On the Resolution Complexity of Graph non-Isomorphism

Jacobo Torán
Institut für Theoretische Informatik
Universität Ulm
Oberer Eselsberg
D-89069 Ulm, Germany
jacobo.toran@uni-ulm.de

Abstract

For a pair of given graphs we encode the isomorphism principle in the natural way as a CNF formula of polynomial size in the number of vertices, which is satisfiable if and only if the graphs are isomorphic. Using the CFI graphs from [12], we can transform any undirected graph G into a pair of non-isomorphic graphs. We prove that the resolution width of any refutation of the formula stating that these graphs are isomorphic has a lower bound related to the expansion properties of G. Using this fact, we provide an explicit family of non-isomorphic graph pairs for which any resolution refutation requires an exponential number of clauses in the size of the initial formula. These graphs pairs are colored with color multiplicity bounded by 4. In contrast we show that when the color classes are restricted to have size 3 or less, the non-isomorphism formulas have tree-like resolution refutations of polynomial size.

1 Introduction

Resolution is one of the most popular and best studied proof systems for propositional logic. Since the first exponential lower bound for the size of resolution refutations proven by Haken [17] for the family of formulas encoding the pigeonhole principle, many other combinatorial principles have been shown to have exponential lower bounds [26, 13, 9, 7, 8]. With the recent development of modern SAT-solvers based on DPLL algorithms and the fact that the resolution principle lies in the core of such algorithms, resolution lower bounds have gained in importance because they also provide lower bounds for the running time of the SAT-solvers. We study here the complexity of testing graph non-isomorphism using resolution. The graph isomorphism problem, GI, asks whether there is a bijection between the nodes of two given graphs preserving the adjacency relationship. The problem has been extensively studied in the past (see e.g [21]) because its intrinsic importance and also because it is one of the few problems in NP that is not known to be solvable in polynomial time but also is not expected to be NP-complete.

The impressive improvement of the performance of SAT-solvers based on DPLL algorithms in the last years has motivated a new way for dealing with NP problems. For many practical applications, these problems are reduced to formulas than are then tested for satisfiability using the SAT-solvers. This method works well in practice for several problems, although strong resolution lower bounds for random instances of some NP-complete problems are known [7, 8]. It is natural to ask how well this approach works for problems in NP that are not believed to be complete in the class, like graph isomorphism. We study here the size of resolution refutations for formulas encoding graph isomorphism in the natural way. Given two graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$, with n nodes each, the formula $F(G_1, G_2)$ over the set of variables $\{x_{i,j} \mid i, j \in [n]\}$ is satisfiable if and only if there if an isomorphism between G_1 and G_2. Each satisfying assignments of the formula encodes an isomorphisms. In such an assignment the variable $x_{i,j}$ receives value 1 if and only if the encoded isomorphism maps vertex $v_i \in V_1$ to $v_j \in V_2$.

Definition 1.1 *For a pair of graphs G_1, G_2 with n vertices each, $F(G_1, G_2)$ is the conjunction of the following sets of clauses:*

Type 1 clauses: for every $i \in [n]$ the clause $(x_{i,1} \vee x_{i,2} \vee \cdots \vee x_{i,n})$ indicating that vertex $v_i \in V_1$ is mapped to some vertex in V_2.

Type 2 clauses: for every $i, j, k \in [n]$ with $i \neq j$ the clause $(\overline{x_{i,k}} \vee \overline{x_{j,k}})$ indicating that not two different vertices are mapped to the same one.

Type 3 clauses:, for every $i, j, k, l \in [n]$ $i < j$ and $k \neq l$ with $(v_i, v_j) \in E_1 \leftrightarrow (v_k, v_l) \notin E_2$, the clause $(\overline{x_{i,j}} \vee \overline{x_{i,k}})$ expressing the adjacency relation (an edge cannot be mapped to a non edge and vice-versa).

Formula $F(G_1, G_2)$ has n^2 variables and $O(n^4)$ clauses. The clauses of Types 2 and 3 have width 2, while the clauses of Type 1 have width n.

It is not hard to find pairs of non-isomorphic graphs whose formulas require exponential size resolution refutations. For example if graph G_1 consists of $n+1$ isolated vertices and G_2 n isolated vertices (no edges), then $F(G_1, G_2)$ is exactly PHP$(n+1,n)$, the formula encoding the pigeonhole principle with $n+1$ pigeons and n holes. It is well known that this formula requires exponential size resolution refutations [17]. More elaborate examples can be constructed for example encoding PHP in pairs of connected graphs with the same number of vertices. In order to find more interesting examples and to investigate whether the apparent inability of resolution for dealing with GI comes only from the difficulty to count, we consider here graphs with colored vertices and bounded color multiplicities (there is a bound on the number of vertices of each color). In an isomorphism between colored graphs, colors must be preserved. A vertex coloring is reflected very naturally in the clauses of Type 1, since for a vertex i in the first graph we only have to include the variables $x_{i,j}$ for the vertices j in the second graph with the same color as i. If the maximum color multiplicity is bounded by k, the clauses of Type 1 are reduced to have at most k literals. This restricts the isomorphism search space. This also prevents from encoding the pigeonhole principle in the formula. Also in this case we can ignore all the variables $x_{i,j}$ when i and j have different colors. This means that the corresponding isomorphism formulas have at most kn variables.

When the input graphs G_1 and G_2 are colored, we will also denote by $F(G_1,G_2)$ the formula defined as above, but with the Type 1 clauses restricted according to the colors.

