The Complexity of the Hajós Calculus *

Toniann Pitassi Alasdair Urquhart

Abstract

The *Hajós Calculus* is a simple, nondeterministic procedure which generates the class of non-3-colorable graphs. Mansfield and Welsch [MW] posed the question of whether there exist graphs which require exponential-sized Hajós constructions. Unless $NP \neq coNP$, there must exist graphs which require exponential-sized constructions, but to date, little progress has been made on this question, despite considerable effort. In this paper, we prove that the Hajós Calculus generates polynomial-sized constructions for all non-3-colorable graphs if and only if Extended Frege systems are polynomially bounded. Extended Frege systems are a very powerful family of proof systems for proving tautologies, and proving superpolynomial lower bounds for these systems is a long-standing, important problem in logic and complexity theory. We also establish a relationship between a complete subsystem of the Hajós Calculus, and bounded-depth Frege systems; this enables us to prove exponential lower bounds on this subsystem of the Hajós Calculus.

Keywords. Graph constructions, complexity of propositional proof systems, 3-colorability.

AMS(MOS) subject classifications. 68R10, 03F20, 05C85.

1 Introduction

The Hajós calculus (or Hajós construction) is a simple, nondeterministic procedure for generating the class of graphs that are not k-colorable [Haj]. [1] Mansfield and Welsh [MW] have posed the problem of determining the complexity of this procedure; in particular, it is an open problem whether or not there exists a polynomial-size Hajós construction for every non-3-colorable graph. Because graph 3-colorability is NP-complete, if there were polynomial-size Hajós constructions of all non-3-colorable graphs, then $NP = coNP$, so we expect that the Hajós calculus is not polynomially bounded. However, there has been very little progress toward a proof of this conjecture, despite considerable effort.

The main result of this paper is a proof that the Hajós calculus is polynomially-bounded if and only if Extended Frege proof systems are polynomially bounded. This result links an open problem in graph theory to an important open problem in the complexity of propositional proof systems. It also shows that the complexity problem for the Hajós calculus is very difficult, since Extended Frege systems are a very powerful class of proof systems for the propositional calculus, and no techniques currently exist which appear adequate to prove super-polynomial lower bounds for them. In addition, we study a subsystem of the Hajós calculus, which is still powerful enough to generate all non-3-colorable graphs. Our results, together with recent lower bounds for bounded-depth Frege proofs ([Ajt1],[PBI],[KPW]), enables us to prove an exponential lower bound for this subsystem of the Hajós calculus.

*Author's addreses: Pitassi – University of California, San Diego, `toni@cs.ucsd.edu`; Urquhart – University of Toronto, `urquhart@cs.toronto.edu`

[1] This procedure was originally formulated due to its connection to the four color conjecture. In particular, when $k = 4$, proving that all graphs generated by the Hajós calculus are not planar is equivalent to proving the four color theorem.

In Section 2, we introduce graph calculus terminology, and prove some facts about the Hajós calculus. In Section 3, we introduce propositional proof system terminology, and prove some lemmas about Extended Frege proof systems. In Section 4, we show how to transform the rules of the Hajós calculus to obtain a propositional proof system, and analogously, how to transform the Extended Frege system into a graph calculus. We then show that there are efficient simulations between these two systems. In Section 5, we prove the main theorems, and finally in Section 6, we discuss the implications of these results for the graph-theoretical complexity problem.

2 Graph calculi and the Hajós calculus

2.1 Graph calculi

The graphs in this chapter are finite simple undirected graphs, that is, they contain no loops or multiple edges. The descriptions of the Hajós construction in the graph-theoretic literature assume that the construction operates on graphs where isomorphic copies of a graph are considered to be the same graph. However, it is more natural to think of operating on standard graphs, where each vertex is labelled with a particular positive integer, and therefore we view isomorphic graphs with different labels as different graphs. Accordingly, we define a graph G to be a pair (V, E), where V is a finite set of positive integers, and E a set of unordered pairs of elements of V; we write $e(G)$ for E, and $v(G)$ for V. Two graphs will be said to be *disjoint* if their vertex sets are disjoint. A k-coloring of a graph is an assignment of one of k distinct colors to each of the vertices of the graph; the coloring is *proper* if no two adjacent vertices receive the same color, otherwise *improper*.

A *graph calculus* is a collection of initial graphs, together with a finite collection of rules which allow us to derive new graphs. We shall restrict our attention to calculi for the class of non-3-colorable graphs. Let $\mathcal{C}$ be a particular graph calculus. A *construction* of a graph G in $\mathcal{C}$ is a sequence of graphs, ending with G, such that every graph in the sequence is either an initial graph, or follows from previous graphs by one of the rules of $\mathcal{C}$. $\mathcal{C}$ is *sound* if every graph constructed by $\mathcal{C}$ is non-3-colorable. $\mathcal{C}$ is *complete* if every non-3-colorable graph can be constructed in $\mathcal{C}$. The Hajós calculus is an example of a sound and complete graph calculus. Let $\Gamma = \{G_1, G_2, ..., G_k\}$ be a set of graphs, and let G be another graph, all with underlying vertex set V. Then Γ *implies* G, written $\Gamma \Rightarrow G$, if for all 3-colorings c of V, if c is an improper 3-coloring of every graph in Γ, then c is also an improper 3-coloring of G. A graph calculus $\mathcal{C}$, is said to be *implicationally sound* if for all $\Gamma = \{G_1, G_2, .., G_k\}$, G, if G can be constructed in $\mathcal{C}$ from Γ, then $\Gamma \Rightarrow G$. A graph calculus $\mathcal{C}$, is said to be *implicationally complete* if for all $\Gamma = \{G_1, G_2, ..., G_k\}$, G if $\Gamma \Rightarrow G$, then there is a construction in $\mathcal{C}$ of G from the graphs in Γ. We will see in the subsequent section that the Hajós calculus is not implicationally sound, but it is implicationally complete. We will also define a complete subsystem of the Hajós calculus, $\mathcal{HC}^-$, which is implicationally sound.

The *size* of a graph G is the number of its edges, that is, $|e(G)|$. The *size* of a graph calculus construction is the sum of the sizes of all graphs in the construction. The *length* of a graph calculus construction is the number of applications of rules in it. A graph calculus $\mathcal{C}$ is *polynomially bounded* if there exists a polynomial p such that every non-3-colorable graph G can be constructed in $\mathcal{C}$ with a construction of size at most $p(|e(G)|)$.

Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be two graph calculus systems. Then $\mathcal{C}_1$ *p-simulates* $\mathcal{C}_2$ if there is a polynomial-time computable function f so that for all graphs G, if s is a graph construction of G in $\mathcal{C}_2$, then $f(s)$ is a graph construction of G in $\mathcal{C}_1$. $\mathcal{C}_1$ and $\mathcal{C}_2$ are *p-equivalent* if $\mathcal{C}_1$ p-simulates $\mathcal{C}_2$, and $\mathcal{C}_2$ p-simulates $\mathcal{C}_1$.

2.2 The Hajós Calculus

In this section, we will describe the Hajós Calculus for $k = 3$; to obtain the Hajós Calculus for a different value of k, simply substitute the complete graph, K_{k+1}, for the initial graph, K_4. The set of initial graphs in the Hajós calculus contains all graphs isomorphic to K_4. There are three rules for generating new graphs:

(1) (Vertex/Edge Introduction) Add (any number of) vertices and edges.

(2) (Join rule) Let G_1 and G_2 be disjoint graphs, a_1 and b_1 adjacent vertices in G_1, and a_2 and b_2 adjacent vertices in G_2. Construct the graph G_3 from $G_1 \cup G_2$ as follows. First, remove edges $[a_1, b_1]$ and $[a_2, b_2]$; then add an edge $[b_1, b_2]$; lastly, contract vertices a_1 and a_2 into a single vertex, named a_1.

(3) (Contraction rule) Contract two nonadjacent vertices into a single vertex, and remove any resulting duplicated edges; the single vertex can be either of the two original vertices.

Since we are using labelled rather than unlabelled graphs, it might seem necessary to include a duplication rule which allows the generation of any graph isomorphic to an already constructed graph. However, the duplication rule applied to a graph G can be simulated by repeated applications of the Contraction rule, applied to G and a collection of isolated vertices. The simulating construction which results has size $O(|v(G)|^2)$, so the systems with and without the duplication rule are p-equivalent.

It is not too hard to see that any graph constructed by means of the above Hajós calculus procedure is not 3-colorable. Moreover Hajós showed [Haj] that the Hajós calculus is complete. The proof of this completeness theorem yields an algorithm which generates a Hajós construction for any non-3-colorable graph. The length of the construction, in the worst case, is exponential in the size of the graph. Mansfield and Welsh [MW] show that for a graph with less than $n^2/3$ edges, there is a Hajós construction of the graph with length at most $2^{n^2/3-|e(G)|+1} - 1$.

In earlier papers on the complexity of the Hajós calculus [MW, HRT], a different definition of Hajós calculus is given. There, a Hajós construction of a graph G is defined to be a construction of a subgraph of G using only the rules (2) and (3). However, this alternative definition results in essentially the same complexity measure. (The unwritten proof of this result is due to Jason Brown.) Additionally, in earlier formulations, the size is taken to be the length rather than the size. However, the two measures are polynomially related for the formulation of the Hajós calculus employed here.

It will be convenient for our purposes to reformulate the Hajós calculus. The system $\mathcal{HC}$ has the same set of initial graphs, as well as rules (1) and (3) of the Hajós calculus, but now rule (2) of the Hajós calculus is replaced by the following rule:

(2) (Edge Elimination rule) Let G_1 and G_2 be two graphs with common vertex set $\{v_1, ..., v_n\}$ which are identical except that G_1 contains edges $[v_1, v_2]$ and $[v_2, v_3]$ and not $[v_1, v_3]$, whereas G_2 contains edges $[v_1, v_2]$ and $[v_1, v_3]$ and not $[v_2, v_3]$. Then from G_1 and G_2, we can construct the graph G_3 which is graph G_1 with edge $[v_2, v_3]$ removed.

Claim 1 *$\mathcal{HC}$ is p-equivalent to the Hajós calculus.*

Proof. Because the only rule which differs is rule (2), it suffices to show that the join rule of the Hajós calculus can be simulated by a construction in $\mathcal{HC}$, that the Edge Elimination rule of $\mathcal{HC}$ can be simulated by a construction in the Hajós calculus, and that in each case the series of simulating steps can be constructed in polynomial time.

Let $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ be two disjoint graphs, where G_1 has a distinguished edge $[a_1, b_1]$, G_2 has a distinguished edge $[a_2, b_2]$ and G is the graph obtained from G_1 and G_2 by applying the join rule. To derive G in $\mathcal{HC}$, we first apply rules (1) and (3) to obtain an isomorphic copy, G_2^*, of G_2 in which a_2 is replaced by a_1. Then we apply rule (1) to G_1 to obtain a new graph, G_1' with underlying vertex set $(V_1 \cup V_2) - \{a_2\}$; the edges of G_1' are the edges of G_1 except for $[a_1, b_2]$, the edges of G_2^*, and the edge $[b_1, b_2]$. Similarly, we apply (1) to G_2^* to obtain the new graph G_2' where G_2' has the same vertex set as G_1', and the edge set is the same except that edge $[a_1, b_1]$ is replaced by edge $[a_1, b_2]$. We can now apply rule (2) of $\mathcal{HC}$ to G_1' and G_2' to obtain the desired graph, G.

