Electronic Colloquium on Computational Complexity, Report No. 63 (2023)

Cutting Planes Width and the Complexity of Graph Isomorphism Refutations

Jacobo Torán and Florian Wörz

Universität Ulm, Germany
{jacobo.toran, florian.woerz}@uni-ulm.de

May 2, 2023

Abstract

The width complexity measure plays a central role in Resolution and other propositional proof systems like Polynomial Calculus (under the name of degree). The study of width lower bounds is the most extended method for proving size lower bounds, and it is known that for these systems, proofs with small width also imply the existence of proofs with small size. Not much has been studied, however, about the width parameter in the Cutting Planes (CP) proof system, a measure that was introduced by Dantchev and Martin in 2011 under the name of CP cutwidth.

In this paper, we study the width complexity of CP refutations of graph isomorphism formulas. For a pair of non-isomorphic graphs G and H, we show a direct connection between the Weisfeiler–Leman differentiation number $\mathsf{WL}(G, H)$ of the graphs and the width of a CP refutation for the corresponding isomorphism formula $\mathrm{Iso}(G, H)$. In particular, we show that if $\mathsf{WL}(G, H) \leq k$, then there is a CP refutation of $\mathrm{Iso}(G, H)$ with width k, and if $\mathsf{WL}(G, H) > k$, then there are no CP refutations of $\mathrm{Iso}(G, H)$ with width $k-2$. Similar results are known for other proof systems, like Resolution, Sherali–Adams, or Polynomial Calculus. We also obtain polynomial-size CP refutations from our width bound for isomorphism formulas for graphs with constant WL-dimension.

Keywords Cutting Planes · Proof Complexity · Linear Programming · Combinatorial Optimization · Weisfeiler–Leman Algorithm · Graph Isomorphism

Funding Supported by the Deutsche Forschungsgemeinschaft (DFG) under project number 430150230, "Complexity measures for solving propositional formulas".

1 Introduction

Central to the field of combinatorial optimization is the NP-hard problem of finding *integer* solutions to linear programs. This is done by optimizing the linear objective function $\langle \mathbf{c}, \mathbf{x} \rangle$ (for

ISSN 1433-8092

a given vector $\mathbf{c} \in \mathbb{R}^n$) over the set of feasible points $\mathbf{x}$ for the *LP relaxation*, described by a rational polytope of the form

$$P = \{\mathbf{x} \in \mathbb{R}^n \mid \mathbf{A}\mathbf{x} \geq \mathbf{b},\ \mathbf{0} \leq \mathbf{x} \leq \mathbf{1}\},$$

where $\mathbf{A} \in \mathbb{Z}^{m \times n}$ is some integer matrix, and $\mathbf{b} \in \mathbb{Z}^m$ is an integer vector.[1] If the polytope is *integral* (i. e., only contains integer vertices), one can optimize over all *real* vectors in P (i. e., solve the linear relaxation with the *simplex algorithm* in weakly polynomial time). Otherwise, one has to consider the *integral hull* $P^{\mathbb{Z}} := \operatorname{conv}(P \cap \mathbb{Z}^n)$ for the optimization, i. e., the smallest polytope containing the integral points of P. As was already suggested in the 1950s by Gomory [Gom63] and later by Chvátal [Chv73], in such a case, one can iteratively refine the set of feasible solutions by adding further valid constraints described by hyperplanes, or, more precisely, half-spaces, to the set of inequalities describing P. These half spaces still contain $P^{\mathbb{Z}}$ but—hopefully—cut off some parts of P. For this purpose, the *cut rule* adds an inequality of the form $\langle \mathbf{a}, \mathbf{x} \rangle \geq \lceil b \rceil$ with an integral vector $\mathbf{a}$ and a rational number b such that every point of P satisfies the inequality $\langle \mathbf{a}, \mathbf{x} \rangle \geq b$. If b is not an integer, then the former inequality is not valid for (some) fractional solutions but still valid for all integer solutions. This process yields a sequence

$$P \supseteq P^{(1)} \supseteq P^{(2)} \supseteq \cdots \supseteq P^{\mathbb{Z}}$$

of polytopes. If some polytope $P^{(i)}$ in this sequence is empty, P cannot have integer solutions.

Cutting Planes Proof System. Using this idea, Cook et al. [CCT87] introduced the Cutting Planes proof system. In this system, one is initially given a set $\{\sum_{j=1}^{n} a_{i,j} x_j \geq b_i \mid i \in [m]\}$ of integer inequalities describing the polytope P. Using the two deduction rules introduced in Definition 2, one can repeatedly deduce new inequalities, aiming to derive the contradictory inequality $0 \geq 1$. Obtaining a sequence of inequalities ending with $0 \geq 1$ is possible if and only if the initial set of inequalities does not admit an integer solution. This yields the Cutting Planes proof system (formally introduced in Section 2.2).

In particular, CP can be used to refute unsatisfiable CNF formulas (by translating them into affine inequalities). Cutting Planes is a strong proof system that can simulate Resolution, and it is exponentially stronger for several formula classes [CCT87]. Exponential lower bounds on the size of a Cutting Planes proof (as measured in the number of inequalities) have been shown using the interpolation method [Pud97, HC99, HP17] and, more recently, using lifting and communication complexity results [GGKS20] that can be traced back to [IPU94, BEGJ00, HN12].

Other complexity measures for CP have been studied. These measures are defined by the directed acyclic graph representing the proof (one connects the premises with the consequences). The *rank* of a proof is the maximum number of applications of the cut rule along any path in the directed graph. This is known as the *Chvátal rank* in linear optimization (see [Juk12] for an excellent overview in this area) and was introduced in [BGH+06] in the area of proof complexity. This measure is the analogon of *depth* in Resolution [Urq11]. Further, Dantchev and Martin [DM12] introduced the parameter *cutwidth*, defined as the maximum number of variables present in an inequality derived by performing a cut. This measure was further studied in [Raz17] under the name of width, where the author presents linear lower bounds for this measure, as well as width/rank tradeoffs. In the case of Resolution, there is also a related complexity measure

[1] Note that we restrict our attention to polytopes in $[0, 1]^n$ rather than polyhedrons in $\mathbb{R}^n$.

of *width* that measures how many literals are present in the largest clause in a refutation. In Polynomial Calculus, the analogous measure is *degree*. The seminal paper [BW01] showed that proving width lower bounds for Resolution is a way to prove size lower bounds for Resolution. This result extends to the corresponding measures in Polynomial Calculus [CEI96, IPS99]. These papers sparked interest in the width/degree complexity measures, resulting in a long line of papers proving lower bounds for these measures. The situation for CP width lower bounds is dramatically more sparse. We are only aware of the two mentioned references [DM12, Raz17].

In this paper, we study graph isomorphism formulas with respect to the parameters rank and width. This allows us to prove size upper bounds for isomorphism formulas based on graphs with constant Weisfeiler–Leman dimension. We also show lower bounds for these formulas in a subsystem of CP. A strong motivation for this study is that Cutting Planes is a promising candidate to be used in future efficient implementations of SAT solvers. Furthermore, proof complexity results also hold for all integer linear programming solvers based on the Gomory–Chvátal rule. These solvers provide up-to-date methods for solving NP-hard Boolean optimization problems.

Weisfeiler–Leman and Proof Complexity. The graph isomorphism problem (GI), i. e., the task of deciding whether two given graphs are isomorphic, has been intensively studied and is well known for its unresolved complexity, as it is one of the few problems in NP that is not known to be complete for this class nor to be in P. It is also unknown whether GI $\in$ co-NP.

A naïve heuristic to distinguish two non-isomorphic colored graphs is the 1-dimensional Weisfeiler–Leman algorithm (WL), or color refinement algorithm. This algorithm updates the original vertex colors according to the multiset of colors of their neighbors. This basic step is applied repeatedly until the colorings stabilize. This procedure can be generalized to the k-dimensional Weisfeiler–Leman algorithm (k-WL) [WL68, Wei76]. In this more refined variant, the set of k-tuples of vertices is partitioned into automorphism-invariant equivalence classes (see, e. g., [Kie20] for an overview of this procedure). It had been conjectured that GI is solvable using the k-dimensional Weisfeiler–Leman algorithm, with k being sublinear in the number of vertices of the graphs. However, this was shown to be false in the seminal work of Cai, Fürer, and Immerman [CFI92]. Fascinatingly, the authors achieved this by relating the power of k-WL to the expressive power of $\mathscr{C}^k$, the k-variable fragment of first-order logic augmented with counting quantifiers, and a variant of an Ehrenfeucht-Fraïssé game [Fra50, Ehr61] called the bijective k-pebble game. Nevertheless, the Weisfeiler–Leman method still plays a central role in the algorithmic research on GI; for example, Babai's famous algorithm for GI [Bab16] uses the Weisfeiler–Leman method as a subroutine.

The field of proof complexity provides a different approach to studying the complexity of the GI problem. Here, one tries to find the smallest size of a proof of the fact that two graphs are non-isomorphic. It holds that GI is in co-NP if and only if there is a concrete proof system with polynomial-size proofs of non-isomorphism. Similar to the Cook–Reckhow program [CR79] for the unsatisfiability problem UNSAT, this defines a clear line of research trying to provide superpolynomial size lower bounds for refuting graph (non)isomorphism formulas in stronger and stronger proof systems. The situation is even more interesting here than in the SAT case since it was proven in [BM88] that GI is in co-AM, a randomized version of co-NP. Hence, it would not be too surprising if GI $\in$ co-NP, and this would imply the existence of polynomial-size proofs for the problem in some system.

In a recent line of work, the power of different proof systems has been studied with respect to their power in refuting graph isomorphism. The first example of such a lower bound was given in [Tor13] for the Resolution proof system. This result led to lower bounds for stronger proof systems. These studies also make use of the Weisfeiler–Leman algorithm. The authors of [BG15] exactly characterized the power of the Weisfeiler–Leman algorithm in terms of an algebraic proof system between degree-k Nullstellensatz and degree-k Polynomial Calculus. Moreover, it has been shown in [AM13, Mal14, GO15] that the power of k-WL lies between the k-th and $(k+1)$-st level of the canonical Sherali–Adams LP hierarchy [SA90]. Furthermore, it was shown in [OWWZ14] and independently in [CSS14] that pairs of non-isomorphic n-vertex graphs exist such that any Sum-of-Squares proof of non-isomorphism must have degree $\Omega(n)$. Closely related are the results of [AO18] that show that Sum-of-Squares degree and Polynomial Calculus degree correlate to the Weisfeiler–Leman dimension (up to constant factors). Recently, in [TW23], an exact connection was shown between the width and depth measures in (narrow) Resolution and the number of variables and the quantifier depth needed to distinguish a pair of graphs by first-order logic sentences. This result extends to a lower bound for the strong SRC-1 proof system, equipping Resolution with a symmetry rule [Urq99].