For any constant k, it is known that GI for graphs with color multiplicity bounded by k can be solved in polynomial time, and even using more restricted resources [6, 15, 5]. In contrast to this fact, we show in this paper than in the case of resolution, there is a big difference between color classes of size 3 and larger classes. When the maximum color multiplicity is 3, the non-isomorphism formulas have polynomial size resolution refutations, (even tree-like refutations). On the other hand we prove an exponential lower bound for the resolution refutation of certain pairs of non-isomorphic graphs with color classes of size 4 or larger. The gap in the complexity of resolution depending on the size of the color classes coincides with the gap in the number of variables required for graph identification [19].

For our lower bound we consider the CFI graphs used by Cai, Fürer and Immerman in [12] to prove the impossibility of Weisfeiler-Lehmann based algorithms for solving GI. In this important paper the authors gave a method to transform any graph G with n vertices and maximum degree d into a pair of non-isomorphic graphs of size $nd2^d$ based on G. We show here that any resolution refutation of the related isomorphism formulas must have exponential size in $\frac{ex(G)}{d}$, were $ex(G)$ is the expansion of the graph G (Definition 4.9). The exponential lower bound follows by considering constant degree graphs with linear expansion. The lower bound holds even for pairs of colored graphs of degree at most 3 and color classes of size at most 4.

The idea behind the proof of the resolution lower bound resembles that from Urquhart [26] for proving resolution lower bounds for Tseitin formulas [25]. We profit however from several newer results that help us to simplify the proof. Especially, we make use the relationship between resolution size and width (the maximum number of literals in a clause in the refutation) proven by Ben-Sasson and Wigderson in [11], which imply size lower bounds by proving bounds on the width.

2 Preliminaries

We deal with Boolean formulas in conjunctive normal form, CNF. A CNF formula F on the set of variables V is a conjunction of clauses $C_1, \ldots, C_m$. Each clause is a disjunction of literals. A literal is either a variable or a negated variable from V. A (partial) assignment α is a (partial) mapping from V in $\{0, 1\}$. For a clause C and an assignment α, we denote by $C|_\alpha$ the result of applying α to C. This is 1 if α assigns value 1 some literal in C, or the result of deleting the literals in C being assigned to 0 otherwise. For a CNF formula F, $F|_\alpha$ is the conjunction of the clauses $C|_\alpha$ for every C in F.

2.1 Resolution

The concept of *resolution* was introduced by Robinson in [22]. Resolution is a refutation proof system for propositional formulas in conjunctive normal form. The only inference rule in this proof system is the resolution rule:

$$\frac{C \vee x \qquad D \vee \bar{x}}{C \vee D} \,.$$

Resolving variable x from clauses $C \vee x$ and $D \vee \bar{x}$ we get the *resolvent* clause $C \vee D$. A resolution refutation of a CNF formula F is a sequence of clauses $C_1, \ldots, C_s$ where each C_i is either a clause from F or is inferred from earlier clauses by the resolution rule, and C_s is the empty clause.

A resolution refutation can be pictured as a directed acyclic graph in which the clauses are the vertices and there are edges from the clauses to their resolvents. The restriction of resolution in which the underlying graph is a tree is called tree-like resolution.

Definition 2.1 *The size of a resolution refutation is the number of clauses it contains. For an unsatisfiable formula F, size$(Res(F))$ denotes the minimal size of a resolution refutation of F.*

We denote the size of the smallest tree-like refutation for F, by size$(TRes(F))$. Families of unsatisfiable formulas exist, for which there is an exponential separation between the size of tree-like resolution refutation and that of resolution refutations without restrictions [10]. It is well known that the size of a tree-like resolution refutations for an unsatisfiable formula corresponds to the running time of a DPLL algorithm on the formula (see e.g. [23]).

Definition 2.2 *[11] The width of a clause is the number of literals appearing in it. For a set of clauses $\mathcal{C}$ ($\mathcal{C}$ can be for example a formula in CNF or a resolution refutation) the width of $\mathcal{C}$, denoted by width$(\mathcal{C})$, is the maximal width of a clause in the set $\mathcal{C}$.*

The width needed for the resolution of an unsatisfiable CNF formula F, denoted by width$(Res(F))$, is the minimal width needed in a resolution of F, that is, the minimum of width(π) over all resolution refutations π of F.

For proving the lower bound on the resolution size we will use the relationship between width and size of a refutation introduced by Ben-Sasson and Widgerson in [11]. This approach allows to reduce the problem of giving lower bounds on the size of a refutation to that of giving lower bounds on the width.

Theorem 2.3 *[11] For an unsatisfiable formula F in CNF with n variables*

$$size(Res(F)) = \ exp(\Omega(\frac{[width(Res(F)) - width(F)]^2}{n})).$$

2.2 Graph Isomorphism

The graphs considered in this paper will be undirected simple graphs, usually denoted by $G = (V, E)$, where V is the vertex set and $E \subseteq \binom{V}{2}$. We say two graphs G_1 and G_2 are *isomorphic* if there is a bijection $\varphi : V_1 \longrightarrow V_2$ such that $(u, v) \in E_1$ iff $(\varphi(u), \varphi(v)) \in E_2$. We write $G_1 \cong G_2$ and call φ an isomorphism. An *automorphism* of a graph G is an isomorphism from G to G. Automorphisms are permutations on the set V, and the set of automorphisms Aut(X) forms a group under permutation composition. We say that a set of vertices $V' \subseteq V$ is set-wise stabilized by an automophism φ, if $V' = \varphi(V')$.

