Both paths never use the same incident edges of any vertex. Avoided horizontal roadblocks are drawn in orange.

observe that a roadblock prevents the robber from passing through a vertex (or class) using a specified set of incident edges, while a cops prevents the robber from passing through the vertex (or class) at all.

► **Lemma 23.** *Let  $t \in [k - 1]$  and  $c \leq \frac{2}{5}k - 1$  be integers. Consider the compressed and blocking  $(k + c)$ -Cops and Robber game on  $\mathcal{C}$  and  $\equiv^t$  and assume that cops are placed in at most  $c$  rows. Then there is a  $t$ -end-to-end twisting that avoids all cop-occupied  $\equiv^t$ -equivalence classes and avoids all roadblocks.*

**Proof Sketch.** We call a roadblock *horizontal* if it blocks the use of exactly the two horizontal incident edges of a vertex or  $\equiv^t$ -class. If there are no horizontal roadblocks in a *cop-free* row, then the straight path through that row is a  $t$ -end-to-end twisting and we are done. Assume for a contradiction, that no  $t$ -end-to-end twisting exists. A cop-free row is *lonely*, if it is sandwiched by cop-occupied rows. We show that there have to be additional (non-horizontal) roadblocks in each non-lonely row. To do this we construct, for non-lonely rows  $i$  and  $i + 1$ , two 2-periodic paths that only use vertices from rows  $i$  and  $i + 1$ , avoid all horizontal roadblocks, and do not share the same incident edges of any vertex in rows  $i$  and  $i + 1$  (see Figure 2). By Lemma 21, if there are no non-horizontal roadblocks in rows  $i$  and  $i + 1$ , then these path would induce  $t$ -end-to-end twistings. Because the two paths do not use common incident edges, an additional roadblock is required for each one to block the path. This allows us to lower bound the number of roadblocks in terms of  $c$  and to contradict the assumption that  $c \leq \frac{2}{5}k - 1$ . Hence, the desired  $t$ -end-to-end twisting exists. ◀

Using the previous lemma, we are ready to prove the main technical result of this section.

► **Lemma 24.** *Let  $1 \leq t \leq \frac{2}{5}k - 1$  be an integer. Then the robber, initially placed on the left or right end of  $\mathcal{C}$ , has a strategy for the first  $\Omega(J)$  rounds in the compressed and blocking  $(k + t)$ -Cops and Robber game on  $\mathcal{C}$  and  $\equiv^t$ .*

**Proof Sketch.** We will convert all roadblocks into cops and make the game harder for the robber. In this way, we use the notions of  $t$ -critical sets and  $t$ -virtual cordons for these positions. The robber always stays at one end of the grid: If the current position is not critical, the robber stays at the current end, until an announced cop or roadblock (seen as a cop) makes the position critical. Then using the  $t$ -end-to-end twisting from Lemma 22 the robber moves to the end of the grid with larger distance to every minimal  $t$ -virtual cordon. This distance is in  $\Omega(J)$  [19]. If the current position is critical, we show that blocking moves only allow the Cops Player to decrease this distance by  $O(k)$ , via a case distinction on the number of cop-occupied rows. While this is at most  $\frac{2}{5}k - 1$ , the robber can always use the  $t$ -end-to-end twisting given by Lemma 23 to switch ends. Otherwise, the number of cop-occupied rows is at least  $\frac{2}{5}k$ . In this case, all intermediate positions between the blocking moves share at least one row in which only one and the same cop is placed, so by inductively applying [19, Proposition 4.10], we show that the minimal  $t$ -virtual cordon before and after the blocking moves are contained within  $O(k)$  subsequent columns.

So, starting from a distance of  $\Omega(J)$ , the robber has a strategy such that this distance decreases by at most  $O(k)$  in each round. Hence, the robber has a strategy for the first  $\Omega(J/O(k)) = \Omega(J)$  rounds (since  $k$  is seen as a constant).  $\blacktriangleleft$

Finally, for sufficiently large  $n$  and choosing  $w = \lceil \sqrt[t+1]{n} \rceil$ , Lemmas 24, 14, 19, and 18 together imply the desired round lower bound for the  $(k+t)$ -pebble game with blocking.