1.1 Our Results and Techniques

We show a strong connection between the Weisfeiler–Leman graph differentiation number and the geometric Cutting Planes proof system. We write $G \equiv_k^{\mathrm{CP}} H$ if there is no width-k Cutting Planes refutation of $\mathrm{Iso}(G, H)$, the set of inequalities encoding the statement that the graphs G and H are isomorphic. Further, we write $G \equiv_k^{\mathrm{WL}} H$ if the graphs G and H cannot be distinguished using the logic $\mathscr{C}^k$. Our main result is the following theorem.

Theorem 1 (Main Result)**.** *Let G and H be two non-isomorphic graphs. Then,*

$$G \equiv_k^{\mathrm{CP}} H \implies G \equiv_k^{\mathrm{WL}} H \implies G \equiv_{k-2}^{\mathrm{CP}} H. \tag{1}$$

In other words,

1. *If $\mathsf{WL}(G, H) \leq k$, then $\mathrm{Iso}(G, H)$ can be refuted by Cutting Planes using width k.*
2. *If $\mathsf{WL}(G, H) > k$, then $\mathrm{Iso}(G, H)$ is not refutable in Cutting Planes using width $k - 2$.*

We achieve the first result by using the winning positions of Spoiler in the bijective pebble game to derive the necessary inequalities. The second result is shown by constructing a set of matrices that "protect" a given point in the isomorphism polytope from being cut away using cuts of a certain width. This result is achieved by proving a so-called protection lemma for graph isomorphism. This type of lemmata has a long tradition in combinatorial optimization (see, e. g., [Juk12]) and has also been used in the area of proof complexity in [BGH+06, DM12, Lau16]. The concrete matrices are being constructed using winning positions for Duplicator in the bijective pebble game. From the first result, we can derive polynomial-size CP refutations for isomorphism formulas for graphs with constant WL-dimension.

We also show a size lower bound for refuting graph isomorphism formulas in the subsystem of tree-like Cutting Planes with polynomially bounded coefficients by using known results from communication complexity.

1.2 Organization of This Paper

The remainder of this paper is organized as follows. Section 2 introduces our notation, the Cutting Planes proof system, the Gomory–Chvátal rule, our encoding of graph isomorphism as a set of affine inequalities, and necessary tools from descriptive complexity. We proceed in Section 3 by showing the tight connection between the Weisfeiler–Leman differentiation number for graphs and the width of refuting the corresponding graph isomorphism formulas in the Cutting Planes proof system. Section 4 establishes the lower bound for isomorphism formulas in Tree-CP with polynomially bounded coefficients. Due to space constraints, the proofs of some lemmas are presented in the full-length version of the paper.

2 Preliminaries

2.1 Notation

We let $\mathbb{N}$ denote the set of positive integers, and for $n \in \mathbb{N}$, we define $[n] := \{k \in \mathbb{N} \mid 1 \leq k \leq n\}$. This paper will denote tuples, vectors, and matrices in boldface. Given two vectors $\mathbf{x}, \mathbf{a} \in \mathbb{R}^n$, we let $\langle \mathbf{a}, \mathbf{x} \rangle := \sum_{i=1}^{n} a_i x_i$ denote the standard inner product.

2.2 The Cutting Planes Proof System

In this paper, we consider Cutting Planes as an inference system used for refuting unsatisfiable CNF formulas, as suggested by [CCT87]. For this, a CNF formula F is translated into a system of affine inequalities that have a 0-1-solution if and only if the corresponding assignment satisfies F. These inequalities can then be manipulated according to certain rules. It is known that a formula is unsatisfiable if and only if, applying these rules, it is possible to obtain the contradiction $0 \geq 1$. A clause $C = (\ell_1 \vee \cdots \vee \ell_k)$ is converted to $\tau(C) \equiv [\tau(\ell_1) + \cdots + \tau(\ell_k) \geq 1]$, where for each literal ℓ_i, we let $\tau(\ell_i) := x$ if $\ell_i = x$ and $\tau(\ell_i) := 1 - x$ if $\ell_i = \neg x$. We also add the additional inequalities $x \geq 0$ and $-x \geq -1$ for each variable x, forcing them to take values between 0 and 1 (this is a relaxation of the condition $x \in \{0, 1\}$).

Definition 2. Let $\mathbf{a} \in \mathbb{Z}^n$, $\mathbf{a^i} \in \mathbb{Z}^n, \gamma_i \in \mathbb{Z}$ for $i \in [m]$, and $\mathbf{x}$ be a vector of n variables. The Cutting Planes proof system (CP) has two rules:

Linear combination: From the linear inequalities $\langle \mathbf{a^1}, \mathbf{x} \rangle \geq \gamma_1, \ldots, \langle \mathbf{a^m}, \mathbf{x} \rangle \geq \gamma_m$ and non-negative integers $\alpha_1, \ldots, \alpha_m$, we can derive the inequality $\sum_{i=1}^{m} \alpha_i \langle \mathbf{a^i}, \mathbf{x} \rangle \geq \sum_{i=1}^{m} \alpha_i \gamma_i$.

Rounding: From $\langle \mathbf{a}, \mathbf{x} \rangle \geq \gamma$, if all the coefficients in $\mathbf{a}$ are divisible by a positive integer $b > 0$, then we can derive the inequality $\langle \frac{\mathbf{a}}{b}, \mathbf{x} \rangle \geq \lceil \frac{\gamma}{b} \rceil$.

We can assume, without loss of generality, as done in [BGH⁺06], that a rounding operation is always applied after each application of the linear combination rule and, therefore, both rules can be merged into a single one (called *Gomory–Chvátal cut*, *GC cut* in [BGH⁺06]).

Remark 3. As is standard (see, e. g., [Juk12]), we will sometimes write $a \leq b$ or $-b \leq -a$ for a Cutting Planes inequality of the form $b \geq a$ when it is more natural in our arguments.

Definition 4. A *Cutting Planes refutation* for a set of affine inequalities $f = \{f_1, \ldots, f_m\}$, is a sequence $(g_1, \ldots, g_t)$ of affine inequalities satisfying that

- each g_i is either an inequality in f (an *axiom*) or is obtained from previous inequalities by a GC cut,
- and g_t is the inequality $0 \geq 1$.

It is well-known that all the above-mentioned derivation rules are sound for integer solutions. Furthermore, the proof system is complete in the sense that each unsatisfiable CNF formula has a Cutting Planes refutation (see, e. g., [Chv73]).

A CP refutation can be represented in the usual way as a directed acyclic graph in which each vertex corresponds to an affine inequality in the proof. The axioms are the sources, $0 \geq 1$ is the only sink, and for every application of a GC cut, there is an edge pointing from each of the vertices whose corresponding inequalities are involved in the cut to the vertex representing the result of the cut. The most common complexity measure for a CP refutation is its *size*, defined as the number of vertices in the refutation graph. Two other complexity measures play a central role in our results:

Definition 5. The *rank* of a CP refutation (also called *depth*) is the length of the longest path from an axiom to the $0 \geq 1$ inequality in the refutation graph.

The *cutwidth*, or just *width*, of a CP refutation is the maximum number of variables in an inequality that results from a GC cut. By this, we mean the number of variables remaining after the linear combination in the rule has been performed or, equivalently, the number of variables after the GC cut (linear combination plus rounding) has been done. If no GC cut is used, we consider the cutwidth to be 0.

For any complexity measure $\mathcal{C}$ and any unsatisfiable system of affine inequalities f, the $\mathcal{C}$-*complexity* of f is the minimum value of $\mathcal{C}$ over all CP refutations of f.

2.3 Two Sets of Affine Inequalities for Graph Isomorphism

We only deal *undirected simple graphs*. Such a graph is a tuple $G = (V_G, E_G)$, where V_G is a finite set of *vertices* and $E_G \subseteq \binom{V_G}{2}$ is the set of *edges*. For a vertex v in a graph G, we denote by $N_G(v)$ the set of its neighbors, and for a set of vertices S, we define $N_G(S)$ as the set of neighbors of the vertices in S. If the graph is clear from the context, we drop the subscripts.

Two graphs $G = (V_G, E_G)$ and $H = (V_H, E_H)$ are *isomorphic* if there is a bijection $\varphi\colon V_G \to V_H$ (called *isomorphism from G to H*) such that $\{u, v\} \in E_G \iff \{\varphi(u), \varphi(v)\} \in E_H$ holds for all $u, v \in V_G$. We will denote this by $G \cong H$.

Let $G = (V_G, E_G)$ and $H = (V_H, E_H)$ be two graphs with $V_G = V_H = \{1, \dots, n\}$. We will use the set of variables $x_{i,j}$ with $i, j \in [n]$. If $x_{i,j}$ is greater than 0, this indicates that vertex i in G is mapped to vertex j in H.

For convenience, we consider two different sets of inequalities for which there is a satisfying integer assignment if and only if there is an isomorphism between G and H. The first set of affine inequalities is the one usually used in linear optimization. Let $\mathbf{A}$ and $\mathbf{B}$ be the adjacency matrices of the graphs G and H. The graphs are isomorphic if and only if there is a permutation matrix $\mathbf{X}$ satisfying $\mathbf{AX} = \mathbf{XB}$. This is expressed by the following sets of inequalities. To keep the following definition concise, we write two inequalities $a \leq b$ and $b \leq a$ as the equality $a = b$.

Definition 6 (MIso Formulas)**.** The set of affine inequalities $\mathrm{MIso}(G, H)$ (for matrix isomorphism) contains the following axioms:

Type 1 axioms: For every $v \in V_G$ the equality $\sum_{w\in V_H} x_{v,w} = 1$; and for every $w \in V_H$ the equality $\sum_{v\in V_G} x_{v,w} = 1$. Applied to the matrix $\mathbf{X}$, these axioms mean that the sum of each row as well as the sum of each column is one.

Type 2 axioms: These encode the matrix product $\mathbf{AX} = \mathbf{XB}$. For each position $(i, j) \in [n]^2$, we have the equality $(\mathbf{AX})_{i,j} = (\mathbf{XB})_{i,j}$, or alternatively $\sum_{k\in N(i)} x_{k,j} = \sum_{\ell\in N(j)} x_{i,\ell}$.

Type 3 axioms: These are for every variable x the CP axioms $x \le 1$ and $x \ge 0$.

An alternative set of affine inequalities over the same set of variables is sometimes more convenient and has been used before for encoding the isomorphism principle in other proof systems like Resolution [Tor13, SS21, TW23] or Polynomial Calculus [BG15]. Instead of the inequalities for the matrices, for every two pairs of vertices $v, v' \in V_G$ and $w, w' \in V_H$ such that (v, v') is an edge in G and (w, w') is not an edge in H (or the other way around) we include an inequality indicating that v is not mapped to w or v' is not mapped to w'.

Definition 7 (Iso Formulas)**.** The set $\mathrm{Iso}(G, H)$ contains the following inequalities:

Type 1 and Type 3 axioms: These are exactly the same as in the MIso formulas.