Conversely, let G_1 and G_2 be two graphs which are identical except that G_1 contains edges $[v_1, v_2]$ and $[v_1, v_3]$ whereas G_2 contains edges $[v_1, v_2]$ and $[v_2, v_3]$. Let G be the graph obtained by applying the Edge Elimination rule. To derive G in the Hajós calculus, first apply rules (1) and (3) to generate an isomorphic copy, G_2^*, of G_2 disjoint from G_1; if v is a vertex of G_2, then v^* is the corresponding vertex of G_2^*. Second, apply the join rule to G_1 and G_2^* to obtain a new graph, G', where vertices v_3 and v_3^* are contracted to a single vertex, v_3, and which contains the edge $[v_1, v_2^*]$, but does not contain edges $[v_2^*, v_3^*]$ or $[v_1, v_3]$. G' contains two copies of each vertex other than vertex v_3; by contracting vertices v and v^* (using rule 3), we obtain the desired graph, G. $\Box$

Definition. Let the graph system $\mathcal{HC}^-$ be the system $\mathcal{HC}$ without the Contraction rule.

In [Be, pp. 352-353], it is shown that $\mathcal{HC}$ is complete. The proof actually shows the stronger result that $\mathcal{HC}^-$ is complete. The following theorem is a a new and stronger form of completeness for $\mathcal{HC}$ than in the earlier proof by Hajós. The proof of this theorem follows from our more general Theorem 3 by setting V' equal to V.

Theorem 2 *$\mathcal{HC}^-$ is implicationally complete.*

Definition. Let $\Gamma = \{G_1, ..., G_q\}$, and let $G_1, ..., G_q$ and G be graphs over vertices V, $|V| = n$. For $V' \subseteq V$, let $G^{V'}$ denote the subgraph of G over the vertices in V'. The implication $\Gamma \Rightarrow G$ is *V'-local* if there exists a subset $V' \subseteq V$ such that: (1) For all $i \leq q$, the set of edges in G_i which do not lie inside V' equals the set of edges of G which do not lie inside V', (2) If c is a 3-coloring to V', and c is a proper 3-coloring of $G^{V'}$, then c is also a proper 3-coloring of $G_j^{V'}$, for some $j \leq q$. The implication will be called V'-local when the underlying vertex set is V'.

Theorem 3 *Let $\Gamma = \{G_1, ..., G_q\}$, and let $G_1, ..., G_q$ and G be graphs over vertices V, $|V| = n$. If there exists $V' \subseteq V$, $|V'| \geq 4$ such that $\Gamma \Rightarrow G$ is V'-local, then there is a $\mathcal{HC}^-$ construction of G from Γ with size at most $O(2^{|V'|}n^2)$.*

Proof. Let $G_1, G_2, ..., G_q, G$ be graphs over vertex set V and let $G_1, ..., G_q \Rightarrow G$. A *triplet* is a subgraph consisting of three vertices and a single edge between two of the three vertices. For a fixed V, $V' \subseteq V$, $|V'| \geq 4$, $G_1, ..., G_q$, we will show that if G is a graph over V such that $G_1, ..., G_q \Rightarrow G$, and the implication is V'-local, then there exists a construction (in $|V|$) of G from $G_1, ..., G_q$ of size $O(2^{|V'|}n^2)$.

The proof is by downward induction on the number of edges in $G^{V'}$. If all edges are present in $G^{V'}$, then $G^{V'}$, and hence G must contain a K_4 subgraph, and thus can be constructed from K_4 by application of rule (1). For the inductive step, assume that we have proven the theorem for all graphs, H, with underlying vertices V, such that: (1) $G_1, ..., G_q \Rightarrow H$, and the implication is V'-local; and (2) the number of edges in $H^{V'}$ is greater than m. Now fix G such that: $G_1, ..., G_q \Rightarrow G$, the implication is V'-local, and $G^{V'}$ has m edges. There are two cases to consider: either $G^{V'}$ contains a triplet, or there are no triplets in $G^{V'}$. If $G^{V'}$ does not contain any triplets, then $G^{V'}$ is a complete k-partite graph, for some k. (This follows because if there are no triplets, then the relation "is not adjacent" is an equivalence relation.) If $k > 3$, then $G^{V'}$, and hence also G, contains a K_4 subgraph and can therefore be constructed from K_4 by rule (1). Otherwise $k \leq 3$. In this case, we will show that G contains some G_i as a subgraph. Label the maximal independent sets of $G^{V'}$ by X, Y and Z. Assume for sake of contradiction that G does not contain any of $G_1, ..., G_q$ as subgraphs. Then each G_i must contain some edge which is contained in either X, Y or Z. Now consider the 3-coloring of $G^{V'}$ which assigns all vertices of X the color red, all vertices of Y the color blue, and all vertices of Z the color green. Then this coloring properly colors $G^{V'}$, but it does not properly color any of $G_1^{V'}, ..., G_q^{V'}$. But this contradicts our assumption that $G_1, ..., G_q \Rightarrow G$ is V'-local. Thus, some G_i must be contained within G, and it follows that G can be constructed from G_i by adding edges.

The second case is when $G^{V'}$ contains at least one triplet. Consider a triplet, T, of $G^{V'}$, with vertices v_1, v_2, v_3, and edge (v_1, v_2). Let G^a be the graph G plus the additional edge (v_2, v_3), and let G^b be the graph G plus the additional edge (v_1, v_3). Because $G_1, ..., G_q \Rightarrow G$, and $G \Rightarrow G^a$, it follows that $G_1, ..., G_q \Rightarrow G^a$. By this fact, and because G^a has more than m edges, we can apply the inductive hypothesis to obtain a construction of G^a from $G_1, ..., G_q$. Similarly, we can construct G^b from $G_1, ..., G_q$. Now, by the edge elimination rule, we can construct G from G^a and G^b.

The number of intermediate graphs constructed is $O(2^{|V'|})$, and each is of size at most $O(|V|^2)$. Thus, the total size of the construction is $O(2^{|V'|}n^2)$. □

It is interesting to note that $\mathcal{HC}$ is not implicationally sound because rule (3) is not sound. However, $\mathcal{HC}^-$ is implicationally sound.

3 Propositional Proof Systems

A *propositional proof system* is a collection of initial propositional formulas (axioms), together with a set of rules which allow us to derive new propositional formulas. The propositional proof systems we consider are systems for showing formulas to be tautologies. A propositional proof system is a *Frege system* if its axioms consists of all instances of a finite number of tautologies, and it has a finite number of inference rules of a certain form which are sound (i.e. preserve truth). We shall also consider *Extended Frege systems*, in which it is possible to introduce new sentence letters as abbreviations for complex formulas. For a more in-depth treatment of propositional proof systems and their relative efficiency, see [CR].

Let $\mathcal{P}$ be a fixed propositional proof system. We say that $\mathcal{P}$ is *sound* if all of its axioms are tautologies, and its rules of inference preserve truth (for each truth assignment). If $\mathcal{P}$ is sound, and $A_1, \ldots, A_n$ and B are formulas of $\mathcal{P}$, then a *proof of B from $A_1, \ldots, A_n$ in $\mathcal{P}$* is a sequence of formulas each of which is either an axiom of $\mathcal{P}$, one of the formulas $A_1, \ldots, A_n$ or derived from earlier formulas in the sequence by one of the rules of $\mathcal{P}$, and in which the last formula is B. We write $A_1, \ldots, A_n \vdash_{\mathcal{P}} B$ if there is a proof of B from $A_1, \ldots, A_n$ in $\mathcal{P}$. The *size* of a proof is defined to be the number of occurrences of symbols in it. If $\Gamma \cup \{A\}$ is a set of formulas, then we write $\Gamma \models A$ if A is a logical consequence of the set of formulas Γ. A proof system $\mathcal{P}$ is *complete* if every tautology has a proof in $\mathcal{P}$; $\mathcal{P}$ is *implicationally complete* if $\Gamma \vdash_{\mathcal{P}} B$ whenever $\Gamma \models B$.

Let $\mathcal{P}_1$ and $\mathcal{P}_2$ be two propositional proof systems which share a common language. The system $\mathcal{P}_1$ *p-simulates* $\mathcal{P}_2$ if there is a polynomial-time computable function f so that for all formulas A, if P is a proof in $\mathcal{P}_2$ of A, then $f(P)$ is a proof of A in $\mathcal{P}_1$. If $\mathcal{P}_1$ p-simulates $\mathcal{P}_2$, then there is a polynomial p so that if there is a proof of A in $\mathcal{P}_2$ of size m, then there is also a proof of A in $\mathcal{P}_1$ of size at most $p(m)$. Two proof systems are *p-equivalent* if they p-simulate each other.

Several of the proof systems we consider in this paper operate with formulas in disjunctive normal form. A *DNF formula* is a finite disjunction of a set of *terms*, each of which is a conjunction of a set of literals (variables or their negations). The complement of a literal l is written as $\overline{l}$. A term will be written in the form $\bigwedge X$, where X is a set of literals, or by juxtaposing literals, as in $l_1 l_2 \ldots l_k$. Disjunctions are written as $\bigvee X$, or in the form $l_1 \vee \ldots \vee l_k$. If X is a set of terms, and l a literal, then Xl will stand for the set of all terms Al, where A is a term in X.

If A is a formula in conjunctive normal form, then $\sim A$ is defined to be the formula in disjunctive normal form equivalent to the negation of A, that is, the formula resulting from A by replacing $\vee$ by $\wedge$, $\wedge$ by $\vee$, and literals by their complements. If l, m, n are literals, then the notation $l \leftrightarrow (m \vee n)$ will be used as an abbreviation for $(\overline{l} \vee m \vee n) \wedge (\overline{m} \vee l) \wedge (\overline{n} \vee l)$ and $(A_1, \ldots, A_k) \supset B$ as an abbreviation for $\sim A_1 \vee \ldots \vee \sim A_k \vee B$.

If A, B are formulas, then $A[B/p]$ is defined to be the formula which results from A by substituting B for every occurrence of the variable p in A. If Γ is a set of formulas, then $\Gamma[B/p]$ is the set of all formulas $A[B/p]$ for A in Γ.

Let f be a DNF formula. Then the formula $f[1/p]$ denotes the formula obtained from f by removing all terms which contain $\overline{p}$, and then removing all occurrences of p. If the resulting formula is the empty disjunction, then $f[1/p]$ is defined to be $(p \wedge \overline{p})$; if the resulting formula contains an empty conjunction, then $f[1/p]$ is defined to be $(p \vee \overline{p})$. Similarly, the formula $f[0/p]$ denotes the formula obtained from f by removing all terms which contain p, and then removing all occurrences of $\overline{p}$. If the resulting formula is the empty disjunction, then $f[0/p]$ is defined to be $(p \wedge \overline{p})$; if the resulting formula contains an empty conjunction, then $f[0/p]$ is $(p \vee \overline{p})$. If f is a CNF formula, then $f[1/p]$, and $f[0/p]$ are defined similarly. Lastly, if Γ is a set of formulas, then $\Gamma[0/p]$ ($\Gamma[1/p]$) is the set of all formulas $A[0/p]$ ($A[1/p]$), for $A \in \Gamma$.