We will deal with graphs with colored vertices. A coloring with k colors is a function $f : V \to \{1, \ldots k\}$. In an isomorphism between colored graphs, the colors have to be preserved. This restricts the search space when looking for isomorphisms. For a color c, the color class corresponding to c is the set of vertices with this color in V. The set of color classes defines a partition of the graph vertices. A *refinement* of a given set of color classes, is a refinement of this partition, that is, every color class in the refinement is a subset of the original partition. When a pair of graphs is given as input for the isomorphism problem, there are two color classes of each color, one in each graph. It should be clear from the context, from which one of the classes we are talking about in the text.

3 Polynomial size tree-like resolution refutations for color multiplicity 2 and 3

For the case of graphs with color classes of size 2, all the clauses in the non-isomorphism formulas have width 2. It is well known that an unsatisfiable set of clauses of width at most 2 has polynomial size tree-like resolution refutations. This simple observation provides an alternative proof for the fact that GI for graphs with color multiplicities at most 2 is in P. We extend this observation to the case of graphs with color classes at most 3.

Theorem 3.1 *Let G_1 and G_2 be two colored non-isomorphic graphs with color classes of size at most 3. Then $F(G_1, G_2)$ has tree-like resolution refutations of polynomial size.*

Proof. We can suppose that the subgraphs induced by every pair of color classes in G_1 and G_2 are isomorphic, because otherwise, there would be an unsatisfiable subformula of constant size in $F(G_1, G_2)$, having a constant size tree-like resolution refutation. For some pairs of color classes, the subgraphs S_1 and S_2, induced by the vertices with these colors in G_1 and G_2 can restrict the set of possible isomorphisms between the subgraphs, thus implying a further refinement in the vertex partition defined by the colors.

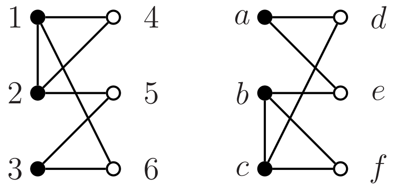

Figure 1: The subgraphs S_1 and S_2 induced by a pair of color classes (black,white).

For example in Figure 1 every possible isomorphism between S_1 and S_2 must map 1 to b or c, 2 to b or c, and 3 to a. This implies that every possible isomorphism between the subgraphs must map 4 to f, 5 to d or e and 6 to d or e. Observe that by considering the subgraphs induced just by the white color classes, no further refinement would have followed.

One can use this refinement in the set of possible isomorphisms between S_1 and S_2 to derive a refinement of the clauses of Type 1 by a constant size resolution refutation from the (constant size) initial set of clauses in $F(S_1, S_2)$. In our example these new clauses would be: $(x_{1,b}, x_{1,c}), (x_{2,b}, x_{2,c})$, $x_{3,a}$, $x_{4,e}$, $(x_{5,d}, x_{5,f})$ and $(x_{6,d}, x_{6,f})$. A way to see that in case of a refinement in the color classes it is always possible to obtain the reduced clauses, is by noticing that if there is no isomorphism between the subgraphs mapping 1 to a, for example, then the subformula obtained by setting $x_{1,a}$ to 1 in $F(S_1, S_2)$ is unsatisfiable and therefore it has a constant size tree-like refutation $\mathcal{R}$. By the standard trick of using the structure of the refutation $\mathcal{R}$, but starting with the clauses in $F(S_1, S_2)$ (instead of $F(S_1, S_2)|_{x_{1,a}=1}$), one derives the literal $\overline{x_{1,a}}$ (or maybe the empty clause in case $F(S_1, S_2)$ was unsatisfiable). By resolving these literals (unitary clauses) with the corresponding clauses of Type 1, one obtains the desired refined clauses.

Because of these observations, we can suppose that in G_1 and G_2 the partition on the vertex set defined by the color classes, cannot be further refined by considering the subgraphs induced by pairs of color classes. Considering this, by inspecting the few possible cases of edge connections between two color classes, it can be seen that for every pair of colors, say black and white, there are two possible situations in the subgraphs S_1 and S_2 induced by these color classes in G_1 and G_2, (this fact has been previously observed [19, 20]). Either:

1. For every possible bijective mapping of the black vertices, there is a *unique* extension to the white vertices that is an isomorphism from S_1 to S_2, or

2. For every possible bijective mapping of the black vertices, every possible bijective extension to the white vertices is an isomorphism from S_1 to S_2.

(This property does not hold when the color classes can have size larger than 3.) We show in Figure 2 the possible edge connections between two color classes when they do not imply a refinement. The first and last situations belong to Case 2, while the second and third belong to Case 1. The situations involving color classes of size smaller than 3 are not included in the figure but are also easy to check.

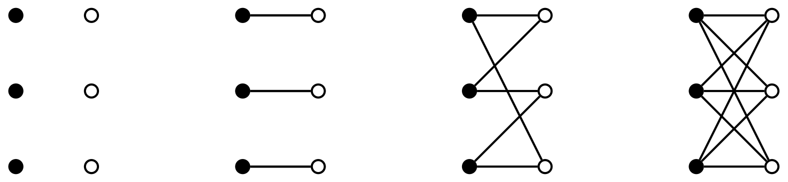

Figure 2: The possible (non refining) edge connections between two color classes of size 3.