Type 2 axioms: For every $v, v' \in V_G$ and $w, w' \in V_H$ such that $\{(v, w), (v', w')\}$ is not an isomorphism in the graphs induced by $\{v, v'\}$ and $\{w, w'\}$, the inequality $x_{v,w} + x_{v',w'} \le 1$, indicating that an edge cannot be mapped to a non-edge or vice-versa.

Both systems of inequalities have the same set of 0-1 solutions, which encode the isomorphisms between G and H but can have different sets of fractional solutions. For example, setting all variables $x_{i,j}$ to $\frac{1}{n}$ is always a solution for $\mathrm{Iso}(G, H)$ (even when the graphs are non-isomorphic) but only satisfies $\mathrm{MIso}(G, H)$ when these are regular graphs. A fractional isomorphism is a solution that satisfies the MIso formulas but is not necessarily integral.

Definition 8. The graphs G and H are *fractional isomorphic* if there exists a doubly stochastic matrix $\mathbf{P}$ with $\mathbf{AP} = \mathbf{PB}$, where $\mathbf{A}$ and $\mathbf{B}$ are the adjacency matrices of G and H, respectively. The matrix $\mathbf{P}$ is then called *fractional isomorphism* between G and H.

We show that there are short CP derivations of each set of inequalities from the other, although, for the derivation of $\mathrm{MIso}(G, H)$ from $\mathrm{Iso}(G, H)$, we need to use the CG-cut rule.

Lemma 9. *There is a polynomial-size* CP *derivation of the set of inequalities* $\mathrm{Iso}(G, H)$ *from* $\mathrm{MIso}(G, H)$ *without using the GC cut rule.*

Proof. We show how to derive a Type 2 inequality $x_{i,j} + x_{k,\ell} \le 1$ from $\mathrm{MIso}(G, H)$ for the case in which $(i, k) \in E_G$ but $(j, \ell) \notin E_H$. Starting from $\sum_{a\in N(k)} x_{a,j} \le \sum_{b\in N(j)} x_{k,b}$, we add the axiom inequality $-1 \le -\sum_{b\in[n]} x_{k,b}$, obtaining

$$\sum_{a\in N(k)} x_{a,j} - 1 \le -\sum_{b\in \overline{N(j)}} x_{k,b}.$$

This last inequality can be rewritten as

$$x_{i,j} + x_{k,\ell} + \sum_{a\in N(k)\setminus\{i\}} x_{a,j} + \sum_{b\in \overline{N(j)}\setminus\{\ell\}} x_{k,b} \le 1.$$

Adding the axioms $-x_{a,j} \le 0$ and $-x_{k,b} \le 0$ for $a \in N(k) \setminus \{i\}$ and for $b \in \overline{N(j)} \setminus \{\ell\}$, we obtain the result. □

Since fractional solutions can only be eliminated in CP using the GC cut rule, this result implies that the set of solutions of $\mathrm{MIso}(G, H)$ is included in the set of solutions of $\mathrm{Iso}(G, H)$. We consider a derivation in the other direction:

Lemma 10. *For any two connected graphs G, H with maximum degree d, there is a polynomial-size CP derivation with rank 2 and width $2d$ of the set of inequalities $\mathrm{MIso}(G, H)$ from $\mathrm{Iso}(G, H)$.*

Proof. For $i, j \in [n]$, we show how to derive a Type 2 inequality like

$$\sum_{a \in N(i)} x_{a,j} \geq \sum_{b \in N(j)} x_{i,b}.$$

The inequality in the other direction is completely analogous. For $a \in \overline{N(i)}$, adding the axioms $x_{a,j} + x_{i,b} \leq 1$ from $\mathrm{Iso}(G, H)$ for $b \in N(j)$, we obtain

$$|N(j)| \cdot x_{a,j} + \sum_{b \in N(j)} x_{i,b} \leq |N(j)|. \tag{2}$$

From the axioms $\sum_{b \in [n]} x_{i,b} \leq 1$ and $-x_{i,b} \leq 0$, we can obtain $\sum_{b \in N(j)} x_{i,b} \leq 1$, which multiplied times $|N(j)| - 1$ and added to (2) becomes

$$|N(j)| \cdot x_{a,j} + |N(j)| \sum_{b \in N(j)} x_{i,b} \leq 2 \cdot |N(j)| - 1.$$

Dividing by $|N(j)|$ and rounding we obtain

$$x_{a,j} + \sum_{b \in N(j)} x_{i,b} \leq 1.$$

We can derive such an inequality for all $a \in \overline{N(i)}$. Adding them all, we obtain

$$\sum_{a \in \overline{N(i)}} x_{a,j} + |\overline{N(i)}| \sum_{b \in N(j)} x_{i,b} \leq |\overline{N(i)}|.$$

Together with the axiom $-\sum_{a \in [n]} x_{a,j} \leq -1$, this becomes

$$-\sum_{a \in N(i)} x_{a,j} + |\overline{N(i)}| \sum_{b \in N(j)} x_{i,b} \leq |\overline{N(i)}| - 1.$$

We can now add the axioms $-x_{a,j} \leq 0$ for $a \in N(i)$, multiplied times $|\overline{N(i)}| - 1$, reaching

$$-|\overline{N(i)}| \sum_{a \in N(i)} x_{a,j} + |\overline{N(i)}| \sum_{b \in N(j)} x_{i,b} \leq |\overline{N(i)}| - 1.$$

Dividing by $|\overline{N(i)}|$ and rounding we get $\sum_{b \in N(j)} x_{i,b} \leq \sum_{a \in N(i)} x_{a,j}$. In this last rounding step, there are $|N(i)| + |N(j)|$ variables in the inequality. ☐

2.4 The Weisfeiler–Leman Number and the Bijective k-Pebble Game

In order to express different properties of graphs by certain fragments of first-order logic sentences, Immerman introduced the following definition.

Definition 11 ([Imm82, Imm99]). For a logic $\mathscr{L}$ (of first-order logic sentences), the graphs G and H are *$\mathscr{L}$-equivalent*, denoted by $G \equiv_{\mathscr{L}} H$, if for all sentences $\psi \in \mathscr{L}$ it holds that

$$G \vDash \psi \Longleftrightarrow H \vDash \psi.$$

Otherwise, we say that $\mathscr{L}$ can *distinguish* G from H, denoted by $G \not\equiv_{\mathscr{L}} H$.

For $n \in \mathbb{N}$, we introduce a *counting quantifier* $\exists^{\geq n}$. The formula $\exists^{\geq n} x\, \psi$ has the meaning that "there are at least n distinct x satisfying ψ". We also need the notion of quantifier depth (also called quantifier rank).

Definition 12 ([Lib04]). The *quantifier depth* of a formula ψ is defined inductively as follows:

- If ψ is atomic, then $\mathrm{qd}(\psi) = 0$;
- $\mathrm{qd}(\neg\psi) = \mathrm{qd}(\psi)$;
- $\mathrm{qd}(\psi_1 \vee \psi_2) = \max\{\,\mathrm{qd}(\psi_1), \mathrm{qd}(\psi_2)\}$;
- $\mathrm{qd}(\exists^{\geq n} x\, \psi) = \mathrm{qd}(\psi) + 1$.

Definition 13. The *k-variable counting logic $\mathscr{C}^k$* is the set of first-order logic formulas that use counting quantifiers but at most k different variables (possibly re-quantifying them). Further, $\mathscr{C}^k_r$ is the subclass of $\mathscr{C}^k$ where the quantifier depth in the formulas is restricted to r.

For example, $\exists x\big[\exists^{\geq 8} y\, E(x,y) \wedge \forall y\big(E(x,y) \to \exists^{\geq 2} x\, E(y,x)\big)\big]$ lies in $\mathscr{C}^2_3$ and says that there is a vertex that has at least 8 neighbors, each of which has at least 2 neighbors themselves.

Definition 14. The *Weisfeiler–Leman differentiation number* of two graphs G and H is defined by

$$\mathsf{WL}(G,H) := \begin{cases} \min\{k \in \mathbb{N} \mid G \not\equiv_{\mathscr{C}^k} H\} & \text{if } G \not\cong H \\ \infty & \text{if } G \cong H. \end{cases}$$

For a graph G, we say that it has *Weisfeiler–Leman dimension* at most k if and only if $G \not\equiv_{\mathscr{C}^{k+1}} H$ for all graphs H non-isomorphic to G.

Let G and H be two graphs for the remainder of this section. We describe the r-round bijective k-pebble game of Hella [Hel96], adapting the excellent notation from [AM13]. This game can be used to test $\mathscr{C}^k_r$-equivalence. We first describe some notation and the concept of partial isomorphism before proceeding to introduce the game itself.

Notation 15. Let $k \in \mathbb{N}$. Suppose $\mathbf{v} = (v_1, \ldots, v_k) \in (V_G \cup \{\star\})^k$. For $i \in [k]$ and $v \in V_G \cup \{\star\}$, we let $\mathbf{v}[i/v]$ denote the tuple $(v_1, \ldots, v_{i-1}, v, v_{i+1}, \ldots, v_k)$. Further, we let $|\mathbf{v}|_\star$ denote the *number of stars* in the tuple $\mathbf{v}$.

Definition 16. Let $k \in \mathbb{N}$ and let $\mathbf{v} = (v_1, \ldots, v_k) \in (V_G \cup \{\star\})^k$ and $\mathbf{w} = (w_1, \ldots, w_k) \in (V_H \cup \{\star\})^k$ be two k-tuples. We say that the pair $(\mathbf{v}, \mathbf{w})$ *induces/is a partial isomorphism* between G and H if, for every $i, j \in [k]$ we have:

1. $v_i = \star$ if and only if $w_i = \star$;
2. $v_i = v_j$ if and only if $w_i = w_j$;
3. $\{v_i, v_j\} \in E_G$ if and only if $\{w_i, w_j\} \in E_H$.

In the following game, Spoiler wants to exhibit a difference between the given graphs, while Duplicator tries to disguise such a difference by maintaining a partial isomorphism.

Definition 17. Let $k, r \in \mathbb{N}$. The *r-round bijective k-pebble game* on the graphs G and H is played by two players, called *Spoiler* and *Duplicator*. There are k pairs of matched pebbles in the game. The game proceeds in rounds. The game position after round r is finished can be represented by a pair $(\mathbf{v}, \mathbf{w}) \in (V_G \cup \{\star\})^k \times (V_H \cup \{\star\})^k$. The game starts with some initial position $(\mathbf{v^0}, \mathbf{w^0})$. If this initial tuple does not induce a partial isomorphism between the graphs, Spoiler wins the game after 0 rounds. We now describe the round $r+1$ of the game. For this, we suppose that the position after round r is given by $(\mathbf{v}, \mathbf{w})$.