3.1 A depth-2 Frege system

The system $\mathcal{F}_2$ is a proof system for DNF formulas, where a term in a DNF formula will be viewed as an AND of an ordered set of literals. The proof system $\mathcal{F}_2$ has a single axiom schema, $p \vee \overline{p}$, and the following five rules. In applying the rules of $\mathcal{F}_2$ and the other systems we consider, the associative and commutative laws for disjunction will be applied tacitly. We will also assume the following generalized commutativity rule for conjunction: $(l_1 \wedge l_2 \wedge ... \wedge l_q) \vee B \Rightarrow (\pi(l_1) \wedge \pi(l_2) \wedge ... \wedge \pi(l_q)) \vee B$, where π is a bijection from $\{l_1, ..., l_q\}$ to $\{l_1, ..., l_q\}$.

$(R0)$ $A \vee A \vee B \Rightarrow A \vee B$, and $A \vee A \Rightarrow A$,

$(R1)$ $A \Rightarrow A \vee B$,

$(R2)$ $AB \vee C \Rightarrow A \vee C$,

$(R3)$ $(A \vee C), (B \vee C) \Rightarrow AB \vee C$,

$(R4)$ $A \vee l, B \vee \overline{l} \Rightarrow A \vee B$,

Theorem 4 *$\mathcal{F}_2$ is implicationally complete for DNF formulas.*

Proof. We prove that if $\Gamma \models A$, then $\Gamma \vdash_{\mathcal{F}_2} A$ by induction on the number of variables in $\Gamma \cup \{A\}$. We will need the following claim, which is proven by induction on the length of the derivation of B from $\Gamma \cup \{A\}$.

Claim. *If $\Gamma, A \vdash_{\mathcal{F}_2} B$, then $\Gamma, A \vee C \vdash_{\mathcal{F}_2} B \vee C$.*

If there is exactly one variable in $\Gamma \cup \{A\}$, and $\Gamma \models A$, then there are two cases to consider. (1) If A is equivalent to 0, p or $\neg p$, then it can be checked that in all cases, we can derive A from Γ. (2) Otherwise, A is equivalent to 1 in which case it is of the form $(pp..p) \vee (\overline{pp}..\overline{p}) \vee B$, and therefore follows from the axiom plus rules $R1$ and $R3$.

Assume that the theorem holds for n variables, that $\Gamma \cup \{A\}$ contains $n+1$ variables, and $\Gamma \models A$. Let p be a variable occurring in A. Then without loss of generality, A can be written in the form $\bigvee Xpp..p \vee \bigvee Y\overline{pp}..\overline{p} \vee \bigvee Z$, where p and $\overline{p}$ do not occur in X, Y or Z. By assumption,

$$\Gamma[1/p] \vdash_{\mathcal{F}_2} \bigvee X \vee \bigvee Z; \qquad \Gamma[0/p] \vdash_{\mathcal{F}_2} \bigvee Y \vee \bigvee Z.$$

By applying the rules $R2$ and $R4$, the set of formulas $\Gamma[1/p]$ can be deduced from $\Gamma \cup \{p\}$; similarly, $\Gamma[0/p]$ can be deduced from $\Gamma \cup \{\overline{p}\}$. Thus, by $R1$ and $R3$,

$$\Gamma, p \vdash_{\mathcal{F}_2} \bigvee Xp \vee \bigvee Z; \qquad \Gamma, \overline{p} \vdash_{\mathcal{F}_2} \bigvee Y\overline{p} \vee \bigvee Z.$$

Hence, by the preceding claim,

$$\Gamma, p \vee \overline{p} \vdash_{\mathcal{F}_2} \bigvee Xp \vee \bigvee Z \vee \overline{p}; \qquad \Gamma, p \vee \overline{p} \vdash_{\mathcal{F}_2} \bigvee Y\overline{p} \vee \bigvee Z \vee p.$$

Since $p \vee \overline{p}$ is an axiom, $\Gamma \vdash_{\mathcal{F}_2} \bigvee Xp \vee \bigvee Y\overline{p} \vee \bigvee Z$ by $R4$ and $R0$. Then by repeated application of $R0$, $R2$ and $R3$, we have $\Gamma \vdash_{\mathcal{F}_2} A$. □

3.2 A depth-d Frege System

By adding a few more rules to the depth-2 Frege system, $\mathcal{F}_2$, we can define a more general Frege system, $\mathcal{F}$, over the basis AND, OR and NOT. We define the rules of this system to be the rules $R0 - R4$ of $\mathcal{F}_2$, plus the following rules $R5 - R9$. The symbol $\Leftrightarrow$ indicates that the rule may be applied either from left to right ($\Rightarrow$), or from right to left ($\Leftarrow$). In all rules $R0 - R9$, the formulas A, B and C are arbitrary formulas over the basis $\vee$, $\wedge$ and $\neg$, where AND and OR are unbounded-fanin boolean functions, and NOT is defined as usual.

$(R5)$ $A \wedge (B_1 \vee ... \vee B_k) \Leftrightarrow (A \wedge B_1) \vee ... \vee (A \wedge B_k)$,

$(R6)$ $A \vee (B_1 \wedge ... \wedge B_k) \Leftrightarrow (A \vee B_1) \wedge ... \wedge (A \vee B_k)$,

$(R7)$ $\neg(A_1 \vee ... \vee A_k) \Leftrightarrow \neg A_1 \wedge ... \wedge \neg A_k$,

$(R8)$ $\neg(A_1 \wedge ... \wedge A_k) \Leftrightarrow \neg A_1 \vee ... \vee \neg A_k$,

$(R9)$ $\neg\neg A \Leftrightarrow A$.

The *depth* of a formula is the depth of the boolean tree which represents the formula. We define a depth-d proof of a formula, A, to be a proof in the above Frege system, where each formula occuring in the proof has depth at most d. Alternatively, the *depth-d Frege system*, $\mathcal{F}_d$, is the system $\mathcal{F}$, where each formula is restricted to have depth at most d.

3.3 Proof systems with extension

Given a proof system, a natural and powerful way to extend it is to add a rule by which a complex formula can be abbreviated by a single variable.

Let $\mathcal{S}$ be any standard Frege system where no restrictions are placed on the depth of formulas (ie., the system $\mathcal{F}$). The *extended version of* $\mathcal{S}$, or $\mathcal{ES}$, is the system which results from $\mathcal{S}$ by allowing as steps in derivations lines of the form $p \leftrightarrow A$, where p is a variable that does not appear in A, nor does p appear in earlier lines, in the assumptions, or the conclusion of the derivation. Such a system is an *Extended Frege system.* Cook and Reckhow [CR] show that any two Extended Frege systems are p-equivalent, so that the results of this paper do not depend on the formal details of a particular system.

In the case of the system $\mathcal{F}_2$, it is more convenient to introduce a form of the extension rule similar to that originally used by Tseitin [Tse] in the context of resolution systems. Let V be a set of variables, and $p_1, \ldots, p_k$ a set of new variables disjoint from those in V. Then $D_1, \ldots, D_k$ is an *extension sequence* for V if for each i, D_i is $p_i \leftrightarrow (l_1 \vee l_2 \vee ... \vee l_q)$, where $l_1, ..., l_q$ are literals which involve variables from $V \cup \{p_1, \ldots, p_{i-1}\}$. We define an $\mathcal{EF}_2$ *proof* of a DNF formula A to be a proof in $\mathcal{F}_2$ of the formula $(D_1, \ldots, D_k) \supset A$, where $D_1, \ldots, D_k$ is an extension sequence for the variables occurring in A.

Although $\mathcal{EF}_2$ only allows proofs of formulas in DNF, $\mathcal{EF}_2$ can be considered as a general proof system for propositional formulas by using the idea of extension. Let A be a propositional formula; for definiteness, let us take A to contain only the connectives $\neg$ and $\vee$. Associate a literal l_B with each subformula B of A so that: (1) the variables in A are associated with themselves; (2) if B has the associated literal l_B, then $\neg B$ has $\overline{l_B}$ as its associated literal; (3) distinct subformulas are associated with distinct literals. Then the *definitional set* for A, $Def(A)$, is the set of all formulas of the form $l_{B \vee C} \leftrightarrow (l_B \vee l_C)$, where $B \vee C$ is a subformula of A. Then we define an $\mathcal{EF}_2$ proof of the formula A to be a proof in $\mathcal{EF}_2$ of $(\bigwedge Def(A) \supset l_A)$.

Lemma 5 *The system $\mathcal{EF}_2$ p-simulates any Extended Frege system.*

Proof. Let $\mathcal{ES}$ be a fixed Extended Frege system, d a derivation of A in $\mathcal{ES}$, and $Def(d)$ the union of all the definitional sets $Def(B)$, where B is a line of d. It can be shown by induction on the length of d that for every line B in d, there is a derivation in $\mathcal{F}_2$ of $Def(d) \supset l_B$; hence there is a derivation d' in $\mathcal{EF}_2$ of A. The new derivation d' can be constructed in polynomial time from the old derivation d, so that $\mathcal{EF}_2$ p-simulates $\mathcal{ES}$. This proof is essentially the same as the proof by Cook and Reckhow [CR] of the corresponding result for Extended resolution. $\square$

3.4 Systems with substitution rules

Another natural and powerful rule used in many propositional proof systems is the the rule of substitution: ¿From A derive $A[B/p]$, where p is a variable, B any formula. This rule is unsound (except if A is required to be a tautology), so that systems including this rule no longer qualify as Frege systems. If $\mathcal{G}$ is a Frege system, then we write $\mathcal{SG}$ for the system which results from $\mathcal{G}$ by adding the rule of substitution. Such systems are called *Frege systems with substitution* by Cook and Reckhow [CR], who prove that any such system can p-simulate any Extended Frege system. [2]

A weak form of the substitution rule is the rule which allows the substitution of the constants 0 and 1 for all occurrences of a propositional variable. This form of the rule we shall call the *{0,1}-substitution rule*. If $\mathcal{G}$ is a Frege system, we write $\mathcal{S}_{0,1}\mathcal{G}$ for the system which results by adding the rules: $A \Rightarrow A[0/p]$, and $A \Rightarrow A[1/p]$ to $\mathcal{G}$. If we do not have the constants 0 and 1 in our system, then $A[0/p]$ and $A[1/p]$ denote the formulas obtained from A as defined earlier. The following lemma, due to Buss [Bu], states that in the context of a Frege system this weak form of the rule is (up to a polynomial) as strong as the unrestricted form of the rule. For completeness, we provide a proof of this lemma.

Lemma 6 *The system $\mathcal{S}_{0,1}\mathcal{F}_2$ p-simulates $\mathcal{EF}_2$.*

Proof. By definition, an $\mathcal{EF}_2$ proof of a formula A is a proof in $\mathcal{F}_2$ of $(D_1, \ldots, D_k) \supset A$, where $D_1, \ldots, D_k$ is an extension sequence for the set of variables in A. Thus it is sufficient to prove that if we are given a proof in $\mathcal{F}_2$ of $(D_1, \ldots, D_k) \supset A$, we can eliminate the antecedent of the conditional efficiently, using the {0,1}-substitution rule.

