THE COMPUTATIONAL COMPLEXITY OF PROPOSITIONAL CIRQUENT CALCULUS

MATTHEW S. BAUER

University of Illinois at Urbana-Champaign, U.S.A.

Abstract. Introduced in 2006 by Japaridze, cirquent calculus is a refinement of sequent calculus. The advent of cirquent calculus arose from the need for a deductive system with a more explicit ability to reason about resources. Unlike the more traditional proof-theoretic approaches that manipulate tree-like objects (formulas, sequents, etc.), cirquent calculus is based on circuit-style structures called cirquents, in which different peer (sibling, cousin, etc.) substructures may share components. It is this resource sharing mechanism to which cirquent calculus owes its novelty (and its virtues). From its inception, cirquent calculus has been paired with an abstract resource semantics. This semantics allows for reasoning about the interaction between a resource provider and a resource user, where resources are understood in the their most general and intuitive sense. Interpreting resources in a more restricted computational sense has made cirquent calculus instrumental in axiomatizing various fundamental fragments of Computability Logic, a formal theory of (interactive) computability. The so-called “classical” rules of cirquent calculus, in the absence of the particularly troublesome contraction rule, produce a sound and complete system CL5 for Computability Logic. In this paper, we investigate the computational complexity of CL5, showing it is \( \Sigma_p^2 \)-complete. We also show that CL5 without the duplication rule has polynomial size proofs and is NP-complete.

1. Introduction

Introduced in 2006 by Japaridze [7], cirquent calculus is a refinement of classical sequent calculus. The advent of cirquent calculus arose from the need for a deductive system with a more explicit ability to reason about resources. Unlike the more traditional proof-theoretic approaches that manipulate tree-like objects (formulas, sequents, etc.), cirquent calculus is based on circuit-style structures called cirquents, in which different peer (sibling, cousin, etc.) substructures may share components. It is this resource sharing mechanism to which cirquent calculus owes its novelty (and its virtues). Cirquents come in a variety of forms. One way to characterize the sort of cirquents studied in this paper in familiar terms is to say that a cirquent is a multiset of sequents (called groups) where each formula — more precisely, each occurrence of a formula — may simultaneously belong to more than one

2012 ACM CCS: [Theory of computation]: Logic - Proof theory; Computational complexity and cryptography - Problems, reductions and completeness.

Key words and phrases: cirquent calculus, computability logic, resource semantics, proof theory, substructural logics.
sequent. This explains the origin of the word cirquent, which is a hybrid of circuit and sequent. From its inception, cirquent calculus has been paired with an abstract resource semantics. This semantics allows for reasoning about the interaction between a resource provider and a resource user, where resources are understood in their most general and intuitive sense.

Interpreting resources in a more restricted computational sense has made cirquent calculus instrumental in axiomatizing various fundamental fragments of Computability Logic, a formal theory of (interactive) computability. The so-called “classical” rules of cirquent calculus, in the absence of the particularly troublesome contraction rule, produce a sound and complete system CL5 for Computability Logic. Born in [2], Computability Logic (CoL) is an ambitious research program aimed at developing a formal theory of interactive computability. To this end, formulas of CoL represent computational problems modeled at games. The notion of “truth” for such formulas becomes synonymous with the notion of “computability” for the computational problems they represent.

While CL5 has shown to be sound and complete with respect to Japridze’s abstract resource semantics, it has also shown to validate a strictly larger class of formulas than affine logic (sequent calculus without the contraction rule), the latter being well studied and sound as a logic of resources. However, due to no shortcomings in effort, a complete resource aware semantics has not been found for affine logic. This had lead Japridze to conclude that “CL5 rather than affine logic adequately materializes the resource philosophy traditionally associated with the latter”. Indeed, the “semantics before syntax” philosophy upon which CL5 was conceived, together with its completeness result provide compelling evidence in this direction.