- If $|\mathbf{v}|_\star = |\mathbf{w}|_\star = 0$, Spoiler must choose a position $i \in [k]$ (otherwise, he can still opt to do this deletion step). The tuples are updated to $\mathbf{v}[i/\star]$ and $\mathbf{w}[i/\star]$.
- Duplicator then chooses a bijection $\varphi\colon V_G \to V_H$ (if no such bijection exists, she has lost).
- Spoiler picks a vertex $v \in V_G$ and a position $i \in [k]$ such that $v_i = w_i = \star$, and the tuples are updated to $\mathbf{v}[i/v]$ and $\mathbf{w}[i/\varphi(v)]$.

If the new $(\mathbf{v}, \mathbf{w})$ does not induce a local isomorphism, then *Spoiler has won after $r+1$ rounds*. Otherwise, the game continues with the next round. We say that *Duplicator has a winning strategy* if she can make the game last indefinitely.

It was shown in [CFI92, Hel96] that $\mathsf{WL}(G, H) \leq k$ if and only if Spoiler has a winning strategy for the bijective k-pebble game on G and H starting from the initial position $(\mathbf{v}, \mathbf{w})$ with $\mathbf{v} = \mathbf{w} = (\star, \dots, \star)$.

3 CP Refutations for Isomorphism Formulas

We fix two graphs G and H. For the remainder of this paper, it is sometimes convenient to use an alternative view of the pebbling configurations used in Section 2.4.

Definition 18 (zip Operator)**.** Let $k \in \mathbb{N}$ and let $\mathbf{v} = (v_1, \dots, v_k) \in (V_G \cup \{\star\})^k$ and $\mathbf{w} = (w_1, \dots, w_k) \in (V_H \cup \{\star\})^k$. We write

$$p = \mathrm{zip}(\mathbf{v}, \mathbf{w})$$

to denote the set $p \subseteq V_G \times V_H$ given by

$$p := \{(v_i, w_i) \mid i \in [k] \text{ such that } v_i \neq \star \text{ and } w_i \neq \star\}.$$

Definition 16 can easily be adapted to game positions denoted in the way above.

Notation 19. Let $k, r \in \mathbb{N}$. For a game position $p \subseteq V_G \times V_H$, we write $p \in D^k(G, H)$ if p is a winning position for Duplicator in the k-bijective game played on G and H. Similarly, the set $D^k_r(G, H)$ is defined for the positions in which Duplicator does not lose in r rounds in the game. We use the notation $S^k_r(G, H)$ to denote winning positions for Spoiler in the respective game.

As in [AM13, BG15], we now define an equivalence relation on $(V_G \cup \{\star\})^k \cup (V_H \cup \{\star\})^k$.

Definition 20 ([AM13, BG15])**.** Let $k \in \mathbb{N}$. Further, let G and H be two graphs and let $K, K' \in \{G, H\}$, not necessarily distinct. Additionally, let $\mathbf{u} \in (V_K \cup \{\star\})^k$ and $\mathbf{u}' \in (V_{K'} \cup \{\star\})^k$. We write $\mathbf{u} \equiv_{D^k} \mathbf{u}'$ if $p := \mathrm{zip}(\mathbf{u}, \mathbf{u}') \in D^k(K, K')$.

It was shown in [AM13, Lemma 3] that $\equiv_{D^k}$ is an equivalence relation.

3.1 Constructing a CP Refutation from the Bijective Pebble Game

We show that if a pair (G,H) of non-isomorphic graphs can be separated by the bijective k-pebble game in r rounds, then there is a CP refutation for $\mathrm{Iso}(G,H)$ having width k and rank r simultaneously. By Lemma 9, the same result holds for the $\mathrm{MIso}(G,H)$ formulas. We use the equivalence relation $\equiv_{D^k}$ to define a bipartite graph with certain properties.

Definition 21. Let $p \subseteq V_G \times V_H$ be an initial position of the bijective pebble game played on the graphs G and H. The bipartite graph $B_r^k(p)$ is defined as $B := B_r^k(p) = (V_G \uplus V_H, E_B)$ with edge set

$$E_B := \Big\{ \{v,w\} \,\Big|\, p \cup \{(v,w)\} \notin S_r^k(G,H) \Big\}.$$

We need the following result from [BG15]:

Lemma 22. *Suppose that Spoiler has a winning position for the bijective k-pebble game played on the graphs G and H in $r+1$ rounds starting from position p. In the graph $B := B_r^k(p)$ there are two sets $S \subseteq V_G$ and $T \subseteq V_H$ with the following properties:*

- *$N(S) = T$, $N(T) = S$, and $|S| > |T|$;*
- *Spoiler can win the game in r rounds from the starting position $p \cup \{(v,w)\}$ for every pair $(v,w) \in V_G \times V_H$ with the property $v \in S \leftrightarrow w \notin T$.*

Proof. By assumption, $p \in S_{r+1}^k(G,H)$. This means that for all bijections $\varphi\colon V_G \to V_H$ that Duplicator can provide, there is always a $v \in V_G$ that Spoiler can choose in return, such that he still has a winning strategy from the position $p \cup \{v, \varphi(v)\}$ in r rounds. Hence for this v, we have $\{v, \varphi(v)\} \notin E_B$. Thus, there can be no perfect matching in the graph B. By Hall's marriage theorem [Hal35], a set $S \subseteq V_G$ exists with $|N_B(S)| < |S|$. We choose S to be an inclusion-maximal set with this property. Further, let

$$T := N_B(S).$$

We claim that $N_B(T) = S$ holds. To reach a contradiction, suppose that there is a vertex

$$v \in N_B(T) \setminus S. \tag{3}$$

The maximality of S implies $N_B(v) \not\subseteq T$. Let

$$w \in N_B(v) \setminus T \tag{4}$$

be a vertex witnessing this fact. Since $v \in N_B(T)$, there exists a vertex

$$w' \in N_B(v) \cap T. \tag{5}$$

Moreover, since $T = N_B(S)$ there is a vertex

$$v' \in N_B(w') \cap S. \tag{6}$$

The choice of the vertices in Equations (3)–(6) implies that there are edges

$$\{v', w'\}, \{v, w'\}, \{v, w\} \in E_B.$$

This means that Duplicator has a winning strategy for the r-round k-bijective pebble game from the starting positions $p \cup \{(v', w')\}$, $p \cup \{(v, w')\}$, and $p \cup \{(v,w)\}$. Since $\equiv_{D^k}$ is an equivalence relation, we thus have that she also has a winning strategy starting from $p \cup \{(v', w)\}$. Hence, $\{v', w\} \in E_B$. However, this contradicts $w \notin N_B(S)$. ☐

For a game position $p = \{(v_1, w_1), \dots, (v_\ell, w_\ell)\} \subseteq V_G \times V_H$ we let $S_p := \sum_{i=1}^{\ell} x_{v_i,w_i}$. Note that, in particular, $S_\emptyset = 0$.

Theorem 23. *Suppose that Spoiler has a winning strategy for the r-round bijective k-pebble game played on the graphs G and H with initial position p_0. Then, there is a* CP *derivation of the inequality $S_{p_0} \leq |p_0| - 1$ from* $\mathrm{Iso}(G, H)$ *having width k and rank r simultaneously.*

Proof. We prove the theorem by induction on r, the number of rounds in the game. First, we consider the base case, where Spoiler wins the game from p_0 in 0 rounds. Since $|V_G| = |V_H|$, it must be that p_0 is not a local isomorphism; therefore, there are two pairs $(v, w), (v', w') \in p_0$ that induce a local non-isomorphism. Hence, the inequality $x_{v,w} + x_{v',w'} \leq 1$ must be a Type 2 axiom of $\mathrm{Iso}(G, H)$. Adding the Type 3 axiom inequalities $x_{a,b} \leq 1$ for all $|p_0| - 2$ many other pairs $(a, b) \in p_0 \setminus \{(v, w), (v', w')\}$, we obtain a derivation of $S_{p_0} \leq |p_0| - 1$.

For the induction step, let $p \subseteq p_0$ with $|p| = \ell < k$ be the set of pairs not deleted by Spoiler at the beginning of the first round in the game. It suffices to show that it is possible to derive the inequality $S_p \leq |p| - 1$. We consider the bipartite graph B from Definition 21. From Lemma 22, we know that there are two sets $S \subseteq V_G$ and $T \subseteq V_H$ with $N(S) = T$, $N(T) = S$ and $|S| > |T|$ and such that for every pair (v, w) with $v \in S \leftrightarrow w \notin T$, Spoiler can win the game in r-rounds from the start position $p \cup \{(v, w)\}$. By the induction hypothesis, there is a CP derivation of $S_p + x_{v,w} \leq |p|$ for all such pairs.

We notice first that we can derive the inequalities

$$\sum_{v \in S,\, w \in T} x_{v,w} \leq |T| \quad \text{and} \quad \sum_{v \in \overline{S},\, w \in \overline{T}} x_{v,w} \leq |\overline{S}|. \tag{7}$$

To derive the first one of them, observe that for each $w \in T$, we have the axiom inequality $\sum_{v \in V_G} x_{v,w} \leq 1$, which can be reduced to $\sum_{v \in S} x_{v,w} \leq 1$ by adding the axioms $x_{v,w} \geq 0$ for all $v \in \overline{S}$. We obtain the first expression by adding the inequalities for all $w \in T$. The second one is completely analogous. Adding both inequalities of (7) together, we get:

$$\sum_{v \in S,\, w \in T} x_{v,w} + \sum_{v \in \overline{S},\, w \in \overline{T}} x_{v,w} \leq |T| + |\overline{S}|. \tag{8}$$

Since $|T| + |\overline{S}| < |S| + |\overline{S}| = n$, Inequality (8) can be weakened to

$$\sum_{v \in S,\, w \in T} x_{v,w} + \sum_{v \in \overline{S},\, w \in \overline{T}} x_{v,w} \leq n - 1.$$

Next, for each vertex $v \in S$ adding over all inequalities $S_p + x_{v,w} \leq |p|$ corresponding to pairs (v, w) for $w \in \overline{T}$ (derived inductively) we get

$$\sum_{w \in \overline{T}} (S_p + x_{v,w}) \leq |\overline{T}|\ell,$$

and adding over all $v \in S$, we obtain

$$\sum_{v \in S} \sum_{w \in \overline{T}} (S_p + x_{v,w}) \leq |S||\overline{T}|\ell. \tag{9}$$

Analogously, considering the pairs with $v \notin S$ and $w \in T$, we get

$$\sum_{w \in T} \sum_{v \in \overline{S}} (S_p + x_{v,w}) \leq |\overline{S}||T|\ell. \tag{10}$$