Let D_k be $p_k \leftrightarrow (l_1 \vee l_2 \vee \ldots \vee l_q)$. ¿From $(D_1, \ldots, D_k) \supset A$ by substituting 1 for p_k we can derive the formula $(D_1, \ldots, D_{k-1}, (l_1 \vee \ldots \vee l_q)) \supset A$; similarly, by substituting 0 for p_k we obtain the formula $(D_1, \ldots, D_{k-1}, (\overline{l_1} \wedge \ldots \wedge \overline{l_q})) \supset A$. By repeated application of $R2$, $R0$ and $R4$, we can then derive $(D_1, \ldots, D_{k-1}) \supset A$. The elimination of the hypothesis D_k takes steps of total size $O(r)$, where r is the length of the formula $(D_1, \ldots, D_k) \supset A$, so that the formula A can be derived in $\mathcal{S}_{0,1}\mathcal{F}_2$ by adding extra steps of total size $O(kr)$. □

Another restricted form of the substitution rule is the renaming rule: From A derive $A[p/q]$, where p, q are propositional variables. If $\mathcal{G}$ is a Frege system, the system which results from $\mathcal{G}$ by adding the renaming rule will be denoted by $\mathcal{RG}$. It is a surprising result of Buss [Bu4] that in the context of Frege systems the renaming rule is as powerful as the $\{0,1\}$-substitution rule (up to a polynomial).

Lemma 7 *The system $\mathcal{RF}_2$ p-simulates $\mathcal{S}_{0,1}\mathcal{F}_2$.*

Proof. The proof presented here is due to Steve Cook. We show how, given a proof of A in $\mathcal{F}_2$, and p a variable in A, we can derive $A[0/p]$ in $\mathcal{RF}_2$ in a relatively efficient way. Let $p_1, \ldots, p_k$ be the variables in A, and let p_i be the variable to be eliminated. Let the length of A be r. ¿From A we can derive $p_i \vee A[0/p_i]$ by $R0$, $R1$, and $R2$; hence by $k-1$ applications of renaming we obtain the formulas $p_1 \vee A[0/p_i]$, $p_2 \vee A[0/p_i]$, ..., $p_k \vee A[0/p_i]$. Since A is a tautology, we can derive the formula $\neg p_1 \vee \neg p_2 \vee \ldots \vee \neg p_k \vee A[0/p_i]$ by a subsidiary derivation of length $O(kr)$. Now by k applications of rule $R4$, we obtain $A[0/p_i]$, as desired. The derivation of $A[0/p_i]$ from A has size $O(r^2)$. An exactly similar process allows the derivation of the formula $A[1/p_i]$, so that the proof of simulation is complete. □

Note: In this section, we have defined all of our proof systems to be depth-2 systems for proving DNF tautologies. However, in the following sections it is more convenient to think in terms of unsatisfiable formulas in CNF. It is easy to interpret our systems as refutation systems for CNF formulas by simply replacing each AND by an OR and each OR by an AND in each rule and axiom of the system. In what follows, we will view $\mathcal{EF}_2$, $\mathcal{RF}_2$, $\mathcal{F}$ and $\mathcal{F}_2$ as refutation systems

[2] Somewhat surprisingly, the converse simulation also holds, a fact first proved by Dowd [Do], and later in [KP].

for CNF formulas. In particular, the depth-2 refutation system, $\mathcal{F}_2$, for deriving unsatisfiable CNF formulas consists of one axiom, $p \wedge \overline{p}$, and the following rules:

$(R0')$ $A \wedge A \wedge B \Rightarrow A \wedge B$,

$(R1')$ $A \Rightarrow A \wedge B$,

$(R2')$ $(A \vee B) \wedge C \Rightarrow A \wedge C$,

$(R3')$ $(A \wedge C), (B \wedge C) \Rightarrow (A \vee B) \wedge C$,

$(R4')$ $A \wedge l, B \wedge \overline{l} \Rightarrow A \wedge B$,

In addition, we have the associativity and commutativity rules for AND, as well as the following generalized rule of commutativity for OR: $(l_1 \vee ... \vee l_q) \wedge A \Rightarrow (\pi(l_1) \vee ... \vee \pi(l_q)) \wedge A$, where π is a bijection from $\{l_1, ..., l_q\}$ to $\{l_1, ..., l_q\}$.

4 Simulation Results

Using the well-known reductions between CNF unsatisfiability and graph non-3-colorability, we can translate the rules and axioms of the Hajós calculus to obtain a propositional refutation system, and similarly, we can translate the rules and axioms of $\mathcal{EF}_2$ to obtain a graph calculus. We will first review the translations between propositional formulas and graphs. Then we show that the Hajós calculus can p-simulate $\mathcal{EF}_2$, translated into a graph calculus, and conversely, that $\mathcal{EF}_2$ can p-simulate the Hajós calculus, translated into a propositional refutation system.

4.1 Translation from Propositional Formulas to Graphs

We use a reduction from the theory of NP-completeness to show the similarity between graph calculus systems and propositional refutation systems. Garey, Johnson and Stockmeyer [GJS] showed that $3SAT$ is reducible to 3-Colorability, by obtaining a polynomial-time, many-one transformation from $3CNF$ formulas to graphs. Here, we slightly modify their construction so that it is a transformation from arbitrary CNF formulas to graphs. Let f be a CNF formula, $f = C_1 \wedge C_2 \wedge ... \wedge C_p$, with underlying variables $x_1, ..., x_n$. For notational convenience, let $C_i = (l_1 \vee l_2 \vee ... \vee l_q)$. Then $Graph(f)$ consists of the following nodes, N:

$$\begin{aligned} N &= \{v1, v2, v3\} \cup \{xi, \overline{xi} \mid 1 \leq i \leq n\} \cup \\ &\quad \{a^i_j, b^i_j, c^i_j \mid 1 \leq i \leq p, 1 \leq j \leq q-1\}. \end{aligned}$$

The set E of edges for $Graph(f)$ is given by:

$$\begin{aligned} E &= \{[v1, v2], [v2, v3], [v1, v3]\} \ \cup \ \{[xi, \overline{xi}] | 1 \leq i \leq n\} \\ &\quad \cup \{[v3, xi], [v3, \overline{xi}] | 1 \leq i \leq n\} \\ &\quad \cup \{G_{C_i} \mid 1 \leq i \leq q\}, \end{aligned}$$

where for a particular clause, $C_i = (l_1 \vee l_2 \vee ... \vee l_q)$ in f, the subgraph G_{C_i} is shown in Figure 1. The superscript i has been omitted for simplicity. When C_i is just a single literal, l, then the construction for G_{C_i} simply puts l in place of c_{q-1}.

A key property of the graph G is: for each $C_i = (l_1 \vee l_2 \vee ... \vee l_q)$, a proper 3-coloring to $l_1, ..., l_q$ can be extended to a proper 3-coloring to the underlying vertices of G_{C_i} if and only if at least one of $l_1, ..., l_q$ has the same color as $v1$. The observation leads to the following lemma, which was proven in [GJS].

Theorem 8 *f is satisfiable if and only if $Graph(f)$ is 3-colorable.*

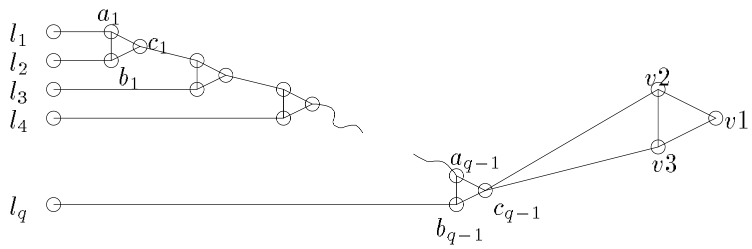

Figure 1: The subgraph G_{C_i} corresponding to C_i

4.2 Translation from Graphs to Propositional Formulas

Conversely, if G is any graph, then there exists a propositional CNF formula, $Form(G)$ with the property that G is 3-colorable if and only if $Form(G)$ is satisfiable. Let $G = (V, E)$ be a graph. We define a propositional statement, $Form(G)$, with underlying variables $\{R_x, B_x, G_x \mid x \in V\}$, which expresses "G is 3-colorable" as follows:

$$\bigwedge_{x \in V} (\overline{R}_x \vee \overline{B}_x \vee \overline{G}_x)(R_x \vee B_x \vee G_x)$$
$$(R_x \vee \overline{B}_x \vee \overline{G}_x)(\overline{R}_x \vee \overline{B}_x \vee G_x)(\overline{R}_x \vee B_x \vee \overline{G}_x)$$
$$\bigwedge_{[x,y] \in E} (\overline{R}_x \vee \overline{R}_y)(\overline{G}_x \vee \overline{G}_y)(\overline{B}_x \vee \overline{B}_y).$$

Lemma 9 *G is 3-colorable if and only if $Form(G)$ is satisfiable.*

4.3 The Simulation Lemmas

By using the translations between propositional formulas and graphs described above, we can translate the Hajós calculus to obtain a new propositional refutation system. Define $Form(\mathcal{HC})$ to be the propositional refutation system obtained by translating the rules and axioms of $\mathcal{HC}$. Specifically, $Form(\mathcal{HC})$ has one axiom: $Form(K_4)$ and three rules, obtained by translating the three rules of $\mathcal{HC}$. Similarly, define $Form(\mathcal{HC}^-)$ to be the propositional refutation system obtained by translating the rules and axioms of $\mathcal{HC}^-$. Analogously, let $Graph(\mathcal{F}_2)$ and $Graph(\mathcal{EF}_2)$ be the graph calculus system obtained by translating the rules and axioms of $\mathcal{F}_2$ and $\mathcal{EF}_2$, respectively. Then we have the following simulation lemmas.