Translating this to resolution, this property intuitively means that in Case 1, an assignment for a possible mapping of one of the color classes fixes an assignment of the variables for another color, and so on, until (in the case of non-isomorphic graphs) a contradiction is found.

Suppose that black and white are two color classes with edge connections as in Case 1, and suppose we had three unitary clauses, specifying a mapping of the black vertices (like for example $x_{1,a}$, $x_{2,b}$, and $x_{3,c}$). By a unit-resolution refutation of constant size, resolving first these clauses with clauses of Type 3 and then using the obtained resolvents together with the clauses of Type 1 for the white vertices, the unitary clauses specifying the corresponding mapping of the white vertices can be obtained. Observe that one would also obtain (by unit-resolution) the unit clauses for the white vertices if instead of the unit clauses for the black vertices one would have started with a partial assignment α defining a mapping of the black vertices (like $x_{1,a} = 1$, $x_{2,b} = 1$, and $x_{3,c} = 1$) and considering the formula $F(G_1, G_2)|_\alpha$.

We can now define a new graph $\mathcal{C}$ in which there is a vertex for each color class in G_1, and there is an edge between two color classes if and only if the edge connections between the vertices of the corresponding classes in G_1 or G_2 are as in Case 1.

If G_1 and G_2 are not isomorphic, then there must be a set of color classes so that the subgraphs induced by these classes in G_1 and G_2 are non-isomorphic. These color classes define a connected component in C. Moreover, if for every pair of color classes the corresponding induced subgraphs in G_1 and G_2 are isomorphic, then there has to be a cycle in $\mathcal{C}$ so that the graphs induced by the colors in this cycle are non isomorphic. Otherwise, it would be possible to extend the isomorphism between two color classes to an isomorphism between G_1 and G_2.

Let black be any color class in such a cycle. By the above observations, from any of the possible partial assignments α of the variables corresponding to a bijective mapping of the black color class, the clauses corresponding to the unique possible mapping of a neighboring color class in the cycle can be derived (by a constant unit-resolution refutation) and so on, coming back to black. A partial isomorphism different from the initial one is then forced on this class, thus forcing a contradiction.

Since the number of colors in the cycle is bounded by the number of vertices, any partial assignment α defining a bijective mapping of the black vertices, defines a polynomial size tree-like (and unit-resolution) refutation of $F(G_1, G_2)|_\alpha$. There are only 6 possible such bijective mappings α. By using again the trick repeating these refutations separately on $F(G_1, G_2)$, one obtains a tree-like derivation of an unsatisfiable set of clauses involving only variables $x_{i,j}$ with i and j in the black classes. This set has constant size, and from it, the empty clause can be derived.

■

4 The CFI graphs and their formulas

We define now the graphs that will be used for the resolution lower bounds. These graphs were considered in [12] to prove lower bounds for the Weisfeiler-Lehman method in isomorphism testing. In [24] a generalization of these graphs was used in order to show that GI is hard for the complexity class DET.

Definition 4.1 *For $k \geq 2$ the graph $X_k = (V_k, E_k)$ is defined as follows:*

$V_k = A_k \cup B_k \cup M_k$ where $A_k = \{a_i \mid i \in [k]\}$, $B_k = \{b_i \mid i \in [k]\}$ and $M_k = \{m_S \mid S \subseteq [k], |S| \text{ even}\}$. The graph is bipartite, the set of edges connect a and b vertices with m vertices $E_k = \{(m_S, a_i) \mid i \in S\} \cup \{(m_S, b_i) \mid i \notin S\}$.

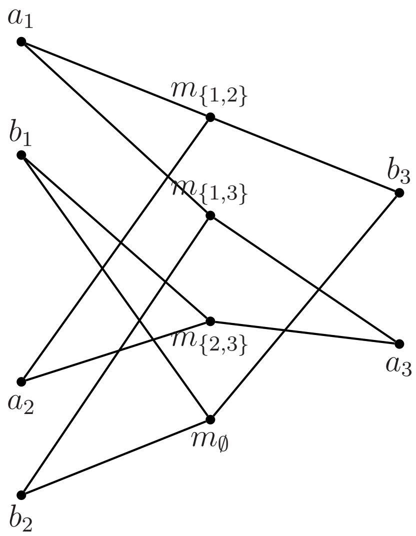

Figure 3. The graph X_3

Graph X_k consists of $2^{k-1} + 2k$ vertices and $k2^{k-1}$ edges. Let us give some intuition on the definition. Suppose that for each i we color the vertex set $\{a_i, b_i\}$ with color i so that any automorphism of X_k must set-wise stabilize these vertex sets. An automorphism in the colored graph, might map some a_i vertices to the corresponding b_i vertex, while fixing the rest of the a and

b vertices. As stated in the following Lemma from [12], describing the set of automorphism in X_k, the graph is constructed in such a way, that their automorphisms correspond to the situations in which the number of $i \in [n]$ with vertex a_i being mapped to b_i is even.

Lemma 4.2 *[12] There are exactly 2^{k-1} automorphisms in X_k stabilizing the sets $\{a_i, b_i\}, i \in [k]$. Each such automorphism is determined by interchanging a_i and b_i for each i in some subset $S \subseteq [k]$ of even cardinality.*

More intuitively, the construction can be understood with the simplification of X_k given in Figure 4. Here we have one v_i vertex for each pair a_i, b_i, and these are connected to a single m vertex for all the vertices in M_k. If we assign $\{0, 1\}$ values to the v_i vertices, the previous lemma just says that the sum of these values has to be even.