Let $\gamma := |S||\overline{T}| + |\overline{S}||T|$. By adding the inequalities corresponding to the long Type 1 axioms for all vertices $v \in V_G$, we can derive the inequality

$$\sum_{v \in V_G,\, w \in V_H} x_{v,w} \geq n.$$

Subtracting (9) and (10) from this, we get

$$\sum_{v \in S,\, w \in T} x_{v,w} + \sum_{v \in \overline{S},\, w \in \overline{T}} x_{v,w} - \gamma S_p \geq n - \gamma \ell.$$

Also subtracting the weakened version of (8), we derive

$$-\gamma S_p \geq 1 - \gamma \ell.$$

Observe that this last inequality has been obtained as the linear combination of axioms and previous inequalities, and therefore, the derivation can be done in one step. Using the rounding rule dividing by γ, we get

$$-S_p \geq \left\lceil \frac{1 - \gamma \ell}{\gamma} \right\rceil = 1 - \ell,$$

which is equivalent to $S_p \leq \ell - 1$. The linear combination and the rounding rule count as one use of the GC-rule. ☐

Corollary 24. *If $G \not\equiv_{\mathscr{C}_r^k} H$, then there is a* CP *refutation for* $\mathrm{Iso}(G, H)$ *having width k and rank r simultaneously.*

Proof. Spoiler can win the game starting at the empty initial position $p_0 = \emptyset$. The above result implies that the contradiction $0 \leq -1$ can be derived with the desired parameters. ☐

Corollary 25. *If a pair of non-isomorphic graphs G, H with n vertices each can be separated by the bijective k-pebble game, then there is a* CP *refutation for* $\mathrm{Iso}(G, H)$ *having size $n^{\mathrm{O}(k)}$.*

Proof. This follows from the observation that the CP refutation of $\mathrm{Iso}(G, H)$ described above only contains axioms and inequalities of the form $S_p \leq |p| - 1$ for sets of pairs p. Since there are at most $\sum_{i=0}^{k} \binom{n}{i}^2 = n^{\mathrm{O}(k)}$ such sets of pairs, the result follows. ☐

Grohe [Gro17] proved that two non-isomorphic graphs in every non-trivial minor-closed graph class can be distinguished using k-WL for a constant k. This implies that for these graphs, the Cutting Planes procedure can produce polynomial-size certificates of graph non-isomorphism. As a concrete example, we mention that it was shown in [KPS19] that the Weisfeiler–Leman dimension of the class of all finite planar graphs is at most 3. Furthermore, 2-WL asymptotically almost surely decides isomorphism for random regular graphs [Bol82, Kuc87].

3.2 CP Width Lower Bound for the Isomorphism Formulas

As described in [Juk12], for a polytope $P \subset \mathbb{R}^n$, the *Chvátal closure* P' is the polytope of all points $\mathbf{x}$ such that, for every $\mathbf{a} \in \mathbb{Z}^n$ and every $b \in \mathbb{R}$, we have

$$[\forall \mathbf{y} \in P : \langle \mathbf{a}, \mathbf{y} \rangle \geq b] \implies \langle \mathbf{a}, \mathbf{x} \rangle \geq \lceil b \rceil; \tag{11}$$

that is, we remove all points of the polytope P that are (in a certain sense) definitely not integer solutions. By iteratively defining $P^{(i+1)} := (P^{(i)})'$, we obtain a sequence $P = P^{(0)} \supseteq P^{(1)} \supseteq P^{(2)} \supseteq \dots$ of polytopes. The Chvátal rank can then be seen as the smallest r such that $P^{(r)} = P^{\mathbb{Z}}$ (it was shown by Schrijver [Sch80] that such an r always exists).

Protection lemmas have a long tradition in optimization theory for the study of the Chvátal rank. For the CP rank, such lemmas have been used in [BGH+06] and [Lau16]. A protection lemma for CP width was introduced in [DM12]. We give a width protection lemma adapted to the graph isomorphism problem. This generalizes (11). The following notation is employed.

Notation 26. Given a matrix $\mathbf{X} \in \mathbb{R}^{n\times n}$ and a set $I \subseteq [n]$ we denote by $\mathbf{X}|_I \in \mathbb{R}^{n\times n}$ the projection of $\mathbf{X}$ to the rows in I, that is, to the positions $\mathrm{Rows}[I] := \{(i,j) \mid i \in I, j \in [n]\}$ (meaning that the rows which are not in I are set to 0).

Definition 27. Let G and H be two graphs with n vertices each and let $P_{G,H}$ be the polytope in $[0,1]^{n\times n}$ defined by the $\mathrm{MIso}(G,H)$ inequalities. For $k \in \mathbb{N}$, we define

$$P'_{G,H}(k) := \left\{ \mathbf{X} \in P_{G,H} \;\middle|\; \begin{array}{l} \forall \mathbf{A} \in \mathbb{Z}^{n\times n},\ \forall b \in \mathbb{R},\ \forall I \subseteq [n] \text{ with } |I| = k : \\ {[\forall\, \mathbf{Y} \in P_{G,H} :\ \langle \mathbf{A}, \mathbf{Y}|_I\rangle_{\mathrm{F}} \geq b]} \implies \langle \mathbf{A}, \mathbf{X}|_I\rangle_{\mathrm{F}} \geq \lceil b \rceil \end{array} \right\}.$$

Here $\langle \mathbf{A}, \mathbf{B}\rangle_{\mathrm{F}} := \sum_{i=1}^{n}\sum_{j=1}^{n} a_{i,j}\, b_{i,j}$ denotes the *Frobenius inner product* between the matrices $\mathbf{A} = (a_{i,j}) \in \mathbb{R}^{n\times n}$ and $\mathbf{B} = (b_{i,j}) \in \mathbb{R}^{n\times n}$.

Lemma 28 (Protection Lemma for Graph Isomorphism)**.** *Let $k \in \mathbb{N}$. Further, let $\mathbf{X} \in [0,1]^{n\times n}$ be a fractional isomorphism in the polytope $P_{G,H}$. Suppose that for any $I \subseteq [n]$ with $|I| \leq k$, there is a set of matrices $\mathbf{Y^1}, \dots, \mathbf{Y^s} \in [0,1]^{n\times n}$ satisfying:*

- *For all $t \in [s]$, $(\mathbf{Y^t})_{i,j} \in \{0,1\}$ in all positions $(i,j) \in \mathrm{Rows}[I]$;*
- *for all $t \in [s]$, the matrix $\mathbf{Y^t}$ is a fractional solution of $P_{G,H}$; and*
- *the restriction $\mathbf{X}|_I$ is a convex combination of $\mathbf{Y^1}|_I, \dots, \mathbf{Y^s}|_I$.*

Then, $\mathbf{X} \in P'_{G,H}(k)$.

Proof. Suppose, to reach a contradiction, that $\mathbf{X}$ is a fractional isomorphism in $P_{G,H}$ but $\mathbf{X} \notin P'_{G,H}(k)$. Then, by Definition 27 there exists a matrix $\mathbf{A} \in \mathbb{Z}^{n\times n}$, a real number $b \in \mathbb{R}$, and a set $I \subseteq [n]$ with $|I| = k$ such that for all $\mathbf{Y} \in P_{G,H}$ we have $\langle \mathbf{A}, \mathbf{Y}|_I\rangle_{\mathrm{F}} \geq b$ but $\langle \mathbf{A}, \mathbf{X}|_I\rangle_{\mathrm{F}} < \lceil b \rceil$. Since $\mathbf{X} \in P_{G,H}$, we have $\langle \mathbf{A}, \mathbf{X}|_I\rangle_{\mathrm{F}} \geq b$. This implies that $\langle \mathbf{A}, \mathbf{X}|_I\rangle_{\mathrm{F}} \notin \mathbb{Z}$.

For all the protection matrices $\mathbf{Y^t} \in \{\mathbf{Y^1}, \dots, \mathbf{Y^s}\}$, since they are 0-1-valued in $\mathrm{Rows}[I]$, we have that $\langle \mathbf{A}, \mathbf{Y^t}|_I\rangle_{\mathrm{F}}$ is an integer. Also, since $\mathbf{Y^t}$ is in the polytope, $\langle \mathbf{A}, \mathbf{Y^t}|_I\rangle_{\mathrm{F}} \geq b$. Combining both facts, we have $\langle \mathbf{A}, \mathbf{Y^t}|_I\rangle_{\mathrm{F}} \geq \lceil b \rceil$. However, since $\mathbf{X}|_I$ is a convex combination of the protection matrices, it must hold $\langle \mathbf{A}, \mathbf{X}|_I\rangle_{\mathrm{F}} \geq \lceil b \rceil$, which is a contradiction. □

Note that for $|I| = k$, the above restrictions consider kn variables. In previously published protection lemmas, these restrictions had size k. However, our version can only make the construction of the protection matrices harder.

For each game position $p \subseteq V_G \times V_H$, we define a matrix $\mathbf{M^p}$ that we will show in Lemma 35 to be a fractional isomorphism between G and H. We begin by first defining auxiliary functions that will be used to define the entries of this matrix. Since $\equiv_{D^k}$ is an equivalence relation, we can define the type of $\mathbf{v} \in (V_G \cup \{\star\})^k$ as the equivalence class of $\mathbf{v}$.

Definition 29 ([BG15])**.** Given a tuple $\mathbf{v} \in (V_G \cup \{\star\})^k$ we let

$$c(\mathbf{v}) := [\mathbf{v}]_{\equiv_{D^k}}$$

be the equivalence class of $\mathbf{v}$. Further, we define

$$t(\mathbf{v}) := |c(\mathbf{v}) \cap (V_G \cup \{\star\})^k|.$$

Definition 30. Let $\mathbf{v} \in (V_G \cup \{\star\})^k$ and $\mathbf{w} \in (V_H \cup \{\star\})^k$. For every non-empty game position $q = \mathrm{zip}(\mathbf{v}, \mathbf{w}) \neq \emptyset$, the function ζ is defined in the following way:

$$\zeta(q) := \begin{cases} 0 & \text{if } c(\mathbf{v}) \neq c(\mathbf{w}) \\ \frac{1}{t(\mathbf{v})} & \text{otherwise.} \end{cases} \tag{12}$$

For $q = \emptyset$, we let $\zeta(\emptyset) := 1$.

We use the function ζ to define the entries of the matrix. For a game position $p \subseteq V_G \times V_H$ and a tuple $(v, w) \in V_G \times V_H$, we use the notation $p \cup vw$ as a shorthand for $p \cup \{(v, w)\}$.

Definition 31. Let $p \subseteq V_G \times V_H$ be a game position with $|p| \leq k-1$. For every $i, j \in [n]$, the number $m^p_{i,j}$ is defined in the following way:

$$m^p_{i,j} := \begin{cases} 0 & \text{if } p \cup v_i w_j \notin D^k(G, H) \\ \frac{\zeta(p \cup v_i w_j)}{\zeta(p)} & \text{otherwise.} \end{cases} \tag{13}$$

We further define the matrix $\mathbf{M^p}$ by letting $(\mathbf{M^p})_{i,j} := m^p_{i,j}$ for each $i, j \in [n]$.