Lemma 10 *$\mathcal{F}_2$ p-simulates $Form(\mathcal{HC}^-)$.*

Proof. $Form(\mathcal{HC}^-)$ has one axiom, $Form(K_4)$, and two rules. Because all rules and axioms of $Form(\mathcal{HC}^-)$ are sound, by the implicational completeness of $\mathcal{F}_2$ (Theorem 4), there exist $\mathcal{F}_2$ proofs of: $Form(K_4)$, as well as the two rules of $Form(\mathcal{HC}^-)$. Furthermore, because each axiom and rule of $Form(\mathcal{HC}^-)$ involves only a constant number of symbols, the size of the proofs in $\mathcal{F}_2$ are polynomial in the size of the original axiom or rule instance in $Form(\mathcal{HC}^-)$. □

Lemma 11 *$\mathcal{EF}_2$ p-simulates $Form(\mathcal{HC})$.*

Proof. We will show that $\mathcal{RF}_2$ p-simulates $Form(\mathcal{HC})$. Then because $\mathcal{EF}_2$ p-simulates $\mathcal{EF}$, and $\mathcal{EF}$ p-simulates $\mathcal{RF}_2$, it follows that $\mathcal{EF}_2$ p-simulates $Form(\mathcal{HC})$. Because $Form(\mathcal{HC}^-)$ is a subsystem of $Form(\mathcal{HC})$, and $\mathcal{F}_2$ is a subsystem of $\mathcal{RF}_2$, we only need to show how the one additional rule of $\mathcal{HC}$, the contraction rule, can be simulated by $\mathcal{RF}_2$. Since the contraction rule is just a renaming of the variables, it can be simulated by the renaming rule. □

Lemma 12 *$\mathcal{HC}$ p-simulates $Graph(\mathcal{EF}_2)$.*

Proof. We will show that $\mathcal{HC}$ p-simulates $Graph(\mathcal{RF}_2)$. By Lemmas 6 and 7, $\mathcal{RF}_2$ p-simulates $\mathcal{EF}_2$; therefore $Graph(\mathcal{RF}_2)$ p-simulates $Graph(\mathcal{EF}_2)$, and it follows that $\mathcal{HC}$ p-simulates $Graph(\mathcal{EF}_2)$. Let P be a construction of some non-3-colorable graph, G, in $Graph(\mathcal{RF}_2)$. We will prove that there exists a polynomial-sized construction of G, by induction on the number of graphs in P. If P contains just one graph, then $P = G$, and G must be the graph $Graph(p \wedge \overline{p})$. In this case, it is easy to see that this graph contains a K_4 subgraph on the vertices p, $\overline{p}$, $v2$ and $v3$, and hence can be constructed easily in $\mathcal{HC}$ Otherwise, assume that we can simulate the first k lines of P, by a polynomial-sized construction in $\mathcal{HC}$. The next graph, $Graph(f')$, is either an axiom, or it follows from previous graphs by a rule. If $Graph(f')$ is an axiom, then it can be constructed in $\mathcal{HC}$ as in the base case.

Otherwise, $Graph(f')$ follows from previous graphs by a rule. We will show that in all cases, $Graph(f')$ can be constructed efficiently in $\mathcal{HC}$. If f' follows from f by Renaming, then $Graph(f')$ can be constructed from $Graph(f)$ by rules (1) and (3). If $f' = A \wedge B$ follows from $f = A \wedge A \wedge B$ by $R0'$, then $Graph(f')$ can be constructed from $Graph(f)$ by repeated application of the contraction rule. (When A is a single literal l, then $Graph(f')$ is equal to $Graph(f)$ so there is nothing to do.) If f' follows from a previous formula, f by $R1'$, then $Graph(f')$ can be constructed from $Graph(f)$ by adding additional vertices and edges. Also, the associativity and commutativity laws for AND hold because $Graph((AB)C) = Graph(A(BC))$, and also $Graph(AB) = Graph(BA)$, up to renaming of vertices. The remaining cases, $R2'$, $R3'$, $R4'$ and the commutativity laws for OR, are more complicated. The following definition and lemmas facilitate the proof of these cases.

Definition. Let G be a graph with underlying vertices $V \cup \{l_1, l_2, ..., l_k\} \cup \{v1, v2, v3\}$. Then we define the graph $G[l_i = 1]$ to be the graph G plus the additional edges $[l_i, v2]$, and $[l_i, v3]$. Any proper 3-coloring of $G[l_i = 1]$ must color l_i the same color as $v1$. Similarly, the graph $G[l_i = 2]$ equals G plus the edges $[l_i, v1]$, and $[l_i, v3]$; and $G[l_i = 3]$ is G plus the edges $[l_i, v1]$ and $[l_i, v2]$. More generally, the graph $G[l_1 = c_1, l_2 = c_2, ..., l_k = c_k]$ is equal to the graph $G'[l_k = c_k]$, where $G' = G[l_1 = c_1, ..., l_{k-1} = c_{k-1}]$. In what follows, setting $l_i = 2$ codes setting l_i to false, and setting $l_i = 1$ codes setting l_i to true.

Lemma 13 *Let $f = AC$ be a CNF formula, where $A = (l_1 \vee l_2 \vee ... \vee l_q)$, and let $G = Graph(f)$. Then $G[l_1 = 2, l_2 = 2, ..., l_q = 2]$ has a polynomial-sized $\mathcal{HC}$ construction.*

Proof. The lemma is obvious when $q = 1$. For $q \geq 2$, recall that the graph $G = Graph(f)$ contains a subgraph, G_C, for each clause C in G. In particular, the underlying subgraph corresponding to clause A, G_A contains a "rail" of triangle graphs, with underlying vertices $\{l_1, ..., l_q\} \cup \{v1, v2, v3\} \cup \{a_i, b_i, c_i \mid 1 \leq i \leq q-1\}$. (See Figure 1.)

Let $G' = G[l_1 = 2, l_2 = 2, ..., l_q = 2]$. First, we will generate the set of graphs: $\{G'[c_1 = 2, c_2 = 2, ..., c_{k-1} = 2, c_k = 1], G'[c_1 = 2, c_2 = 2, ..., c_{k-1} = 2, c_k = 3] \mid 1 \leq k \leq q-1\}$, and also the graph $G'[c_1 = 2, c_2 = 2, ..., c_{q-1} = 2]$. Because each of these graphs is non-3-colorable, we have $(\emptyset \Rightarrow H)$, for all graphs H described above. Further, the implication is $V' - local$, where $|V'| \leq 8$. Therefore, by Theorem 3, there exist polynomial-sized constructions for each of these graphs.

Secondly, we will construct the desired graph, G', from the above graphs. We will show by downward induction on k $(1 \leq k \leq q-1)$, that we can construct the graph $G'[c_1 = 2, c_2 = 2, ..., c_k = 2]$ from the previous graphs. The base case holds because the graph $G'[c_1 = 2, ..., c_{q-1} = 2]$ is in our initial set of graphs. Now fix $k < q-1$; then we want to construct the graph $H = G'[c_1 = 2, ..., c_k = 2]$. By the inductive hypothesis, assume that we have constructed the graph $H[c_{k+1} = 2]$. Additionally, we have the graphs $H[c_{k+1} = 1]$, and $H[c_{k+1} = 3]$ in our initial set of graphs. Applying the edge elimination rule three times, we can construct H from $H[c_{k+1} = 1]$, $H[c_{k+1} = 2]$, and $H[c_{k+1} = 3]$. □

Lemma 14 *Let $f = AC$, $f' = A'C$, $A = (l_1 \vee ... \vee l_q)$, and $A' = (\pi(l_1) \vee ... \vee \pi(l_q))$, where π is a permutation of $\{l_1, ..., l_q\}$. Then for each k, $1 \leq k \leq q$, there exists a polynomial-*

sized construction of $G'[l_1 = 2, ..., l_{k-1} = 2, l_k = 1]$ from G, where $G = Graph(f)$, and $G' = Graph(f')$.

Proof. Again, the lemma is obvious when $q = 1$. For $q \geq 2$, we first construct the graph $G[l_1 = 2, ..., l_{k-1} = 2, l_k = 1]$ from G by adding edges. Because there exists a proper 3-coloring of G_A consistent with $c(l_1) = c(v2), c(l_2) = c(v2), ..., c(l_k) = c(v1)$, and with b_i colored $c(v3)$ for $i \geq k$, we can apply the contraction rule to rename the vertices labelled a_i, b_i, c_i, $1 \leq i \leq q-1$, to either $v1$, $v2$ or $v3$ to obtain the graph $G''[l_1 = 2, ..., l_{k-1} = 2, l_k = 1]$, where $G'' = G \setminus e(G_A)$. (By contracting b_i to $v3$ for all $i \geq k$, we are assured that we introduce no new edges from l_i for $i > k$ to $v1$ or $v2$.) Now by adding edges and vertices to $G''[l_1 = 2, ..., l_{k-1} = 2, l_k = 1]$, we can construct the desired graph $G'[l_1 = 2, ..., l_{k-1} = 2, l_k = 1]$. □

Lemma 15 *Let $f = AC$, where $A = (l_1 \vee l_2 \vee ... \vee l_q)$, and let $G = Graph(f)$. Then there exists a polynomial-sized $\mathcal{HC}$ construction of G from the set of graphs: $\mathcal{G} = \{G[l_1 = 1], G[l_1 = 2, l_2 = 1], ..., G[l_1 = 2, ..., l_{q-1} = 2, l_q = 1], G[l_1 = 2, ..., l_q = 2]\}$.*

Proof. We will prove by downward induction on k, $0 \leq k \leq q$, that we can construct the graph $G[l_1 = 2, ..., l_k = 2]$. The base case ($k = q$) holds because $G[l_1 = 2, ..., l_q = 2]$ is an initial graph. Now fix $k < q$. By the inductive hypothesis, assume that we have constructed the graph $G[l_1 = 2, ..., l_k = 2, l_{k+1} = 2]$; also , $G[l_1 = 2, ..., l_k = 2, l_{k+1} = 1]$ is an initial graph. Therefore, by the edge elimination rule, the graph $G[l_1 = 2, ..., l_k = 2]$ can be constructed from the graphs $G[l_1 = 2, ..., l_k = 2, l_{k+1} = 2]$, and $G[l_1 = 2, ..., l_k = 2, l_{k+1} = 1]$. The number of intermediate graphs generated is $O(q)$; therefore the construction of G is polynomial-sized. □

The following four claims complete the proof of Lemma 12.

Claim 16 (Commutativity) *Let $f = AC$, $A = (l_1 \vee l_2 \vee ... \vee l_q)$, and let $f' = A'C$, $A' = (\pi(l_1) \vee \pi(l_2) \vee ... \vee \pi(l_q))$, where π is a permutation of $\{l_1, ..., l_q\}$. Then there exists a polynomial-sized $\mathcal{HC}$ construction of $G' = Graph(f')$ from $G = Graph(f)$.*

Proof. By Lemma 13, there exists a polynomial-sized construction of $G'[l_1 = 2, l_2 = 2, ..., l_q = 2]$. By Lemma 14, there exists a polynomial-sized construction of $G'[l_1 = 2, ..., l_{k-1} = 2, l_k = 1]$ for all $1 \leq k \leq q$. Therefore, by Lemma 15, there exists a polynomial-sized construction of G'. □

Claim 17 (Rule R2') *Let $f = (A \vee B)C$, and let $f' = AC$. Then there exists a polynomial-sized $\mathcal{HC}$ construction of $G' = Graph(f')$ from $G = Graph(f)$.*

Proof. Let $A = (l_1 \vee l_2 \vee ... \vee l_q)$. Then by Lemma 13, there exists a polynomial-sized $\mathcal{HC}$ construction of $G'[l_1 = 2, l_2 = 2, ..., l_q = 2]$. By the same argument as in the proof of Lemma 14, there exists a polynomial-sized $\mathcal{HC}$ construction of $G''[l_1 = 2, ..., l_{k-1} = 2, l_k = 1]$ for all $1 \leq k \leq q$, where $G'' = G \setminus e(G_{A \vee B})$ from G. Now by adding edges and vertices to $G''[l_1 = 2, ..., l_{k-1} = 2, l_k = 1]$, we can construct the graphs $G'[l_1 = 2, ..., l_{k-1} = 2, l_k = 1]$, for all $1 \leq k \leq q$. Therefore, by Lemma 15, there exists a polynomial-sized $\mathcal{HC}$ construction of G'. □