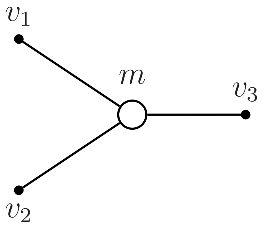

Figure 4.

We now transform a graph G into a graph $X(G)$ by substituting its vertices by the gadgets of Definition 4.1.

Definition 4.3 *Let $G = (V, E)$ be a connected graph with minimum degree at least 2. We transform G in a new graph $X(G)$ in which every vertex v of degree d in G is substituted by a copy $X(v)$ of the gadget X_d, and these are connected in the following way:*

To each edge $e = (u, v)$ having v as endpoint we associate two vertices $\{a^v_e, b^v_e\}$ in $X(v)$ and two vertices $\{a^u_e, b^u_e\}$ in $X(u)$. We then join with an edge the a_e vertices in $X(v)$ and $X(u)$ and the b_e vertices in $X(v)$ and $X(u)$. This means that every edge in G is transformed into two edges in $X(G)$. $X(G)$ can be intuitively understood as the result of going back from the graph in Figure 4, to the one in Figure 3, for every vertex.

If G has maximum degree d then $X(G)$ has at most $|V|d2^d$ vertices and $2|E| + |V|d2^{d-1}$ edges. It should be clear that the set of automorphisms of $X(G)$ stabilizing the pairs $\{a^v_e, b^v_e\}$ have to be edge respecting in the sense of the following definition.

Definition 4.4 *A permutation φ acting on the set $\{a^v_e, b^v_e \mid e$ is an incident edge with vertex v in $G\}$ is called edge respecting if it stabilizes all the pairs $\{a^v_e, b^v_e\}$ and has the property that for every edge $e = (u, v)$ in G, $\varphi(a^u_e) = a^u_e$ if and only if $\varphi(a^v_e) = a^v_e$.*

The following observation is a direct consequence of Lemma 4.2.

Observation 4.5 *There is a 1-1 correspondence between the set of edge respecting permutations φ acting on the set $\{a^v_e, b^v_e \mid e$ is an incident edge with vertex v in $G\}$ and with the property that for every vertex v, φ interchanges the vertices a^v_e and b^v_e for an* even *number of edges e incident with v, and the set of automorphism in $Aut(X(G))$ stabilizing the sets $\{a^v_e, b^v_e\}$.*

For $E' \subseteq E$, let $\tilde{X}(G, E')$ be a copy of $X(G)$ but in which all the edges $e = (u, v) \in E'$ are twisted, that is a^u_e is connected to b^v_e and b^u_e is connected to a^v_e. The next lemma shows that depending on the number of twisted edges in $\tilde{X}(G, E')$ we can only have two possible isomorphism classes.

Lemma 4.6 *[12] Let $G = (V, E)$ be a connected graph with minimal degree at least 2 and let $E' \subseteq E$ with $||E'|| = t$. If t is even then $\tilde{X}(G, E')$ is isomorphic to $X(G)$, and if t is odd, then $\tilde{X}(G, E')$ is isomorphic to $\tilde{X}(G, \{e\})$, for any edge $e \in E$. Moreover, $X(G)$ and $\tilde{X}(G, \{e\})$ are non-isomorphic.*

We will say that an edge (u, v) in G is *straight*, if the corresponding edge in $\tilde{X}(G, E')$ has not been twisted. For simplicity, we will denote by $\tilde{X}(G)$ the graph $\tilde{X}(G, \{e\})$ for some fixed $e \in E$. Since all the graphs defined in this way are isomorphic, for our purposes it does not matter which of these graphs we are considering. Analogously we will refer to the formula $F(X(G), \tilde{X}(G))$, considering that $\tilde{X}(G)$ is a fixed graph.

We extend Definition 4.4 to the set of bijections between the vertices of $X(G)$ and $\tilde{X}(G)$.

Definition 4.7 *A bijection φ between the sets $\{a^v_e, b^v_e \mid a^v_e, b^v_e \in V(X(G))\}$ and $\{a^v_e, b^v_e \mid a^v_e, b^v_e \in V(\tilde{X}(G))\}$ is called edge respecting if for every vertex v and incident edge e, $\{\varphi(a^v_e), \varphi(b^v_e)\} = \{a^v_e, b^v_e\}$ and fulfills the following property:*

For every edge $e = (u, v)$ in G, if e is straight then $\varphi(a^u_e) = a^u_e$ if and only if $\varphi(a^v_e) = a^v_e$, and if e is twisted then $\varphi(a^u_e) = a^u_e$ if and only if $\varphi(a^v_e) = b^v_e$.

For graph G, the variables in the formula $F(X(G), \tilde{X}(G))$ are of the form $x_{i,j}$ representing the mapping of vertex v_i in $X(G)$ to vertex v_j in $\tilde{X}(G)$. For clarity we will divide the set of x variables in two kinds during the exposition:

The y variables correspond to the endpoints of the original edges in G, (that have been doubled in $X(G)$). For a vertex v in G and an edge e incident with v, the vertices corresponding to v and e in $X(G)$ are $\{a^v_e, b^v_e\}$. $y_{a^v_e,b^v_e}$, for example is the variable representing the mapping from a^v_e in $X(G)$ to b^v_e in $\tilde{X}(G)$. For simplicity, when the edge is clear from the context, we will sometimes denote this variable by $y^v_{a,b}$. Also we will consider the graphs $X(G)$ and $\tilde{X}(G)$ to be colored so that for a vertex v in G and an edge e incident with v, $\{a^v_e, b^v_e\}$ are the only two vertices having the color (v,e). Since we are only interested in color preserving isomorphisms, the clause of Type 1 for a vertex a^v_e is $(y^v_{a_e,a_e} \vee y^v_{a_e,b_e})$ and has width 2 (analogous for the vertex b^v_e). This only restricts the number of possible isomorphisms and makes it easier to refute the formula.