► **Theorem 25.** *For all integers  $k \geq 3$ ,  $1 \leq t \leq \frac{2}{5}k - 1$ , and  $n \in \mathbb{N}$ , there are two colored graphs  $\mathcal{G}$  and  $\mathcal{H}$  of order  $\Theta(n)$  and color class size 8 such that*

1.  $\mathcal{G} \not\preceq^{k+1} \mathcal{H}$ , that is, Spoiler wins the  $(k+1)$ -pebble game on  $\mathcal{G}, \mathcal{H}$ , and
2.  $\mathcal{G} \preceq_{\mathcal{B}}^{k+t, \Omega(n^{k/(t+1)})} \mathcal{H}$ , that is, Duplicator has a strategy for the first  $\Omega(n^{k/(t+1)})$  rounds in the  $(k+t)$ -pebble game with blocking on  $\mathcal{G}, \mathcal{H}$ .

## 7 Supercritical Width versus Tree-Like Size Trade-Offs

We finally derive our main results; starting with narrow resolution.

► **Theorem 26.** *For all integers  $k \geq 3$ ,  $1 \leq t \leq \frac{2}{5}k - 1$ , and  $n \in \mathbb{N}$ , there are two colored graphs  $\mathcal{G}$  and  $\mathcal{H}$  of order  $\Theta(n)$  and color class size 16 such that*

1. *there is a  $k$ -narrow resolution refutation of  $\text{ISO}(\mathcal{G}, \mathcal{H})$ , and*
2. *every  $(k+t-1)$ -narrow tree-like resolution refutation of  $\text{ISO}(\mathcal{G}, \mathcal{H})$  has size  $2^{\Omega(n^{k/(t+1)})}$ .*

**Proof.** Let  $k \geq 3$  and  $1 \leq t \leq \frac{2}{5}k - 1$ . By Theorem 25, for all  $n \in \mathbb{N}$ , there are graphs  $\mathcal{G}$  and  $\mathcal{H}$  of color class size 8 and order  $\Theta(n)$  such that  $\mathcal{G} \not\preceq^{k+1} \mathcal{H}$  and  $\mathcal{G} \preceq_{\mathcal{B}}^{k+t, \Omega(n^{k/(t+1)})} \mathcal{H}$ . It is easy to see that  $\mathcal{X}(\mathcal{G})$  and  $\mathcal{X}(\mathcal{H})$  have color class size 16. By Theorem 5 and Lemma 6, there is a  $k$ -narrow resolution refutation for  $\text{ISO}(\mathcal{X}(\mathcal{G}), \mathcal{X}(\mathcal{H}))$ . Moreover, from Lemma 9 it follows that Delayer has a strategy to score  $\Omega(n^{k/(t+1)})$  points in the  $(k+t)$ -narrow Prover-Delayer game on  $\mathcal{X}(\mathcal{G}), \mathcal{X}(\mathcal{H})$ . Therefore, by Lemma 4, the result follows.  $\blacktriangleleft$

**Theorem 1** is the case  $t = 1$  of Theorem 26. We now lift Theorem 26 to usual resolution (without the narrow resolution rule). First, if  $\mathcal{G}$  and  $\mathcal{H}$  have color class size  $c$ , then we can convert every  $k$ -narrow refutation of  $\text{ISO}(\mathcal{G}, \mathcal{H})$  into a (usual) refutation of  $\text{ISO}(\mathcal{G}, \mathcal{H})$  of width  $k+c$ . Second, a width- $k$  refutation is in particular a width- $k$  narrow refutation.

**Theorem 2** follows immediately. Note that while Assertion 2 of Theorem 2 provides a lower bound for all  $t \leq \frac{2}{5}k - 1$ , Assertion 1 only guarantees a refutation of width  $k+16$ . Therefore, the existing refutation must be large only for  $k \geq 45$  and  $17 \leq t \leq \frac{2}{5}k - 1$ .