In parallel with the development of cirquent calculus, recent work [3–6, 10] has introduced sound and complete axiomizations for several fragments of CoL, the most fundamental of these being CL4, which contains the propositional connectives ¬ (negation), ∨ (parallel disjunction), ∧ (parallel conjunction), ⊔ (choice disjunction) and ⊓ (choice conjunction) as well as the “choice” quantifiers ⊔ and ⊓ and the “blind” quantifiers ∀ and ∃. For a full discussion of these operators and the semantics of CoL, see [9]. While the semantics of CoL differs drastically from that of classical logic, the set of valid formulas of CL4 is identical to that of classical logic when restricted to its operators and the so-called “elementary” sort of atoms. Thus, the presence of the quantifiers ∀ and ∃ within CL4’s language guarantees its undecidability. In [10], however, the ∀,∃-free fragment of CL4 was shown to be decidable in polynomial space. A PSPACE-completeness proof was later given in [11].

The deductive apparatus of CL4 is far removed from traditional Gentzen or Hilbert style axiomizations. Further, the system does not extend very naturally to other fragments of Computability Logic. A rectification to this shortcoming came with the advent of cirquent calculus. As mentioned previously, the fragment of cirquent calculus not containing the contraction rule, produces a sound and complete system for the fragment of Computability Logic known as CL5. This system contains the operators ∨, ∧ and ¬ and in this paper we show it to be Σ^p_2-complete.

We further investigate the complexity of the logical system described by the rules of CL5, but with the absence of the duplication rule. We call this logic CL5^- and show that every theorem in CL5^- has a polynomial size proof. This effectively places the problem of deciding CL5^- provability in NP. A reduction from the k vertex cover problem to CL5^- provability is then given, solidifying the logic as NP-complete. In some sense, CL5 is the CoL “counterpart” to multiplicative linear logic, the former being a proper extension of
the latter. Here, \( \text{CL}5^- \) lies strictly between multiplicative affine logic (linear logic with weakening) and \( \text{CL}5 \). Among the virtues of multiplicative affine logic is that, unlike the coNP-complete classical logic, it is in NP. \( \text{CL}5^- \) thus presents a nice and natural extension of multiplicative affine logic that gets “closer” to classical logic while still remaining in NP.

With the tight relationship between cirquent calculus and Computability Logic, one should not overlook the potential impact of cirquent calculus on other areas of logic and proof theory. In [19], Xu constructs a cirquent calculus based system for the propositional fragment of independence friendly (IF) logic, allowing one to account for independence from propositional connectives in the same vein that traditional IF logic accounts for independence from quantifiers. In [8] a cirquent calculus based proof system was developed which, among other benefits, yields polynomial size proofs for all instances of the pigeonhole principle. To date, this is the first proof system to achieve such a result without leveraging cut, extension or substitution.

This paper is organized as follows. In section 2, we provide an introduction to the rules of cirquent calculus and describe the systems \( \text{CL}5 \) and \( \text{CL}5^- \). Section 3 studies the system \( \text{CL}5^- \) and proves its NP-completeness. In the final section, we show the full \( \text{CL}5 \) to be \( \Sigma_p^2 \)-complete by a reduction from the TQBF-\( \Sigma_2 \) problem.

2. Core cirquent calculus

The present section provides the technical definitions and information necessary for understanding the results of this paper. For a full discussion of the concepts of cirquent calculus, see [7, 9]. As noted previously, a formula of the language of cirquent calculus is syntactically identical to that of classical propositional logic, where formulas are built from the connectives \( \neg, \land \) and \( \lor \) as well as non-logical atoms (also known as propositional letters). The only difference between the two being that the language of cirquent calculus does not contain logical atoms such as \( \top \) or \( \bot \); the latter can simply be understood as abbreviations of \( P \land \neg P \) and \( P \lor \neg P \), respectively, for some (whatever) atom \( P \). Our language further mandates that \( \neg \) can only be applied to atoms. As always, a literal is an atom with or without the prefix \( \neg \).

A \( k \)-ary pool, for \( k \in \mathbb{N} \), is a sequence \( \Pi_k = \langle F_1, F_2, ..., F_k \rangle \) of formulas. The formulas in a pool are not required to be unique. We refer to a particular occurrence of a formula as an oformula. A \( k \)-ary structure, for \( k \in \mathbb{N} \), is a finite sequence \( \text{St}_k = \langle \Gamma_1, \Gamma_2, ..., \Gamma_m \rangle \) for \( m \geq 0 \), where each \( \Gamma_i \), called a group of \( \text{St}_k \), is a subset of \( \{1, 2, ..., k\} \). It is permitted that \( \Gamma_i = \Gamma_j \) for \( i \neq j \) and hence we use the term ogroup to refer to a particular occurrence of a group. We are now ready to give our definition for a cirquent.