The z variables correspond to the m vertices in the $X(v)$ gadgets. For a vertex v of degree d in G, there are 2^{d-1} vertices m^v_S, in $X(G)$ and in $\tilde{X}(G)$. The variables $z^v_{S,S'}$ are the ones representing the mappings between these vertices. Analogously as in the case of the y variables, for a vertex v we will consider that the vertices m^v_S, in $X(G)$ and $\tilde{X}(G)$ are the only ones colored with color v. This implies that the clauses of Type 1 for a vertex m^v_S have width 2^{d-1}.

For a vertex v in G we denote by $F(X(v))$ the set of initial clauses in $F(X(G), \tilde{X}(G))$ containing some variable y^v or z^v (observe that for two vertices u and v, $F(X(u))$ and $F(X(v))$ might not be disjoint. Analogously, for a set of vertices $C \subseteq V$ we denote by $F(X(C))$ the union of the clauses $F(X(v))$ for $v \in C$.

By Lemma 4.6, for any graph G, the formula $F(X(G), \tilde{X}(G))$ is unsatisfiable. However, as stated in the next lemma, for any vertex from G there are assignments satisfying simultaneously all the formula clauses except some of the clauses in $F(X(v))$.

Lemma 4.8 *For any graph $G = (V, E)$ and for every $v \in V$ there is an assignment satisfying all the clauses in $F(X(G), \tilde{X}(G))$ except two clauses in $F(X(v))$.*

Proof. Consider first the easy case in which $\tilde{X}(G)$ is the version of $X(G)$ in which exactly one edge $e = (u,v)$ is twisted, for some neighbor u of v in G. The assignment $x_{i,j} = 1$ if and only if $j = i$ satisfies all the clauses in $F(X(G), \tilde{X}(G))$ except the two Type 3 clauses $(\overline{y_{a^u_e,a^u_e}} \vee \overline{y_{a^v_e,a^v_e}})$ and $(\overline{y_{b^u_e,b^u_e}} \vee \overline{y_{b^v_e,b^v_e}})$. In the general case, by Lemma 4.6, $\tilde{X}(G)$ is isomorphic to the copy of $X(G)$ with only twisted edge $e = (u,v)$. Let φ be an isomorphism between these graphs. The assignment $x_{i,j} = 1$ if and only if $j = \varphi(i)$ satisfies all the clauses in $F(X(G), \tilde{X}(G))$ except the two Type 3 clauses $(\overline{y_{a^u_e,\varphi(a^u_e)}} \vee \overline{y_{a^v_e,\varphi(a^v_e)}})$ and $(\overline{y_{b^u_e,\varphi(b^u_e)}} \vee \overline{y_{b^v_e,\varphi(b^v_e)}})$. ■

We will show in the next section that the size of the resolution refutations of $F(X(G), \tilde{X}(G))$ for any graph G are related to the expansion of G.

Definition 4.9 *Let $G = (V, E)$ be an undirected graph with $|V| = n$. The expansion of G, $ex(G)$ is defined as:*

$$ex(G) = \min k : \ \exists S \subseteq V, |S| \in \left[\frac{n}{3}, \frac{2n}{3}\right], \ |\{(x, y) \in E : \ x \in S, y \notin S\}| = k.$$

Intuitively this represents the minimum number of edges that have to be cut in order to separate a big component of G from the rest.

5 Resolution lower bounds for color multiplicity larger than 3

We show next that for certain pairs of non-isomorphic graphs G_1, G_2, the size of any resolution refutation of $F(G_1, G_2)$ is exponential in n, the number of vertices. The proof follows the ideas introduced in [9] and [11] for proving resolution lower bounds. We will prove that for any connected graph G of minimum degree at least 2, the width of any refutation of $F(X(G)\tilde{X}(G))$ is at least the expansion of G. The lower bound on the size follows by considering a graph G with large expansion and applying Theorem 2.3.

Theorem 5.1 *Let $G = (V, E)$ be a connected graph with maximum degree d and minimum degree at least 2. Any resolution refutation of the colored version of $F(X(G), \tilde{X}(G))$ requires width at least $\frac{ex(G)}{d}$.*

Proof. Let $\mathcal{R}$ be a resolution refutation for $F(X(G), \tilde{X}(G))$. For a vertex v in G, let $G - \{v\}$ be the subgraph of G induced by the set of vertices $V \setminus \{v\}$. An assignment α of all the variables in $F(X(G), \tilde{X}(G))$ is called v-*critical*, if it satisfies all the clauses in $F(X(G), \tilde{X}(G))$ except maybe some clauses in $X(v)$. Observe that by Lemmas 4.6 and 4.8, that that there are v-critical assignments for every vertex v, and that if α is v-critical, then the number of vertices a_e^v being mapped to b_e^v for some edge e incident with v, is odd, while for every other vertex $u \neq v$ the number of such vertices is even.