Observe that in the case $\zeta(p) = 0$, the value of $m^p_{i,j}$ is 0 because the first case in (12) implies that $p \cup v_i w_j \notin D^k(G, H)$, ensuring that we do not divide by zero in (13). The following result follows directly from the definition of the matrix entries.

Lemma 32. *If $p \in D^k(G, H)$ and $(v_i, w_j) \in p$, then*

(i) $m^p_{i,j} = 1$, *and*

(ii) $m^p_{i',j} = m^p_{i,j'} = 0$ *for* $i \neq i'$ *and* $j \neq j'$.

Notation 33. Let $\mathbf{v} = (v_1, \ldots, v_k) \in (V_G \cup \{\star\})^k$ such that there is an $i \in [k]$ with $v_i = \star$. Such tuples represent positions in the bijective pebble game and are thus closed under permutations when the corresponding tuple in the other graph is permuted with the same permutation; see, e. g., [AM13, Claim 11]. For $v \in V_G$, we let $\mathbf{v}v$ be the tuple that results by replacing any $\star$ in $\mathbf{v}$ with v.

In the following, we tacitly assume an ordering $v_1 \prec v_2 \prec \cdots \prec v_n$ on the vertices of the graph and often identify a vertex v_i with its number i in this order. Hence, we can now speak of matrix positions (v, w). This helps to keep the following notation clear. The following technical lemma is needed in the next results. It follows from the properties of the equivalence relations defined by the bijective game.

Lemma 34. *Let $p \subseteq V_G \times V_H$ with $|p| \leq k-1$, and $p = \mathrm{zip}(\mathbf{a}, \mathbf{b})$. Then, for every $(v, w) \in V_G \times V_H$, if $c(\mathbf{a}\,v) = c(\mathbf{b}\,w)$, then*

$$t(\mathbf{a}\,v) = t(\mathbf{a}) \cdot \left|\{w' \in V_H \mid c(\mathbf{a}\,v) = c(\mathbf{b}\,w')\}\right|.$$

Proof. Since $c(\mathbf{a}\,v) = c(\mathbf{b}\,w)$, we have

$$\left|\{w' \in V_H \mid c(\mathbf{a}\,v) = c(\mathbf{b}\,w')\}\right| = \left|\{v' \in V_G \mid c(\mathbf{a}\,v) = c(\mathbf{a}\,v')\}\right| = \frac{|c(\mathbf{a}\,v)|}{|c(\mathbf{a})|} = \frac{t(\mathbf{a}\,v)}{t(\mathbf{a})}. \qquad \square$$

Lemma 35. *Let $\mathbf{a} \in (V_G \cup \{\star\})^k$ and $\mathbf{b} \in (V_H \cup \{\star\})^k$ be such that $c(\mathbf{a}) = c(\mathbf{b})$ and such that $p := \mathrm{zip}(\mathbf{a}, \mathbf{b})$ has size $|p| < k-1$. Then, the matrix $\mathbf{M^p}$ is a fractional isomorphism between G and H.*

Proof. We first show that when p is as above, the axioms expressed that we are dealing with a double stochastic matrix are satisfied by $\mathbf{M^p}$ (even when $|p| = k-1$). For each $v \in V_G$ we have

$$\sum_{w \in V_H} (\mathbf{M^p})_{v,w} = \sum_{\substack{w \in V_H \\ c(\mathbf{a}\,v) = c(\mathbf{b}\,w)}} \frac{\zeta(p \cup vw)}{\zeta(p)} = \sum_{\substack{w \in V_H \\ c(\mathbf{a}\,v) = c(\mathbf{b}\,w)}} \frac{t(\mathbf{a})}{t(\mathbf{a}\,v)}.$$

By Lemma 34 we have $\left|\{w \in V_H \mid c(\mathbf{a}\,v) = c(\mathbf{b}\,w)\}\right| = t(\mathbf{a}\,v)/t(\mathbf{a})$. Hence, the sum of a row in the matrix adds to 1. The proof for the columns is analogous.

For the case of the isomorphism axioms, let $(v, w) \in V_G \times V_H$. We have to show

$$\sum_{i \in N(v)} m^p_{i,w} = \sum_{j \in N(w)} m^p_{v,j}. \tag{14}$$

By the result on the double stochasticity of the matrices just proved above, since $|p \cup iw| \leq k-1$, we have that for every $i \in N(v)$,

$$1 = \sum_{j \in V_H} m^{p \cup iw}_{v,j} = \sum_{j \in N(w)} m^{p \cup iw}_{v,j},$$

the last equality holds because only for the neighbors of w the value of $m^{p\cup iw}_{v,j}$ can be different from 0. By the definition, if $m^{p\cup iw}_{v,j} \neq 0$ then this number can be expressed as $\xi \cdot m^p_{v,j}$, with

$$\xi := \frac{t(\mathbf{a}\,v) \cdot t(\mathbf{a}\,i)}{t(\mathbf{a}) \cdot t(\mathbf{a}\,i\,v)}.$$

Therefore

$$\sum_{j \in N(w)} m^p_{v,j} = \sum_{j \in N(w)} m^{p \cup iw}_{v,j} \frac{1}{\xi} = \frac{1}{\xi}.$$

Similarly for every $j \in N(w)$, we have

$$1 = \sum_{i \in N(v)} m^{p \cup vj}_{i,w},$$

and also the numbers $m^{p \cup vj}_{i,w}$ (when different from 0) can be expressed as $\xi \cdot m^p_{i,w}$. Therefore both sums in 14 are equal. $\square$

We observe that in the previous result it does not suffice that $|p| \leq k-1$ in order for the matrix $\mathbf{M^p}$ to be a fractional isomorphism between G and H. As a counterexample consider G to be a cycle with 6 vertices and H to be the union of two cycles with 3 vertices each, and let $\mathbf{A}$ and $\mathbf{B}$ be the adjacency matrices of these graphs. Duplicator wins the 2-pebble game on G, H, however, it can be easily checked that for $p = (v, w)$ for any pair $v \in V_G, w \in V_H$, the matrix $\mathbf{M^p}$ does not satisfy $\mathbf{AM^p} = \mathbf{M^pB}$.

Theorem 36. *Let G and H be two non-isomorphic graphs with n vertices each such that $G \equiv_{\mathscr{C}^k} H$. Further, let $p \in D^k(G,H)$ with $|p| < k-1$ and consider the matrix $\mathbf{M^p}$. For any $I \subseteq [n]$ with $|I| < k-1$, there is a set of matrices $\mathbf{Y^1}, \dots, \mathbf{Y^s}$, satisfying:*

- *Each of these matrices is 0-1-valued on Rows$[I]$;*
- *each of these matrices is a fractional isomorphism in $P_{G,H}$ of the form $\mathbf{M^{p'}}$, with $|p'| < k-1$, and $p' \in D^k(G,H)$; and*
- *the restriction $\mathbf{M^p}|_I$ is a convex combination of $\mathbf{Y^1}|_I, \dots, \mathbf{Y^s}|_I$.*

Proof. We prove the result by induction on $\ell = |I|$. For the induction base $\ell = 1$, let p be a game starting position as above and let $I = \{i_1\}$. Consider the matrix $\mathbf{M^p}$. We can suppose that w. l. o. g. that i_1 is not a vertex contained in a tuple of p and also that for all $j \in [n]$, the matrix entry $m^p_{i_1,j} \neq 1$. Otherwise, $\mathbf{M^p}$ already has the desired properties.

Let us start with the simpler case in which $|p| < k-2$. Also, not all the positions in a row i_1 of $\mathbf{M^p}$ can be 0 since we are dealing with a fractional isomorphism. Under these conditions, there is a set of at least two non-zero elements in that row; let us call this set $\mathrm{NZ}(i_1)$. This follows from the fact that the sum of the row elements adds to 1. For each $j \in \mathrm{NZ}(i_1)$ let $p_j := p \cup v_{i_1}w_j$ and consider the matrices $\mathbf{Y^j} := \mathbf{M^{p_j}}$ for $j \in \mathrm{NZ}(i_1)$.

These matrices have the following properties: According to Lemma 32, they have 0-1 values on the row i_1. Due to Lemma 35, the matrices $\mathbf{M^{p_j}}$ are fractional isomorphisms since $|p_j| < k-1$. All the p_j considered as game positions are winning positions for Duplicator in the k-bijective game since they can be reached if Spoiler adds the pair (v_{i_1}, w_j) (for any $j \in \mathrm{NZ}(i_1)$) which is a valid move since these positions are non-zero in $\mathbf{M^p}$, meaning that $p \cup v_{i_1}w_j$ is also a winning position for Duplicator. It is only left to show that $\mathbf{M^p}|_I$ is a convex combination of the restriction to Rows$[I]$ of the matrices $\mathbf{M^{p_j}}$, but this follows from the fact that for each $j \in \mathrm{NZ}(i_1)$, the matrix $\mathbf{M^{p_j}}$ has a 1 in position (i_1, j), and 0's in all other positions in the row i_1, and all these positions have the same value in $\mathbf{M^p}$. Therefore, $\mathbf{M^p}|_I$ can be obtained as a convex combination of the restriction to Rows$[I]$ of the new matrices, multiplying each one of them times $(\mathbf{M^p})_{i_1,j}$. This is a correct combination since for $p = \mathrm{zip}(\mathbf{a}, \mathbf{b})$, and $c(\mathbf{a}\, v_{i_1}) = c(\mathbf{b}\, w_j)$, we have

$$(\mathbf{M^p})_{i_1,j} = \frac{t(\mathbf{a})}{t(\mathbf{a}\, v_{i_1})}$$

and the number of such matrices is equal to

$$|\mathrm{NZ}(i_1)| = \big|\{j \mid c(\mathbf{a}\, v_{i_1}) = c(\mathbf{b}\, w_j)\}\big| = \frac{t(\mathbf{a}\, v_{i_1})}{t(\mathbf{a})}.$$