**Conclusion and Open Questions.** We established a new super-critical (narrow) width vs. tree-like size trade-off on graph isomorphism formulas for resolution. The lower bound of  $2^{\Omega(n^{k/2})}$  obtained for  $t = 1$  in Theorems 2 and 26 is close to the upper bound of  $2^{n^k}$  for the tree-like size of resolution of (narrow) width  $k$ . We exploited a compressed variant of the CFI graphs and round number lower bounds in the  $k$ -pebble game on them. However, we had to move from the  $k$ -pebble game to the  $k$ -pebble game with blocking, and reprove the round number lower bounds in this setting. This raises the question of whether there is a generic translation from round number lower bounds in the  $k$ -pebble game to tree-like size resolution lower bounds. Another question is whether the decrease in the robustness in the trade-off from  $2k$  in [19] to  $\frac{7}{5}k$  in Theorem 26 is necessary. More broadly, we ask for a more robust compression or trade-off that can be applied to a much wider range than  $2k$ .

## References

- 1 Albert Atserias and Víctor Dalmau. A combinatorial characterization of resolution width. *J. Comput. Syst. Sci.*, 74(3):323–334, 2008. doi:10.1016/J.JCSS.2007.06.025.
- 2 Albert Atserias, Meena Mahajan, Jakob Nordström, and Alexander Razborov. Proof complexity and beyond. *Oberwolfach Report*, 2024. Workshop held 24–29 March 2024. doi:10.14760/OWR-2024-15.
- 3 Albert Atserias and Elitza N. Maneva. Sherali-Adams relaxations and indistinguishability in counting logics. *SIAM J. Comput.*, 42(1):112–137, 2013. doi:10.1137/120867834.
- 4 László Babai. Graph isomorphism in quasipolynomial time [extended abstract]. In *48th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2016, Cambridge, MA, USA, June 18-21, 2016*, pages 684–697. ACM, 2016. doi:10.1145/2897518.2897542.
- 5 Paul Beame, Chris Beck, and Russell Impagliazzo. Time-space trade-offs in resolution: Superpolynomial lower bounds for superlinear space. *SIAM J. Comput.*, 45(4):1612–1645, 2016. doi:10.1137/130914085.
- 6 Chris Beck, Jakob Nordström, and Bangsheng Tang. Some trade-off results for polynomial calculus: extended abstract. In *Symposium on Theory of Computing Conference, STOC’13, Palo Alto, CA, USA, June 1-4, 2013*, pages 813–822. ACM, 2013. doi:10.1145/2488608.2488711.
- 7 Eli Ben-Sasson, Russell Impagliazzo, and Avi Wigderson. Near optimal separation of tree-like and general resolution. *Comb.*, 24(4):585–603, 2004. doi:10.1007/S00493-004-0036-5.
- 8 Eli Ben-Sasson and Jakob Nordström. Short proofs may be spacious: An optimal separation of space and length in resolution. In *49th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2008, October 25-28, 2008, Philadelphia, PA, USA*, pages 709–718. IEEE Computer Society, 2008. doi:10.1109/FOCS.2008.42.
- 9 Eli Ben-Sasson and Jakob Nordström. Understanding space in proof complexity: Separations and trade-offs via substitutions. In *Innovations in Computer Science - ICS 2011, Tsinghua University, Beijing, China, January 7-9, 2011. Proceedings*, pages 401–416. Tsinghua University Press, 2011. URL: <http://conference.iis.tsinghua.edu.cn/ICS2011/content/papers/3.html>.
- 10 Eli Ben-Sasson and Avi Wigderson. Short proofs are narrow - resolution made simple. In *Proceedings of the Thirty-First Annual ACM Symposium on Theory of Computing, May 1-4, 1999, Atlanta, Georgia, USA*, pages 517–526. ACM, 1999. doi:10.1145/301250.301392.
- 11 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. doi:10.1109/FOCS.2012.48.
- 12 Christoph Berkholz and Martin Grohe. Limitations of algebraic approaches to graph isomorphism testing. In *Automata, Languages, and Programming - 42nd International Colloquium, ICALP 2015, Kyoto, Japan, July 6-10, 2015, Proceedings, Part I*, volume 9134 of *Lecture Notes in Computer Science*, pages 155–166. Springer, 2015. doi:10.1007/978-3-662-47672-7\_13.
- 13 Christoph Berkholz and Martin Grohe. Linear diophantine equations, group CSPs, and graph isomorphism. In *Proceedings of the Twenty-Eighth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2017, Barcelona, Spain, Hotel Porta Fira, January 16-19*, pages 327–339. SIAM, 2017. doi:10.1137/1.9781611974782.21.
- 14 Christoph Berkholz, Moritz Lichter, and Harry Vinall-Smeeth. Supercritical size-width tree-like resolution trade-offs for graph isomorphism. *CoRR*, 2024. arXiv preprint. doi:10.48550/arXiv.2407.17947.
- 15 Christoph Berkholz and Jakob Nordström. Near-optimal lower bounds on quantifier depth and Weisfeiler-Leman refinement steps. In *31st Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2016, New York, NY, USA, July 5-8, 2016*, pages 267–276, 2016. doi:10.1145/2933575.2934560.