Claim 18 (Rule R3') *Let $f_1 = AC$, $f_2 = BC$, $f' = (A \vee B)C$. Then there exists a polynomial-sized $\mathcal{HC}$ construction of $G' = Graph(f')$ from $G_1 = Graph(f_1)$ and $G_2 = Graph(f_2)$.*

Proof. Let $A = (l_1 \vee l_2 \vee ... \vee l_m)$, and let $B = (l_{m+1} \vee ... \vee l_q)$. By Lemma 13, there exists a polynomial-sized $\mathcal{HC}$ construction of $G'[l_1 = 2, ..., l_q = 2]$. By the argument in the proof of Lemma 14, for all k, $1 \leq k \leq m$, there exists a polynomial-sized $\mathcal{HC}$ construction of $G'[l_1 = 2, ..., l_{k-q} = 2, l_k = 1]$ from G_1. Also, from G_2, we can easily construct $G_2[l_1 = 2, ..., l_m = 2]$ by adding edges, and then again by the proof of Lemma 14, for all k, $m+1 \leq k \leq q$, there exists a polynomial-sized $\mathcal{HC}$ construction of $G'[l_1 = 2, ..., l_{k-1} = 2, l_k = 1]$ from $G_2[l_1 = 2, ..., l_m = 2]$. Thus, by Lemma 15, there exists a polynomial-sized $\mathcal{HC}$ construction of G'. □

Claim 19 (Rule R4') *Let $f_1 = A\bar{l}$, $f_2 = Bl$, $f' = AB$. Then there exists a polynomial-sized $\mathcal{HC}$ construction of $G' = Graph(f')$ from $G_1 = Graph(f_1)$ and $G_2 = Graph(f_2)$.*

Proof. ¿From $G_1 = Graph(A\bar{l})$, we can construct the graph $G'_1 = Graph(AB\bar{l})$ by adding vertices and edges. Similarly, from $G_2 = Graph(Bl)$, we can construct the graph $G'_2 = Graph(ABl)$ by adding vertices and edges. Because $\{G'_1, G'_2\} \Rightarrow G'$, and the implication is V'-local where $|V'|$ is constant, by Theorem 3, there exists a polynomial-sized construction of G' from G'_1 and G'_2. □

5 The Main Theorem

In this section, we will prove that $\mathcal{EF}_2$ is polynomially bounded if and only if $\mathcal{HC}$ is polynomially bounded. We will first state and prove that if $\mathcal{HC}$ is polynomially bounded, then so is $\mathcal{EF}_2$ (Theorem 20). In order to prove this theorem, we begin with an unsatisfiable CNF formula f, and using the fact that $\mathcal{HC}$ is polynomially bounded, we obtain a short refutation of $Form(Graph(f))$. Since this doubly translated formula is not the same as the original formula f, we still need to show (Lemma 21) how to derive f efficiently from $Form(Graph(f))$. Similarly, to prove the other direction of the equivalence, we need to show how to derive G efficiently from $Graph(Form(G))$; this is accomplished by Lemma 26.

Theorem 20 *If $\mathcal{HC}$ is polynomially-bounded, then so is $\mathcal{EF}_2$.*

Proof. Let f be an unsatisfiable CNF formula, and assume that $\mathcal{HC}$ is polynomially-bounded. Then $Graph(f)$ is a non-3-colorable graph, and therefore, $Graph(f)$ has a polynomial-size $\mathcal{HC}$ construction. Thus, there is also a short refutation of $Form(Graph(f))$ in $Form(\mathcal{HC})$. By Lemma 11, this implies that there are polynomial-sized $\mathcal{EF}_2$ refutations of $Form(Graph(f))$. Because $\mathcal{EF}_2$ p-simulates $\mathcal{F}$ (by Lemma 5), it follows by the lemma below that we can derive a polynomial-size refutation of f in $\mathcal{EF}_2$. □

Lemma 21 *Let f be a CNF formula. Then from $Form(Graph(f))$, we can derive a depth-5 refutation of f in $\mathcal{F}$, of size polynomial in the length of f.*

Proof. First we will obtain a polynomial-sized Extended Frege proof of f; then we will see how to remove the extensions. Let $f = C_1 \wedge C_2 \wedge .. \wedge C_q$ be a CNF formula, with underlying variables $\{x_1, ..., x_n\}$. The proof follows the basic idea behind the [GJS] proof that if $Graph(f)$ is non-3-colorable, then f is unsatisfiable. We will define a particular coloring for $Graph(f)$, based on the propositional variables $\{x_1, ..., x_n\}$.

Let $C_i = (l_1 \vee l_2 \vee ... \vee l_q)$ be a clause in f, where each l_k is a literal over $\{x_1, ..., x_n\}$. We define the following extensions for all $1 \le j \le q-1$, and $1 \le k \le q$.

$$
\begin{aligned}
& R_{l_k} \leftrightarrow l_k;\ B_{l_k} \leftrightarrow \overline{l_k};\ G_{l_k} \leftrightarrow 0 \\
& R_{\overline{l_k}} \leftrightarrow \overline{l_k};\ B_{\overline{l_k}} \leftrightarrow l_k;\ G_{\overline{l_k}} \leftrightarrow 0 \\
& R_{a^i_j} \leftrightarrow (\overline{l}_1 \wedge ... \wedge \overline{l_{j+1}});\ B_{a^i_j} \leftrightarrow (l_1 \vee ... \vee l_j) \wedge \overline{l_{j+1}}; \\
& \qquad G_{a^i_j} \leftrightarrow l_{j+1} \\
& R_{b^i_j} \leftrightarrow 0;\ B_{b^i_j} \leftrightarrow l_{j+1};\ G_{b^i_j} \leftrightarrow \overline{l_{j+1}}; \\
& R_{c^i_j} \leftrightarrow (l_1 \vee ... \vee l_{j+1});\ B_{c^i_j} \leftrightarrow (\overline{l_1} \wedge ... \wedge \overline{l_{j+1}}); \\
& \qquad G_{c^i_j} \leftrightarrow 0; \\
& R_{v1} \leftrightarrow 1;\ B_{v1} \leftrightarrow 0;\ G_{v1} \leftrightarrow 0 \\
& R_{v2} \leftrightarrow 0;\ B_{v2} \leftrightarrow 1;\ G_{v2} \leftrightarrow 0 \\
& R_{v3} \leftrightarrow 0;\ B_{v3} \leftrightarrow 0;\ G_{v3} \leftrightarrow 1
\end{aligned}
$$

Now consider each clause in $Form(Graph(f))$ after applying the above extensions. It can be checked that all clauses with the exception of clauses of the form $(\overline{B_{c^i_{q-1}}} \vee \overline{B}_{v2})$ can be simplified to "true". For each i, $1 \le i \le q$, the only clause remaining is $(\overline{B_{c^i_{q-1}}} \vee \overline{B}_{v2})$, which becomes $\overline{B_{c^i_{q-1}}} = C_i$ after applying the substitution. Combining all of the C_i's, we can then derive f. Furthermore, it is not too hard to see that this derivation has depth 5, and polynomial-size.

The following lemma shows that we can remove all extensions in the above proof, without increasing the size or depth by more than a constant factor. The main idea behind the lemma is that any logarithmic-depth, polynomial-sized circuit can be converted into a polynomial-sized formula.

Definition. Let P be an Extended Frege proof. Let the variables introduced by extension axioms be $A_1, ..., A_m$, and assume that they are introduced in P in this order. Each extension variable has an associated *recursion depth*, defined as follows. The recursion depth of A_1 is $depth(A_1)$; Suppose that A_k is defined based on extension variables $A_1, ..., A_{k-1}$. Let max be the maximum recursion depth of $A_1, ..., A_{k-1}$. Then the recursion depth of A_k is $max + depth(A_k)$.

Lemma 22 *Let P be a depth-d Extended Frege proof of f such that each extension variable has recursion depth which is no greater than $\lceil log(|P|) \rceil$. Then there exists a Frege proof P' of f such that $|P'| \le p(|P|)$, where p is a fixed polynomial, independent of f, P, and P'.*

Because the recursion depth of the extension sequence defined above is 3, the above lemma implies that from $Form(Graph(f))$, there exists a constant-depth, polynomial-size refutation in $\mathcal{F}$ of f. This completes the proof of Lemma 21. □

Corollary 23 *If $\mathcal{HC}^-$ is polynomially-bounded, then so is $\mathcal{F}_5$.*

Proof of Corollary. The proof of this corollary is almost identical to the proof of Theorem 20, with $\mathcal{EF}_2$ replaced by $\mathcal{F}_5$, $\mathcal{HC}$ replaced by $\mathcal{HC}^-$, and Lemma 11 replaced by Lemma 10. □

Recently, it has been shown in [PBI,KPW] that any depth-d proof in $\mathcal{F}$ of the propositional pigeonhole principle, PHP_n, must have size at least $2^{\Omega(n^{6^{-d}})}$. This lower bound, together with the above results gives us the following corollary.

Corollary 24 *There exists a family of non-3-colorable graphs, $\{G_n \mid n \in N\}$ such that for n sufficiently large, any $\mathcal{HC}^-$ construction of G_n has size at least 2^{n^ϵ}, for some ϵ, $0 < \epsilon < 1$.*

The converse to Theorem 20. is much more surprising, because $\mathcal{HC}$ is quite simple compared to the formulation of an Extended Frege proof system.

Theorem 25 *If $\mathcal{EF}_2$ is polynomially bounded, then so is $\mathcal{HC}$.*

Proof. Let G be a non-3-colorable graph, and assume that $\mathcal{EF}_2$ is polynomially bounded. Then $Form(G)$ is an unsatisfiable formula, and therefore $Form(G)$ has a polynomial-size $\mathcal{EF}_2$ refutation. Thus there is also a polynomial-size construction of $Graph(Form(G))$ in $Graph(\mathcal{EF}_2)$. By Lemma 12, this implies that there are polynomial-size constructions of $Graph(Form(G))$ in $\mathcal{HC}$. Now by the lemma below, there is a polynomial-size $\mathcal{HC}$ construction of G from $Graph(Form(G))$. □

Lemma 26 *If G is not 3-colorable, then there exists a polynomial-sized $\mathcal{HC}$ construction of G from the graph $Graph(Form(G))$.*

Proof. Let $Graph(Form(G))$ be denoted by $H = \overline{(V_H, E_H)}$. For a particular vertex x in G, let the corresponding set of nodes in H, $\{R_x, B_x, G_x, \overline{R}_x, \overline{B}_x, \overline{G}_x\}$ be called $N(x)$. For each vertex x in G, there is a set of five clauses in $Form(G)$ which express that x is assigned to exactly one color. (Namely, they say that exactly one of the variables R_x, B_x, G_x is true.) Let $S_1(x)$ denote the induced subgraph of $Graph(Form(G))$ corresponding to these five clauses associated with