We define the *significance* of a clause C in $\mathcal{R}$, abbreviated by $\sigma(C)$, as the number of vertices v such that there is a v-critical assignment, that falsifies C. It should be clear, that the initial clauses in $F(X(G), \tilde{X}(G))$ have significance 1 or 0. The empty clause, at the end of the resolution refutation $\mathcal{R}$, has significance n. Moreover, when K is the resolvent of two clauses K_1, K_2, having significance s_1 and s_2, then the significance from K is at most $s_1 + s_2$, since every assignment that falsifies K, falsifies also K_1 or K_2. From this follows, that there must be a clause C in $\mathcal{R}$ with significance $s \in [\frac{n}{3}, \frac{2n}{3}]$. (One can choose the first clause C in $\mathcal{R}$ with $\sigma(C) \geq \frac{n}{3}$). Let V' be the set of vertices

v for which there exists some v-critical assignment α, falsifying C. $|V'| = s$. For every vertex $w \in V \setminus V'$, it holds that *all* w-critical assignments satisfy clause C. Since $s \in [\frac{n}{3}, \frac{2n}{3}]$, there are at least $ex(G)$ edges joining a vertex in V' with a vertex in $V \setminus V'$. Let $e = (v, w)$ be such an edge and let d be the degree of v. We modify α in a few positions, so that it mutates to a w-critical assignment α_e: we toggle the values of the variables related to the end points of e, $y^v_{a,a}, y^v_{a,b}, y^v_{b,a}, y^v_{b,b}$, as well as toggling the values from $y^w_{a,a}, y^w_{a,b}, y^w_{b,a}, y^w_{b,b}$. Moreover, we set in α_e the values of the z variables from vertex v so that the assignment restricted to $X(v)$ defines a partial isomorphism. This is always possible since the number of vertices a^v being mapped to b^v for the edges incident with v, by α_e is even. All the other values in α are not changed in α_e. Because of this, α_e is w-critical. As a consequence of the modification, α_e satisfies the clause C. This implies that at least one of the changed variables must occur in C. Observe that for two edges $e = (v, w), e' = (v', w')$ with $v, v' \in V'$ and $w, w' \in V \setminus V'$ if $v \neq v'$ then the sets of changed variables in α_e and $\alpha_{e'}$ are disjoint. If $v = v'$ then α_e and $\alpha_{e'}$ can coincide in the values of some of the changed z variables. But v has degree at most d. This implies that for every set of d edges $e = (v, w)$ with $v \in V'$ and $w \in V \setminus V'$ a different variable must occur in C and therefore width$(C) \geq \frac{ex(G)}{d}$. ■

The lower bound follows:

Corollary 5.2 *There exists a family of graphs $\mathcal{G}$ such that for any n, $G_n \in \mathcal{G}$ has n vertices and the resolution refutation of the formula $F(X(G_n), \tilde{X}(G_n))$ expressing that the graphs $X(G_n)$ and $\tilde{X}(G_n)$ are non-isomorphic, requires size $exp(\Omega(n))$. $X(G_n)$ and $\tilde{X}(G_n)$ are colored graphs with color multiplicity at most* 4.

Proof. It is known that there are constructive families $\mathcal{G}$ of graphs of degree 3 and with an expansion that is linear in the number of vertices (see e.g. [1]). For a graph $G_n \in \mathcal{G}$ with n vertices, the graph $X(G_n)$ has $O(n)$ vertices, and color multiplicity at most 4. The formula $F(X(G_n), \tilde{X}(G_n))$ contains $O(n)$ variables and $O(n^2)$ clauses. Observe that the number of variables is linear in n because the size of the color classes is bounded. The width of these clauses is at most 4. By the above result, the width of any resolution refutation of the formula is $\Omega(n)$. By Theorem 2.3, the size of any resolution refutation of $F(X(G_n), \tilde{X}(G_n))$ is $\exp(\Omega(n))$. ■

6 Discussion

We have shown that the natural encoding of the isomorphism problem in CNF formulas requires exponential size resolution refutations for a certain family of colored graphs. These graphs have colored classes of size 4 and maximum degree 3. In contrast, when the size of the color classes is bounded by 3, the formulas have polynomial size tree-like resolution refutations. The formulas used for the lower bound are based on the CFI graphs from [12]. In these pairs of graphs, every vertex of a certain color has the same degree, the same number of neighbors of another color or the same distance to any color. Therefore, the difficulty of the resolution system in performing counting (as shown for example in the resolution lower bounds for the pigeon hole principle), is not the reason for the large refutations, since counting does not help in this context. As shown in [12], the non-isomorphic graphs we use, are indistinguishable using even inductive logic with counting. The lower bound can be explained as an "encoding" of the Tseitin tautologies (for which resolution lower bounds are known), into graph isomorphism instances. I believe that this new connection between Tseitin tautologies and isomorphism might help to solve some open question in the area of proof complexity. An example of this might be the proof of exponential lower bounds for Tseitin tautologies in stronger systems, like the cutting plane proof system. Such a result is only known for the case in which a parameter called the degree of falsity is bounded [16, 18]. Knowledge on graph isomorphism problem might help to attack the question from another perspective.