- 16 Christoph Berkholz and Jakob Nordström. Supercritical space-width trade-offs for resolution. *SIAM J. Comput.*, 49(1):98–118, 2020. doi:10.1137/16M1109072.
- 17 Jin-yi Cai, Martin Fürer, and Neil Immerman. An optimal lower bound on the number of variables for graph identification. *Combinatorica*, 12(4):389–410, 1992. doi:10.1007/BF01305232.
- 18 Anuj Dawar, Erich Grädel, and Moritz Lichter. Limitations of the invertible-map equivalences. *J. Log. Comput.*, September 2022. doi:10.1093/logcom/exac058.
- 19 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. *CoRR*, abs/2411.14267, 2024. arXiv preprint. doi:10.48550/arXiv.2411.14267.
- 20 Martin Fürer. Weisfeiler-Lehman refinement requires at least a linear number of iterations. In *28th International Colloquium on Automata, Languages, and Programming, ICALP 2001, Crete, Greece, July 8-12, 2001, Proceedings*, volume 2076 of *Lecture Notes in Computer Science*, pages 322–333. Springer, 2001. doi:10.1007/3-540-48224-5\_27.
- 21 Nicola Galesi and Neil Thapen. Resolution and pebbling games. In *Theory and Applications of Satisfiability Testing, 8th International Conference, SAT 2005, St. Andrews, UK, June 19-23, 2005, Proceedings*, volume 3569 of *Lecture Notes in Computer Science*, pages 76–90. Springer, 2005. doi:10.1007/11499107\_6.
- 22 Erich Grädel, Martin Grohe, Benedikt Pago, and Wied Pakusa. A finite-model-theoretic view on propositional proof complexity. *Log. Methods Comput. Sci.*, 15(1), 2019. doi:10.23638/LMCS-15(1:4)2019.
- 23 Martin Grohe. Fixed-point definability and polynomial time on graphs with excluded minors. *J. ACM*, 59(5):27:1–27:64, 2012. doi:10.1145/2371656.2371662.
- 24 Martin Grohe, Moritz Lichter, and Daniel Neuen. The iteration number of the Weisfeiler-Leman algorithm. *ACM Trans. Comput. Log.*, 26(1):6:1–6:31, 2025. doi:10.1145/3708891.
- 25 Martin Grohe, Moritz Lichter, Daniel Neuen, and Pascal Schweitzer. Compressing CFI graphs and lower bounds for the Weisfeiler-Leman refinements. In *64th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2023, Santa Cruz, CA, USA, November 6-9, 2023*, pages 798–809. IEEE, 2023. doi:10.1109/FOCS57990.2023.00052.
- 26 Martin Grohe and Daniel Neuen. Recent advances on the graph isomorphism problem. In *Surveys in Combinatorics, 2021: Invited lectures from the 28th British Combinatorial Conference, Durham, UK, July 5-9, 2021*, pages 187–234. Cambridge University Press, 2021. doi:10.1017/9781009036214.006.
- 27 Martin Grohe and Daniel Neuen. Isomorphism for tournaments of small twin width. In *51st International Colloquium on Automata, Languages, and Programming, ICALP 2024, July 8-12, 2024, Tallinn, Estonia*, volume 297 of *LIPICs*, pages 78:1–78:20. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2024. doi:10.4230/LIPICs.ICALP.2024.78.
- 28 Martin Grohe and Martin Otto. Pebble games and linear equations. *J. Symb. Log.*, 80(3):797–844, 2015. doi:10.1017/JSL.2015.28.
- 29 Neil Immerman. Upper and lower bounds for first order expressibility. *J. Comput. Syst. Sci.*, 25(1):76–98, 1982. doi:10.1016/0022-0000(82)90011-3.
- 30 Richard M. Karp. Reducibility among combinatorial problems. In *Proceedings of a symposium on the Complexity of Computer Computations, held March 20-22, 1972, at the IBM Thomas J. Watson Research Center, Yorktown Heights, New York, USA*, The IBM Research Symposia Series, pages 85–103. Plenum Press, New York, 1972. doi:10.1007/978-1-4684-2001-2\_9.
- 31 Moritz Lichter. Witnessed symmetric choice and interpretations in fixed-point logic with counting. In *50th International Colloquium on Automata, Languages, and Programming (ICALP 2023)*, volume 261 of *LIPICs*, pages 133:1–133:20. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2023. doi:10.4230/LIPICs.ICALP.2023.133.
- 32 Ryan O’Donnell, John Wright, Chenggang Wu, and Yuan Zhou. Hardness of robust graph isomorphism, Lasserre gaps, and asymmetry of random graphs. In *Proceedings of the Twenty-*