Let us now suppose $|p| = k-2$. In this situation, we cannot just add elements to p since then, we cannot guarantee that the resulting matrix is a fractional isomorphism, and we have to delete some elements from p first. Let (v, w) be any pair in p and let $\hat{p} = p \setminus \{(v, w)\}$. For any $j \in \mathrm{NZ}(i_1)$ let $p'_j := \hat{p} \cup v_{i_1}w_j$ and consider the matrices $\mathbf{Y^j} := \mathbf{M^{p'_j}}$. Again these matrices have 0-1 values on the row i_1 and encode fractional isomorphisms since each p'_j has the right length and is a winning position for Duplicator in the k-bijective game since these positions can be reached if Spoiler deletes (v, w) from p and adds (v_{i_1}, w_j), which are valid moves since these positions are non-zero in $\mathbf{M^p}$, meaning that $p \cup v_{i_1}w_j$ is also a winning position for Duplicator and, therefore, p'_j is also one. It is only left to show that $\mathbf{M^p}|_I$ is a convex combination of the restriction to Rows$[I]$ of the matrices $\mathbf{M}^{\mathbf{p}'_{\mathbf{j}}}$. Let $p = \mathrm{zip}(\mathbf{a}\,v, \mathbf{b}\,w)$. The value of a non-zero position in row i_1 in $\mathbf{M}^{\mathbf{p}}$ is

$$\frac{t(\mathbf{a}\,v)}{t(\mathbf{a}\,v\,v_{i_1})}.$$

If there is a non-zero position in row i_1 in $\mathbf{M}^{\mathbf{p}}$, then the same position in $\mathbf{M}^{\hat{\mathbf{p}}}$ is also non-zero since $\hat{p} \subseteq p$. Each matrix $\mathbf{M}^{\mathbf{p}'_{\mathbf{j}}}$ has a 1 in position (i_1, j) and 0's in the other positions in that row. If $(\mathbf{M}^{\mathbf{p}})_{i_1,j} \neq 0$, then $\mathbf{M}^{\mathbf{p}'_{\mathbf{j}}}$ is one of the $\mathbf{Y}$ matrices since $(\mathbf{M}^{\hat{\mathbf{p}}})_{i_1,j} \neq 0$. There are

$$\big|\{j \mid c(\mathbf{a}\,v\,v_{i_1}) = c(\mathbf{b}\,w\,w_j)\}\big| = \frac{t(\mathbf{a}\,v\,v_{i_1})}{t(\mathbf{a}\,w)}$$

non-zero positions in row i_1 in $\mathbf{M}^{\mathbf{p}}$. Multiplying the $\mathbf{Y}$ matrices corresponding to these positions times $\frac{t(\mathbf{a}\,v)}{t(\mathbf{a}\,v\,v_{i_1})}$ and adding them together, we obtain the convex combination.

The induction step is completely analogous. Given $\mathbf{M}^{\mathbf{p}}$ and $I = \{i_1, \dots, i_\ell\}$, let $I' = \{i_1, \dots, i_{\ell-1}\}$. By induction, we can construct a set of matrices $\mathbf{Y}^{\mathbf{t}}$ of the form $\mathbf{M}^{\mathbf{p}'}$ with p' containing a set of pairs $\big\{(i_1, j_1), \dots, (i_{\ell-1}, j_{\ell-1})\big\}$ satisfying the conditions and such that $\mathbf{M}^{\mathbf{p}}|_{I'}$ is a convex combination of the constructed matrices. These are 0-1 on Rows$[I']$. In one last step, we can construct from these the matrices for I as in the case for $\ell = 1$. A convex combination from convex combinations is still one. □

Corollary 37. *If Duplicator has a winning strategy for the k-pebble bijective game played on G, H, then there is no* CP *refutation of* $\mathrm{MIso}(G,H)$ *of width $k-2$.*

Proof. This follows from Lemma 28 and the previous result since they together imply that each $\mathbf{M}^{\mathbf{p}}$ corresponding to a winning position p for Duplicator of size $|p| \leq k-2$ survives cuts of size $k-2$. At each step, starting from the empty position $p = \emptyset$ we consider the fractional isomorphism $\mathbf{M}^{\mathbf{p}}$. There are protection matrices for it that also correspond to winning positions p' for the Duplicator with size $|p'| \leq k-2$. For each of these new positions p' there are also protection matrices and therefore, it is not possible, allowing only cuts of width $k-2$, to eliminate any of these fractional isomorphisms from $P_{G,H}$. □

A close inspection of the proof of the previous theorem, together with Lemma 28, also gives a connection to CP rank.

Corollary 38. *Let $k \geq 3$. If Duplicator has a winning strategy for the r-round k-pebble bijective game played on G, H, then there is no* CP *refutation of* $\mathrm{MIso}(G,H)$ *of width $k-2$ and rank $\frac{r}{k-2}$.*

Proof. The hypothesis implies that the empty position belongs to $D^k_r(G,H)$. For any $r' \leq r$ and any position $p \in D^k_{r'}(G,H)$, the protection matrices $\mathbf{M}^{\mathbf{p}'}$ for $\mathbf{M}^{\mathbf{p}}$ correspond to positions p' with $|p'| \leq k-2$ that can be reached from p in the game in at most $k-2$ steps (the maximum number of steps happens when $p \cap p' = \emptyset$). This means that the new position p' belongs to $D^k_{r'-(k-2)}(G,H)$. Therefore, if the cuts have width at most $(k-2)$ in a CP refutation, the rank has to be at least $\frac{r}{k-2}$. □

4 Tree-CP* Size Lower Bounds For Refuting Isomorphism

Proving size lower bounds for Cutting Planes refutations of the isomorphism problem is a challenging open question. Basically, the two only known methods for proving such bounds are interpolation and lifting. Neither of these methods is suitable for isomorphism formulas. Interpolation requires some monotone problem, and GI is highly non-monotone. Also, after applying lifting, one obtains some constructed formulas that are not isomorphism formulas. Using some known results from communication complexity, we can, however, show size lower bounds for the restricted case of tree-like Cutting Planes proofs with polynomially bounded coefficients (we denote this system with Tree-CP*). A refutation is *tree-like* if the underlying directed acyclic graph is a tree. A CP proof for a formula F has *polynomially bounded coefficients* if there exists a constant $c > 0$ such that the absolute value of all coefficients used in inequalities of the proof is bounded by $\mathrm{O}(n^c)$, where n is the number of variables of F. The system Tree-CP* is non-trivial, allowing, for example, polynomial-sized proofs for the pigeonhole principle [CCT87].

In [IPU94], the size of Tree-CP proofs for a formula F was related to the communication complexity of a search problem for F, showing that if the underlying search problem has high communication complexity, this implies a lower bound for the Tree-CP size of refuting F.

Critical block sensitivity is a communication complexity measure introduced in [HN12], extending the classical concept of block sensitivity [Nis91]. It is an easy fact that a critical block sensitivity lower bound for a problem implies the same bound for the communication complexity of the search problem.

In [GP18, Theorem 3], lower bounds on the critical block sensitivity of Tseitin formulas were proved. The authors showed that there exist graph families of bounded degree, with critical block sensitivity communication $\Omega(n/\log n)$ which by the results in [IPU94] imply a size lower bound of $\Omega(2^{n/\log^2 n})$ for Tree-CP* refutations of Tseitin formulas.

It was shown in [Tor04, Lemma 4.2] that there is a direct reduction from Tseitin to isomorphism formulas, and it is, thus, possible to obtain lower bounds for isomorphism formulas from lower bounds for Tseitin formulas. As a direct consequence of all these results, we obtain:

Corollary 39. *There are families of non-isomorphic graphs G, H, with n vertices each, and such that the refutation of* $\mathrm{MIso}(G, H)$ *in* Tree-CP* *requires size* $\Omega(2^{n/\log^2 n})$.

5 Conclusions and Open Problems

We have shown an exact characterization of the Weisfeiler–Leman graph differentiation number of two graphs in terms of the cutwidth needed for refuting the corresponding isomorphism formula. Let us emphasize that Equation (1) holds for both the Iso and MIso formulas. For this, we have introduced a new protection lemma for the graph isomorphism polytope. This new connection enabled us to show that the Cutting Planes proof system can show graph non-isomorphism in polynomial time for graphs with a constant Weisfeiler–Leman dimension. Furthermore, by using known results from communication complexity, we were able to give a lower bound for the size of tree-like CP refutations with polynomially bounded coefficients for refuting graph isomorphism inequalities. Some important questions remain open. Maybe the most interesting one is to prove CP size lower bounds for isomorphism formulas. This is quite challenging since basically all the lower bounds for this kind of formula are based on graphs related to the Tseitin formulas, and recently a quasi-polynomial upper bound for the CP size of such formulas has been shown [DT20]. Furthermore, it would be interesting to have trade-off results between the dimension of the WL algorithm and its iteration number (this is equivalent to a trade-off between the number k of pebbles in Hella's bijective pebble game and the number r of rounds). While trade-off results are known for these parameters [BN16, GLN23], they do not hold for structures of bounded arity (like graphs). However, due to the connection of these parameters to the Resolution proof system [TW23] and the Cutting Planes proof system, as shown in this paper, such results would immediately imply proof complexity trade-offs (in our case, between width and rank for Cutting Planes). Moreover, it is open if the second implication in (1) can be improved.

References

[AM13] Albert Atserias and Elitza N. Maneva. Sherali–Adams relaxations and indistinguishability in counting logics. *SIAM Journal on Computing*, 42(1):112–137, 2013. Earlier conference version in *ITCS '12*. doi:10.1137/120867834.

[AO18] Albert Atserias and Joanna Ochremiak. Definable ellipsoid method, sums-of-squares proofs, and the isomorphism problem. In *Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science (LICS 18)*, pages 66–75, 2018. doi:10.1145/3209108.3209186.

[Bab16] László Babai. Graph isomorphism in quasipolynomial time [extended abstract]. In *Proceedings of the 48th Annual ACM SIGACT Symposium on Theory of Computing (STOC '16)*, pages 684–697, 2016. Full-length version in *arXiv:1512.03547*. doi:10.1145/2897518.2897542.

[BEGJ00] Maria L. Bonet, Juan L. Esteban, Nicola Galesi, and Jan Johannsen. On the relative complexity of resolution refinements and cutting planes proof systems. *SIAM Jornal on Computing*, 30(5):1462–1484, 2000. doi:10.1137/S0097539799352474.

[BG15] Christoph Berkholz and Martin Grohe. Limitations of algebraic approaches to graph isomorphism testing. In *Proceedings of the 42nd International Colloquium on Automata, Languages, and Programming (ICALP '15)*, pages 155–166, 2015. doi:10.1007/978-3-662-47672-7_13.

[BGH+06] Joshua Buresh-Oppenheim, Nicola Galesi, Shlomo Hoory, Avner Magen, and Toniann Pitassi. Rank bounds and integrality gaps for cutting planes procedures. *Theory Comput.*, 2(4):65–90, 2006. doi:10.4086/toc.2006.v002a004.

[BM88] László Babai and Shlomo Moran. Arthur–Merlin games: A randomized proof system, and a hierarchy of complexity classes. *Journal of Computer and System Sciences*, 36(2):254–276, 1988. doi:10.1016/0022-0000(88)90028-1.

[BN16] Christoph Berkholz and Jakob Nordström. Near-optimal lower bounds on quantifier depth and Weisfeiler–Leman refinement steps. In *Proceedings of the 31st Annual ACM/IEEE Symposium on Logic in Computer Science (LICS '16)*, pages 267–276, 2016. doi:10.1145/2933575.2934560.

[Bol82] Béla Bollobás. Distinguishing vertices of random graphs. In *North-Holland Mathematics Studies*, volume 62, pages 33–49. Elsevier, 1982. doi:10.1016/S0304-0208(08)73545-X.