Although the main interest for the results has a theoretical motivation, the isomorphism formulas discussed here could be used as benchmarks for testing sat-solvers. To my knowledge this has only been done for formulas encoding sub-graph isomorphism [3, 4]. A way to do this, for example, would be to consider a (regular) graph and color its vertices with color classes of a bounded size. Considering then a random permutation of the vertices, one obtains an isomorphic copy of the graph. If the size of the color classes is at most 3, we know by Theorem 3.1 that there is a variable ordering under which the running time of a DPLL algorithm testing isomorphism is polynomial. For color classes of size larger than 3 we only have non trivial resolution upper bounds (that might guide the sat-solvers) for the case of the CFI graph pairs. Because of the connection between such isomorphism formulas and the Tseitin tautologies, the results from [2] relating the width of a resolution refutation for a Tseitin formula with a structural parameter (branch-width) of the underlying graph, can also be applied to the isomorphism formulas. This provides a way to design example instances for isomorphism formulas with bounded resolution width.

Acknowledgement: The author would like to thank Nicola Galesi for interesting discussions related to this paper and the anonymous reviewers for many useful suggestions.

References

[1] M. Ajtai. Recursive construction for 3-regular expanders. *Combinatorica* 14(4) 379–416, 1994.

[2] M. Alekhnovich and A. A. Razborov. Satisfiability, branch-width and Tseitin tautologies. *Computational Complexity* 20(4), 649–678, 2011.

[3] C. Anton and C. Neal. Notes on generating satisfiable SAT instances using random subgraph isomorphism. *Proc. 23rd Canadian Conference on AI*, Springer LNCS 6085, 315–318, 2010.

[4] C. Anton. An improved satisfiable SAT generator based on random subgraph isomorphism. *Proc. 24th Canadian Conference on AI*, Springer LNCS 6657, 44–49, 2011.

[5] V. Arvind, P. P. Kurur, and T.C. Vijayaraghavan. Bounded color multiplicity graph isomorphism is in the #L Hierarchy. *In Proceedings of the 20th Conference on Computational Complexity,* 13–27, 2005.

[6] L. Babai. Monte Carlo algorithms for Graph Isomorphism testing. Tech. Rep. 79-10, Dép. Math. et Stat., Univ. de Montréal, 1979.

[7] P. Beame, J.C. Culberson, D.G. Mitchell and C. Moore. The resolution complexity of random graph k-colorability. *Discrete Applied Mathematics* 153(1-3), 25–47, 2005.

[8] P. Beame, R. Impagliazzo and A. Sabharwal. The resolution complexity of independent sets and vertex covers in random graphs. *Computational Complexity* 16(3), 245–297, 2007.

[9] P. Beame and T. Pitassi. Simplified and improved resolution lower bounds. In *37th Annual IEEE Symposium on Foundations of Computer Science*, 274–282, 1996.

[10] E. Ben-Sasson, R. Impagliazzo, and A. Wigderson. Near-optimal separation of treelike and general resolution. *Combinatorica* 24(4): 585–603, 2004.

[11] E. Ben-Sasson and A. Wigderson. Short proofs are narrow – resolution made simple. *Journal of the ACM*, 48(2):149–169, 2001.

[12] J. Cai, M. Fürer and N. Immerman, An optimal lower bound on the number of variables for graph identifications. *Combinatorica* 12(4): 389-410, 1992

[13] V. Chvátal and E. Szemerédi. Many hard examples for resolution. *Journal of the ACM* 35, 759–768, 1988.

[14] M. Davis, G. Logemann and D. Loveland. A machine program for theorem proving. *Communications of the ACM* 5, 394–397, 1962.

[15] M. Furst, J. Hopcroft and E. Luks. Polynomial time algorithms for permutation groups. *Proc. 21st IEEE Symp. on Foundations of Computer Science*, 36–41, 1980.

[16] A. Goerdt. The cutting plane proof system with bounded degree of falsity. *Proc. CSL*, Springer LNCS 626, 119–133, 1991.

[17] A. Haken. The intractability of resolution. *Theoretical Computer Science*, 39(2-3):297–308, 1985.

[18] E. A. Hirsch, A. Kojevnikov, A. S. Kulikov, and S. I. Nikolenko, Complexity of semialgebraic proofs with restricted degree of falsity. *Journal on Satisfiability, Boolean Modeling and Computation*, 6, 53–69, 2008.

[19] Neil Immerman and Eric Lander, Describing graphs: a first-order approach to graph canonization, Complexity Theory Retrospective, Alan L. Selman editor, Springer 59–81 1990.

[20] B. Jenner, J. Köbler, P. McKenzie and J. Torán. Completeness results for graph isomorphism. *J. Comput. Syst. Sci.* 66(3), 549–566, 2003.

[21] J. Köbler, U. Schöning, and J. Torán. *The Graph Isomorphism problem: Its structural complexity.* Birkhauser, 1993.

[22] J.A. Robinson. A machine oriented logic based on the resolution principle. *Journal of the ACM* 12(1), 23–41, 1965.

[23] U. Schöning and J. Torán. *Das Erfllbarkeitsproblem SAT - Algorithmen und Analysen*, Lehmann 2012.

[24] J. Torán, On the hardness of Graph Isomorphism. *SIAM Journal on Computing*, 33, 5: 1093–1108, 2004.

[25] G.S. Tseitin. On the complexity of derivation in propositional calculus. In *Studies in Constructive Mathematics and Mathematical Logic, Part 2.*, pages 115–125. Consultants Bureau, 1968.

[26] A. Urquhart. Hard examples for resolution. *Journal of the ACM* 34, 209–219, 1987