- Fifth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2014, Portland, Oregon, USA, January 5-7, 2014*, pages 1659–1677. SIAM, 2014. doi:10.1137/1.9781611973402.120.
- 33 Benedikt Pago. Finite model theory and proof complexity revisited: Distinguishing graphs in Choiceless Polynomial Time and the extended polynomial calculus. In *31st EACSL Annual Conference on Computer Science Logic, CSL 2023, February 13-16, 2023, Warsaw, Poland*, volume 252 of *LIPIcs*, pages 31:1–31:19. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2023. doi:10.4230/LIPICS.CSL.2023.31.
  - 34 Pavel Pudlák and Russell Impagliazzo. A lower bound for DLL algorithms for  $k$ -SAT (preliminary version). In *Proceedings of the Eleventh Annual ACM-SIAM Symposium on Discrete Algorithms, January 9-11, 2000, San Francisco, CA, USA*, pages 128–136. ACM/SIAM, 2000. URL: <http://dl.acm.org/citation.cfm?id=338219.338244>.
  - 35 Alexander A. Razborov. A new kind of tradeoffs in propositional proof complexity. *J. ACM*, 63(2):16:1–16:14, 2016. doi:10.1145/2858790.
  - 36 Pascal Schweitzer and Constantin Seebach. Resolution with symmetry rule applied to linear equations. In *38th International Symposium on Theoretical Aspects of Computer Science, STACS 2021, March 16-19, 2021, Saarbrücken, Germany (Virtual Conference)*, volume 187 of *LIPIcs*, pages 58:1–58:16. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2021. doi:10.4230/LIPICS.STACS.2021.58.
  - 37 Paul D. Seymour and Robin Thomas. Graph searching and a min-max theorem for tree-width. *J. Comb. Theory, Ser. B*, 58(1):22–33, 1993. doi:10.1006/jctb.1993.1027.
  - 38 Neil Thapen. A tradeoff between length and width in resolution. *Theory Comput.*, 12(1):1–14, 2016. doi:10.4086/TOC.2016.V012A005.
  - 39 Jacobo Torán. On the hardness of graph isomorphism. *SIAM J. Comput.*, 33(5):1093–1108, 2004. doi:10.1137/S009753970241096X.
  - 40 Jacobo Torán. On the resolution complexity of graph non-isomorphism. In *Theory and Applications of Satisfiability Testing - SAT 2013 - 16th International Conference, Helsinki, Finland, July 8-12, 2013. Proceedings*, volume 7962 of *Lecture Notes in Computer Science*, pages 52–66. Springer, 2013. doi:10.1007/978-3-642-39071-5\_6.
  - 41 Jacobo Torán and Florian Würz. Cutting planes width and the complexity of graph isomorphism refutations. In *26th International Conference on Theory and Applications of Satisfiability Testing, SAT 2023, July 4-8, 2023, Alghero, Italy*, volume 271 of *LIPIcs*, pages 26:1–26:20. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2023. doi:10.4230/LIPICS.SAT.2023.26.
  - 42 Jacobo Torán and Florian Würz. Number of variables for graph differentiation and the resolution of graph isomorphism formulas. *ACM Trans. Comput. Log.*, 24(3):23:1–23:25, 2023. doi:10.1145/3580478.
  - 43 Alasdair Urquhart. The depth of resolution proofs. *Stud Logica*, 99(1-3):349–364, 2011. doi:10.1007/S11225-011-9356-9.