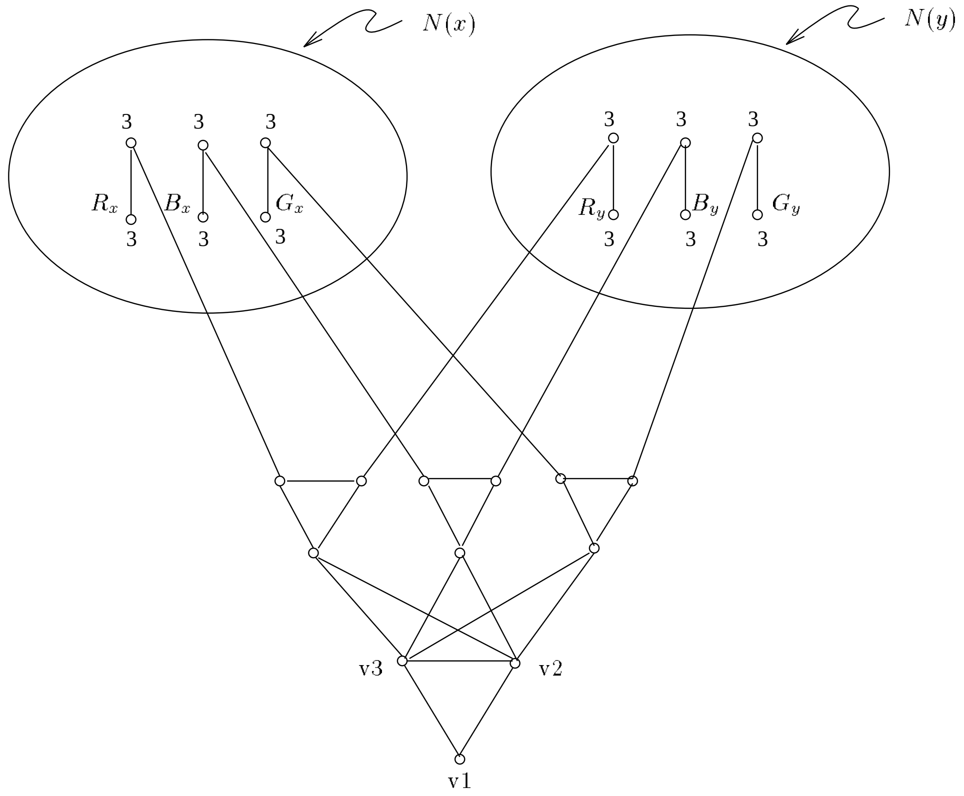

Figure 2: The subgraph $N(x, y)$

x. For any edge $[x, y]$ in G, there is a set of three clauses in $Form(G)$ which express that x and y must be assigned different colors. edge $[x, y]$ in G, let the set of Let $N(x, y)$ denote the induced subgraph of $Graph(Form(G))$ corresponding to these three clauses associated with the edge $[x, y]$. (The vertices in the subgraph $N(x, y)$ are the vertices in $N(x)$ and $N(y)$ as well as the triangle graph with underlying vertices v_1, v_2, and v_3.) Note that $N(x, y)$ is the same as $N(y, x)$ because our graphs are undirected. Figure 2 identifies $N(x, y)$ for edge $[x, y]$. Special edges that will be referred to later are labelled. For brevity, a vertex labelled by '1' indicates that this vertex is connected to vertex $v1$, and similarly for labels '2' and '3'.

The graph $G = (V_G, E_G)$ will be constructed from H in four steps.

(1) Starting with the graph $Graph(Form(G))$, we obtain an enlarged graph, H_1, by adding additional vertices and edges.

(2) From H_1, we construct the subgraph of H_1 where for each edge $[x, y]$ in G, the edges e^R_{xy}, e^B_{xy}, e^G_{xy} are removed. Call this graph H_2.

(3) From H_2, we construct the graph $G \cup T$, where T is the triangle graph, G is the graph that we would like to construct, and there are no edges between G and T.

(4) From $G \cup T$, we construct the graph G.

Step (1). We construct the graph H_1 by adding the following subgraphs to H.

(a) Add the disjoint graph G.

(b) For each vertex $x \in G$, we add a subgraph, called $S'(x)$. $S'(x)$, connects x to $N(x)$ such that if c is a proper 3-coloring of H_1 such that $c(R_x) = c(v1)$, $c(B_x) = c(v2)$, $c(G_x) = c(v2)$, then $c(x) = c(v1)$; if $c(R_x) = c(v2)$, $c(B_x) = c(v1)$, $c(G_x) = c(v2)$, then $c(x) = c(v2)$; and if $c(R_x) = c(v2)$, $c(B_x) = c(v2)$, $c(G_x) = c(v1)$, then $c(x) = c(v3)$. For node

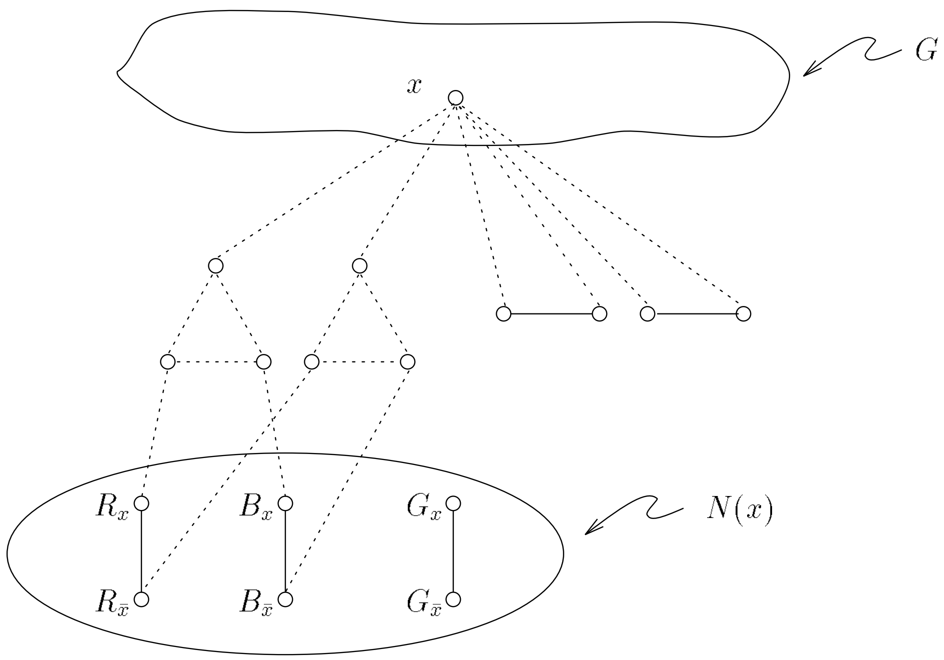

Figure 3: The subgraph $S'(x)$

x, $S'(x)$ is shown in Figure 3. Let $S(x)$ denote the induced subgraph containing all edges and vertices of $S_1(x)$ plus all edges and vertices of $S'(x)$.

(c) For each edge $[x, y]$ in G, we add a few extra vertices and edges to $N(x, y)$; let $N'(x, y)$ denote the subgraph with vertex set $N(x, y)$ plus these new vertices. For edge $[x, y]$, the extra edges and vertices are shown in Figure 4. (The new edges are indicted by dotted lines.) For each $[x, y]$, the subgraph $N'(x, y)$ has the property that if c is a 3-coloring of the vertices of $N'(x, y)$ such that the only monochromatic edge is e^R_{xy}, then both R_x and R_y have the color $c(v1)$.

Step (2). We will show how to remove the edges e^R_{xy}, e^B_{xy}, and e^G_{xy}, for all $[x, y] \in E$, one at a time. Let us begin with the graph $H_1 = (V, E)$ constructed above; we will show how to efficiently construct the graph $H_1 \setminus e^R_{xy}$, where $[x, y] \in G$. Let $W(x, y)$ be the subgraph of H_1 consisting of $\{S(x), S(y), N'(x, y), x, y\}$. Note that the size of $W(x, y)$ is constant, independent of $|V|$.

Claim 27 *If c is a 3-coloring to the vertices of $W(x, y)$ such that edge e^R_{xy} is monochromatic, then so is some other edge in $W(x, y)$*

Proof of Claim. If e^R_{xy} is monochromatic, then either some edge in $N'(x, y)$ is also monochromatic, or vertices R_x and R_y are both colored $c(v1)$. When both vertices R_x and R_y are both colored $c(v2)$ and $N'(x, y)$ is properly colored, then either some edge in $S(x)$ or $S(y)$ is monochromatic, or edge $[x, y] \in G$ is monochromatic. Thus, when edge e^R_{xy} is monochromatic, some edge in $W(x, y)$ is also monochromatic. □

The only difference between H_1 and the desired graph, $H_1 \setminus e^R_{xy}$ is the edge e^R_{xy}. Therefore, the above claim shows that $H_1 \Rightarrow H_1 \setminus e^R_{xy}$. Therefore, by Theorem 2, there exists a construction of the desired graph, $H_1 \setminus e^R_{xy}$, from H_1. Furthermore, because the implication is V'-local, where $|V'|$ is constant, by Theorem 3, the construction has polynomial size. Applying this argument repeatedly to remove all edges e^R_{xy}, e^B_{xy}, and e^G_{xy}, we will eventually obtain the desired graph H_2. After removal of e^R_{xy}, e^B_{xy}, e^G_{xy} from H_1, $N'(x, y)$ is replaced by two subgraphs, $N'_x(x, y)$ which is the empty subgraph, and $N'_y(x, y)$, which consists of $N'(x, y)$ minus the edges e^R_{xy}, e^B_{xy} and e^G_{xy}.

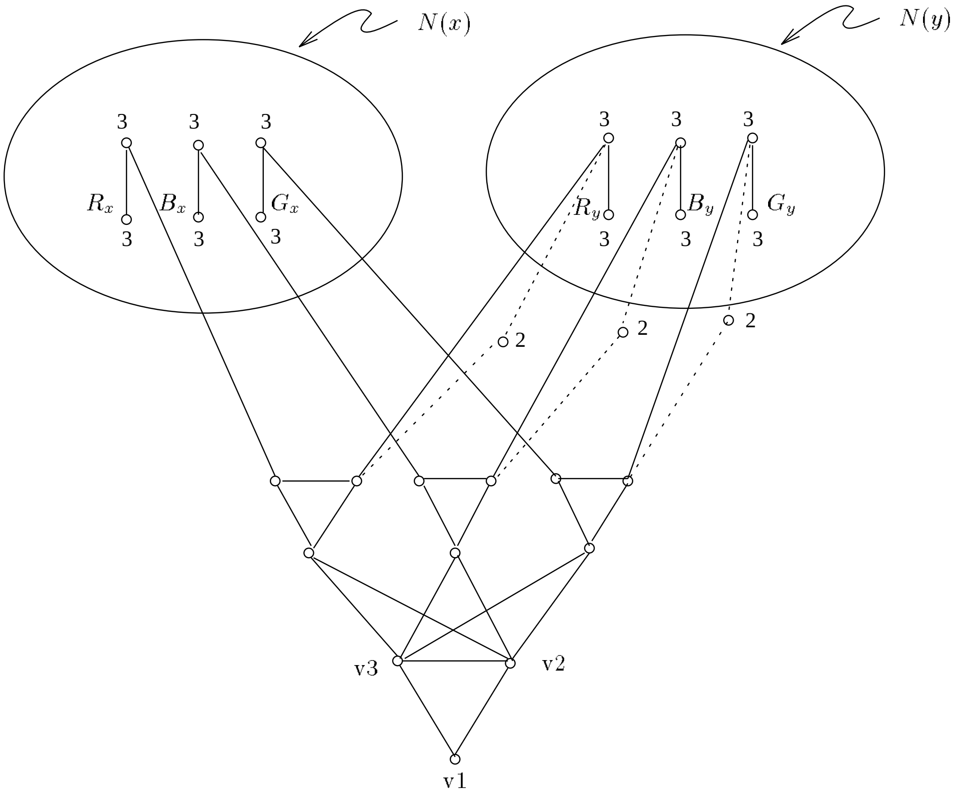

Figure 4: The subgraph $N'(x, y)$

Step (3). We will now construct the graph $G \cup T$ from H_2. For each vertex $x \in G$, let $Q(x)$ denote the induced subgraph of G containing $S(x)$ and $\{N'_x(x,y) \mid [x,y] \in G\}$. Note that for every pair $x, y \in G$, the intersection of $Q(x)$ and $Q(y)$ is the common triangle on vertices $v1$, $v2$ and $v3$. Also, note that for every $x \in G$, and for every possible coloring to $x \in G$, there exists a consistent 3-coloring to the subgraph $Q(x)$.