[BW01] Eli Ben-Sasson and Avi Wigderson. Short proofs are narrow—resolution made simple. *Journal of the ACM*, 48(2):149–169, 2001. Earlier conference versions in *STOC '99* and *CCC '99*. doi:10.1145/375827.375835.

[CCT87] William J. Cook, Collette R. Coullard, and György Turán. On the complexity of cutting-plane proofs. *Discrete Applied Mathematics*, 18(1):25–38, 1987. doi:10.1016/0166-218X(87)90039-4.

[CEI96] Matthew Clegg, Jeffery Edmonds, and Russell Impagliazzo. Using the Groebner basis algorithm to find proofs of unsatisfiability. In *Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC '96)*, pages 174–183, May 1996. doi:10.1145/237814.237860.

[CFI92] Jin-yi Cai, Martin Fürer, and Neil Immerman. An optimal lower bound on the number of variables for graph identifications. *Combinatorica*, 12(4):389–410, 1992. Earlier conference version in *FOCS '89*. doi:10.1007/BF01305232.

[Chv73] Vasek Chvátal. Edmonds polytopes and a hierarchy of combinatorial problems. *Discrete Mathematics*, 4(4):305–337, 1973. doi:10.1016/0012-365X(73)90167-2.

[CR79] Stephen A. Cook and Robert A. Reckhow. The relative efficiency of propositional proof systems. *The Journal of Symbolic Logic*, 44(1):36–50, 1979. doi:10.2307/2273702.

[CSS14] Paolo Codenotti, Grant Schoenebeck, and Aaron Snook. Graph isomorphism and the Lasserre hierarchy, 2014. arXiv:1401.0758.

[DM12] Stefan S. Dantchev and Barnaby Martin. Cutting planes and the parameter cutwidth. *Theory of Computing Systems*, 51(1):50–64, 2012. doi:10.1007/s00224-011-9373-0.

[DT20] Daniel Dadush and Samarth Tiwari. On the complexity of branching proofs. In *Proceedings of the 35th Computational Complexity Conference (CCC '20)*, volume 169 of *LIPIcs*, pages 34:1–34:35, 2020. doi:10.4230/LIPIcs.CCC.2020.34.

[Ehr61] Andrzej Ehrenfeucht. An application of games to the completeness problem for formalized theories. *Fundamenta Mathematicae*, 49:129–141, 1961. doi:10.4064/fm-49-2-129-141.

[Fra50] Roland Fraïssé. Sur une nouvelle classification des systèmes de relations. *Comptes Rendus*, 230:1022–1024, 1950.

[GGKS20] Ankit Garg, Mika Göös, Pritish Kamath, and Dmitry Sokolov. Monotone circuit lower bounds from resolution. *Theory of Computing*, 16:1–30, 2020. Earlier conference version in *STOC '18*. doi:10.4086/toc.2020.v016a013.

[GLN23] Martin Grohe, Moritz Lichter, and Daniel Neuen. The iteration number of the Weisfeiler–Leman algorithm, 2023. arXiv:2301.13317.

[GO15] Martin Grohe and Martin Otto. Pebble games and linear equations. *The Journal of Symbolic Logic*, 80(3):797–844, 2015. Earlier conference version in *CSL '12*. doi:10.1017/jsl.2015.28.

[Gom63] Ralph E. Gomory. An algorithm for integer solutions of linear programs. In R. L. Graves and P. Wolfe, editors, *Recent Advances in Mathematical Programming*, pages 269–302. McGraw-Hill, New York, 1963.

[GP18] Mika Göös and Toniann Pitassi. Communication lower bounds via critical block sensitivity. *SIAM Journal on Computing*, 47(5):1778–1806, 2018. doi:10.1137/16M1082007.

[Gro17] Martin Grohe. *Descriptive Complexity, Canonisation, and Definable Graph Structure Theory*, volume 47 of *Lecture Notes in Logic*. Cambridge University Press, 2017. doi:10.1017/9781139028868.

[Hal35] Philip Hall. On representatives of subsets. *Journal of the London Mathematical Society*, 10(1):26–30, 1935. doi:https://doi.org/10.1112/jlms/s1-10.37.26.

[HC99] Armin Haken and Stephen A. Cook. An exponential lower bound for the size of monotone real circuits. *Journal of Computer and System Sciences*, 58(2):326–335, 1999. doi:10.1006/jcss.1998.1617.

[Hel96] Lauri Hella. Logical hierarchies in PTIME. *Information and Computation*, 129(1):1–19, 1996. doi:10.1006/inco.1996.0070.

[HN12] Trinh Huynh and Jakob Nordström. On the virtue of succinct proofs: amplifying communication complexity hardness to time-space trade-offs in proof complexity. In *Proceedings of the 44th Symposium on Theory of Computing Conference (STOC '12)*, pages 233–248, 2012. doi:10.1145/2213977.2214000.

[HP17] Pavel Hrubes and Pavel Pudlák. Random formulas, monotone circuits, and interpolation. In *Proceedings of the 58th Annual IEEE Symposium on Foundations of Computer Science (FOCS '17)*, pages 121–131, 2017. doi:10.1109/FOCS.2017.20.

[Imm82] Neil Immerman. Upper and lower bounds for first order expressibility. *Journal of Computer and System Sciences*, 25(1):76–98, 1982. Earlier conference version in *FOCS '80*. doi:10.1016/0022-0000(82)90011-3.

[Imm99] Neil Immerman. *Descriptive Complexity*. Graduate texts in computer science. Springer, 1999. doi:10.1007/978-1-4612-0539-5.

[IPS99] Russell Impagliazzo, Pavel Pudlák, and Jiří Sgall. Lower bounds for the polynomial calculus and the Gröbner basis algorithm. *Computational Complexity*, 8(2):127–144, 1999. doi:10.1007/s000370050024.

[IPU94] Russell Impagliazzo, Toniann Pitassi, and Alasdair Urquhart. Upper and lower bounds for tree-like cutting planes proofs. In *Proceedings of the 9th Annual IEEE Symposium on Logic in Computer Science (LICS '94)*, pages 220–228, July 1994. doi:10.1109/LICS.1994.316069.

[Juk12] Stasys Jukna. *Boolean Function Complexity – Advances and Frontiers*, volume 27 of *Algorithms and Combinatorics*. Springer, 2012. doi:10.1007/978-3-642-24508-4.

[Kie20] Sandra Kiefer. *Power and limits of the Weisfeiler–Leman algorithm.* Dissertation, RWTH Aachen University, 2020. doi:10.18154/RWTH-2020-03508.

[KPS19] Sandra Kiefer, Ilia Ponomarenko, and Pascal Schweitzer. The Weisfeiler–Leman dimension of planar graphs is at most 3. *Journal of the ACM*, 66(6):44:1–44:31, 2019. doi:10.1145/3333003.

[Kuc87] Ludek Kucera. Canonical labeling of regular graphs in linear average time. In *Proceedings of the 28th Annual IEEE Symposium on Foundations of Computer Science (FOCS '87)*, pages 271–279, 1987. doi:10.1109/SFCS.1987.11.

[Lau16] Massimo Lauria. A rank lower bound for cutting planes proofs of Ramsey's theorem. *ACM Transactions on Computation Theory*, 8(4):17:1–17:13, 2016. doi:10.1145/2903266.

[Lib04] Leonid Libkin. *Elements of Finite Model Theory.* Texts in Theoretical Computer Science: An EATCS Series. Springer, 2004. doi:10.1007/978-3-662-07003-1.

[Mal14] Peter N. Malkin. Sherali–Adams relaxations of graph isomorphism polytopes. *Discrete Optimization*, 12:73–97, 2014. doi:10.1016/j.disopt.2014.01.004.

[Nis91] Noam Nisan. CREW PRAMs and decision trees. *SIAM Journal on Computing*, 20(6):999–1007, 1991. doi:10.1137/0220062.

[OWWZ14] 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 25th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA '14)*, pages 1659–1677, 2014. doi:10.1137/1.9781611973402.120.

[Pud97] Pavel Pudlák. Lower bounds for resolution and cutting plane proofs and monotone computations. *The Journal of Symbolic Logic*, 62(3):981–998, 1997. doi:10.2307/2275583.

[Raz17] Alexander A. Razborov. On the width of semialgebraic proofs and algorithms. *Math. Oper. Res.*, 42(4):1106–1134, 2017. doi:10.1287/moor.2016.0840.

[SA90] Hanif D. Sherali and Warren P. Adams. A hierarchy of relaxations between the continuous and convex hull representations for zero-one programming problems. *SIAM Journal on Discrete Mathematics*, 3(3):411–430, 1990. doi:10.1137/0403036.

[Sch80] Alexander Schrijver. On cutting planes. *Annals of Discrete Mathematics*, 9:291–296, 1980. doi:10.1016/S0167-5060(08)70085-2.

[SS21] Pascal Schweitzer and Constantin Seebach. Resolution with symmetry rule applied to linear equations. In *Proceedings of the 38th International Symposium on Theoretical Aspects of Computer Science (STACS '21)*, volume 187 of *LIPIcs*, pages 58:1–58:16, 2021. doi:10.4230/LIPIcs.STACS.2021.58.

[Tor04] Jacobo Torán. On the hardness of graph isomorphism. *SIAM Journal on Computing*, 33(5):1093–1108, 2004. doi:10.1137/S009753970241096X.

[Tor13] Jacobo Torán. On the resolution complexity of graph non-isomorphism. In *Proceedings of the 16th International Conference on Theory and Applications of Satisfiability Testing (SAT '13)*, pages 52–66, 2013. doi:10.1007/978-3-642-39071-5_6.

[TW23] Jacobo Torán and Florian Wörz. Number of variables for graph differentiation and the resolution of graph isomorphism formulas. *ACM Transactions on Computational Logic*, 24(3):23:1–23:25, April 2023. Earlier conference version in *CSL '22*. doi:10.1145/3580478.

[Urq99] Alasdair Urquhart. The symmetry rule in propositional logic. *Discrete Applied Mathematics*, 96–97:177–193, 1999. doi:10.1016/S0166-218X(99)00039-6.

[Urq11] Alasdair Urquhart. The depth of resolution proofs. *Studia Logica*, 99(1-3):349–364, 2011. doi:10.1007/s11225-011-9356-9.

[Wei76] Boris Weisfeiler. *On Construction and Identification of Graphs*, volume 558 of *Lecture Notes in Mathematics*. Springer, 1976. doi:10.1007/BFb0089374.

[WL68] Boris Weisfeiler and Andrei Leman. The reduction of a graph to canonical form and the algebra which appears therein. *Nauchno-Technicheskaya Informatsia, Seriya 2*, 9, 1968. Translation from Russian into English by Grigory Ryabov available under https://www.iti.zcu.cz/wl2018/pdf/wl_paper_translation.pdf.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il