We will show how to eliminate the edges in $Q(x)$ from H_2, for each $x \in G$, until we eventually obtain the desired graph $G \cup T$. Let $G' = G \cup T \cup Q(x_1) \cup Q(x_2) \cup ... \cup Q(x_k)$. We will show how to construct the graph $G'' = G \cup T \cup Q(x_1) \cup ... \cup Q(x_{k-1})$ from G'. First, we construct the graph $G''[x_k = 1]$. When x_k is colored the same color as $v1$, there exists a proper 3-coloring of $Q(x_k)$. Therefore, there exists a way to rename each of the vertices in $Q(x_k) \setminus \{v1, v2, v3, x\}$ to either $v1$, $v2$, or $v3$. Applying this renaming to the graph G', we obtain the desired graph $G''[x_k = 1]$. Similarly, we can construct the graphs $G''[x_k = 2]$ and $G''[x_k = 3]$ from G'. By applying the edge elimination rule, the graph G'' can then be constructed from the three graphs $G''[x_k = 1]$, $G''[x_k = 2]$ and $G''[x_k = 3]$.

In the same manner, we can remove all $Q(x)$ to eventually obtain the graph $G \cup T$, as desired.
Step (4). The graph G is not 3-colorable, thus G contains an odd cycle. This fact, combined with the Odd-cycle Lemma below proves that from $G \cup T$, we can construct G in size linear in $|G|$. □

Lemma 28 (Odd-cycle Lemma) *Let G be a graph which contains an odd cycle, and let T be a disjoint triangle graph. Then there exists a linear-sized construction of G from $G \cup T$.*

Proof of the Odd-cycle Lemma. Label the vertices of the smallest odd cycle in G by $0, 1, 2, ..., n$, where n is even. First, we embed T into vertices $0, 1, 2$ of G (by the contraction rule) to obtain the graph G plus the edge $[0, 2]$ – call this graph G_1. Secondly, we embed T into vertices $2, 3, 4$ of G to obtain the graph G plus the edge $[2, 4]$. We can then apply Edge Elimination to these two graphs to obtain a new graph with the edge $[0, 4]$ – call this graph G_2. Thirdly, we embed T into vertices $4, 5, 6$ of G to obtain the graph G plus the edge $[4, 6]$. Again, we can apply Edge elimination to this new graph plus graph G_2 to obtain G_3 which consists of G plus the extra edge $[0, 6]$. We continue to generate G_i, $i \leq n/2$, until eventually we obtain the graph $G_{n/2}$, which consists of G plus the edge $[0, n-2]$. We then embed T in G once again, this time to the vertices $0, n, n-1$ to obtain G plus the extra edge $[0, n-1]$. We can then apply the edge elimination rule one last time to obtain the graph G. □

6 Graph-theoretical consequences

In this section, we explain a connection between our work relating the complexity of the Hajós calculus to the complexity of Extended Frege systems, and results of Stephen Cook connecting such systems with feasibly constructive arithmetic. This connection supports the belief that proving superpolynomial lower bounds for $\mathcal{HC}$ will be very difficult. More importantly, it should guide the search for hard examples for $\mathcal{HC}$.

Intuitively, a proof of a mathematical theorem is feasibly constructive if it involves only feasible predicates, and the logical reasoning in the proof involves only feasibly computable functions. (Here we are using the common identification of "feasible" with "polynomial-time computable".) In a seminal paper [C], Cook introduced a free-variable system of arithmetic, PV, which contains a primitive symbol for every polynomial-time function and predicate, together with a rule of induction on notation. Boolean connectives are included, but not quantifiers. Cook proposed to make the notion of "feasibly constructive proof" precise (at least in the case of free variable formulas) by identifying it with provability in PV.

Cook also demonstrated a close connection between PV and $\mathcal{EF}_2$. If F is a formula of PV, then there is a family F_n of formulas in DNF, in which the nth formula F_n expresses the assertion: "The formula F is true for all numerical inputs of length n or less." The formula F_n is polynomial-time computable from n and F; secondly, F is valid if and only if all of the formulas

F_n are tautologies. If in addition F is provable in PV, then even stronger consequences follow. The following basic simulation result was proved by Cook [C].

Theorem 29 *If F is provable in PV, then every F_n has a proof in $\mathcal{EF}_2$ of polynomial size.*

In later work, Buss considered more general systems of feasibly constructive mathematics [Bu2]. In particular, he investigated a system of bounded arithmetic, S_2^1, based on classical predicate logic, and containing an induction scheme restricted to NP predicates. If a primitive function symbol is added to S_2^1 for each polynomial-time function and predicate, together with appropriate defining equations for each such function and predicate, then the resulting system is a conservative extension of Cook's PV [Bu2]. This result shows that the notion of "feasibly constructive proof" is robust.

The above theorem has important consequences for proving lower bounds for $\mathcal{HC}$. Let us suppose that we have chosen a fixed method of encoding graphs as binary numbers. Then we can express the predicate "n encodes a graph" as a predicate $Graph(n)$ of PV. Furthermore, colorings can be encoded as numbers, and the predicate "c encodes a proper coloring of the graph coded by n" is polynomial-time computable, and hence can be expressed as a primitive predicate $Proper(c, n)$ of PV. We then have the following general result relating PV to $\mathcal{HC}$.

Theorem 30 *Let G be a primitive function symbol of PV for which the formulas $Graph(G(n))$, and $\neg Proper(c, G(n))$ are theorems of PV. Then there are polynomial-size $\mathcal{HC}$ constructions for the family of graphs G_n which are encoded by the numbers $G(n)$.*

Proof. By the above theorem, there is a family of tautologies F_k in which the tautology F_k formalizes the assertion that the above two theorems of PV are true when restricted to inputs of length k or less. Furthermore, this family has polynomial-size proofs in $\mathcal{EF}_2$. By choosing k large enough, we can find a tautology F_k which formalizes the assertion "G_n is not 3-colorable." Furthermore, this formula is polynomial-time computable from G_n. ¿From this formula we can derive the formula $\neg Form(G_n)$ in $\mathcal{EF}_2$ by a derivation which is polynomial in the size of G_n. The results of the previous section now imply that there is an $\mathcal{HC}$ construction of G_n whose size is polynomial in the size of the $\mathcal{EF}_2$ derivation of $\neg Form(G_n)$. $\Box$

This connection gives a very easy way to check whether or not a family of graphs is a potential candidate for proving a superpolynomial lower bound for $\mathcal{HC}$. As an example, consider the family of non-3-colorable graphs constructed by Toft which are discussed in [MW] as possible candidates for graphs which show the Hajós calculus not polynomially bounded. In fact, these graphs have short proofs by the Hajós construction, although this is not immediately obvious. However, the proof which shows all the graphs in Toft's family to be non-3-colorable is feasibly constructive, so we can infer immediately by the above result that they can be ruled out as possible hard examples. The same remark applies to other families of examples in which non-3-colorability is demonstrated by elementary constructive reasoning.

References

[Ajt1] M. Ajtai, "The complexity of the pigeonhole principle," forthcoming. Preliminary version, *29th Annual Symposium on the Foundations of Computer Science* (1988), 346-355.

[Be] C. Berge, *Graphs.* North-Holland, Amsterdam 1985.

[BIKPPW] P. Beame, R. Impagliazzo, J. Krajíček , T. Pitassi, P. Pudlák , W. Woods, "Exponential lower bounds for the pigeonhole principle," Proceedings of STOC '92.

[BPU] S. Bellantoni, T. Pitassi and A. Urquhart, "Approximation and small depth Frege proofs," Preliminary Version, *Structures in Complexity Theory* (1991), 367-391. To appear in SIAM Journal on Computing, December, 1992.

[Bu2] S. Buss, "Bounded Arithmetic," Bibliopolis, Napoli, 1986.

[Bu4] S. Buss, "Weak formal systems and connections to computational complexity," Lecture notes for a topics course, University of California, Berkeley, January-May 1988.

[C] S. Cook, "Feasibly constructive proofs and the propositional calculus," Proceedings of the Foundations of Computer Science Conference, 1975, 83-97.

[CR] S. Cook, R. Reckhow, "The relative efficiency of propositional proof systems," *Journal of Symbolic Logic*, 44, 1979, 36-50.

[Do] M. Dowd, "Model-theoretic aspects of $P \neq NP$," manuscript, 1985.

[GJS] M.R. Garey, D.S. Johnson, L. Stockmeyer, "Some simplified NP-complete graph problems," *Theoretical Computer Science*, 1, 1976, 237-267.

[Haj] G. Hajós , "Über eine Konstruktion nicht n-färbbarer Graphen," *Wiss. Zeitschr. Martin Luther Univ. Halle-Wittenberg*, A 10, 1961, 116-117.

[HRT] D. Hanson, G.C. Robinson, B. Toft, "Remarks on the graph color theorem of Hajós ," *Proceedings 17th Southeastern Conference on Combinatorics, Graph Theory and Computing*, Boca Raton, 1986, Congressus numerantium, 55 (1986), 69-76.

[KPW] J. Krajíček, P. Pudlák, A. Woods, "Exponential lower bounds to the size of bounded-depth Frege proofs of the pigeonhole principle," preprint (1991).

[Ly] J. Lynch "A Depth-Size Tradeoff for Boolean Circuits with Unbounded Fan-in," *Structures in Complexity Theory Proceedings*, Lecture Notes in Computer Science 223, Springer 1986, 234-248.

[MW] A.J. Mansfield, D.J.A. Welsh, "Some coloring problems and their complexity," *Annals of Discrete Mathematics*, 13, (1982), 159-170.

[Ore] O. Ore, *The Four-Color Problem*, Academic Press, 1967.

[PBI] T. Pitassi, P. Beame, R. Impagliazzo, "Exponential lower bounds for the pigeonhole principle," University of Toronto TR 257/91, (1991).

[PU] T. Pitassi, A. Urquhart, "The complexity of the Hajós calculus," Preliminary verison, Proceedings of the 33rd Symposium on the Foundations of Computing, 1992.