**Definition 2.1.** [7] A \( k \)-ary \((k \geq 0)\) cirquent is a pair \( C = (\text{St}_C, \Pi^C) \), where \( \text{St}_C \), called the structure of \( C \), is a \( k \)-ary structure, and \( \Pi^C \), called the pool of \( C \), is a \( k \)-ary pool.

For example, let \( \Pi^C = \langle A, B, A, D \rangle \) and \( \text{St}_C = \langle \{1, 2\}, \{2, 3\}, \{4\} \rangle \). Here, \( C \) has 4 oformulas and 3 ogroups and is typically represented by the diagram below.

```
A   B   A   D
▼ ▼ ▼ ▼
```

Following [7], we will adopt the notion that a diagram simply “is” (rather than just “represents”) a cirquent. When an ogroup $\Gamma$ is connected with an arc to an oformula $G$, we say that $\Gamma$ contains $G$.

Before defining the rules for our inference system, let us first give some additional terminology necessary for the definition of our rules. For a given cirquent, two oformulas $F$ and $G$ are called adjacent if $G$ is positioned immediately to the right of $F$. In such a case, it is said that $F$ immediately precedes $G$ and $G$ immediately follows $F$. Merging two adjacent ogroups $\Gamma$ and $\Delta$ in a given cirquent $C$ means replacing in $C$ the two ogroups $\Gamma$ and $\Delta$ by a single ogroup $\Gamma \cup \Delta$. The rightmost cirquent below represents the cirquent that results from merging the first and second ogroups in the leftmost cirquent.

Merging two adjacent oformulas $F$ and $G$ into a new oformula $H$ is the result of replacing $F$ an $G$ by $H$ and redirecting to it all of the arcs that were pointing to $F$ or $G$. The rightmost cirquent below represents the cirquent obtained from merging, in the leftmost cirquent, (the first) $A$ and $B$ into a single oformula $E$.

With these definitions in mind, we are now equipped to present the so-called “core” cirquent calculus rules. The rules we give here are only those relevant to our language and are by no means exhaustive. In its full generality, CoL encompasses numerous other logical operators all accompanied by a deep and meaningful semantics. As predicted earlier in [7], recent works have produced cirquent calculus axiomations for logics containing some of the more powerful operators of Computability Logic. See, for example, [10, 11].

2.1. Axioms (A). Axioms are rules with an empty set of premises. In cirquent calculus, they come in two forms: the empty cirquent axiom and the identity axiom. Both varieties of the axiom rule are illustrated below. It is important to note that the identity axiom is actually a scheme of infinitely many axioms, as $F$ stands for an arbitrary formula.

As will be our convention throughout, the letter placed to the right of the horizontal line represents the rule by which the conclusion was obtained.
2.2. Mix (M). The mix rule takes two premises. Its conclusion is obtained by placing each of the two premise cirquents side by side in a single cirquent, as illustrated below.

![Mix rule diagram]

The remaining rules described in subsections 2.3 to 2.8 all take a single premise cirquent.

2.3. Exchange (E). The exchange rule comes in two varieties, oformula exchange and ogroup exchange. The conclusion of the oformula exchange rule is obtained by swapping the positions of two adjacent oformulas in the premise cirquent. The ogroup exchange rule is similar in that it allows two adjacent ogroups in a premise cirquent to exchange positions in the conclusion. In both varieties of the rule, the arcs from each ogroup to its oformulas should be preserved. Below is an example of oformula (resp. ogroup) exchange in which the oformulas F and G (resp. ogroups #1 and #2) are swapped.

![Exchange rule diagrams]

2.4. Weakening (W). The weakening rule has two forms; ogroup weakening and pool weakening. In the case of ogroup weakening, the conclusion is obtained from the premise by adding a new arc between a pre-existing ogroup and oformula pair. In a application of pool weakening, the conclusion is obtained by inserting a new oformula at any position in the pool of the premise.

![Weakening rule diagrams]
2.5. **Duplication (D)**. The duplication rule can be applied in one of two ways, called *downward duplication* and *upward duplication*. The conclusion of the *downward duplication* rule is obtained from its premise by replacing an ogroup with two adjacent ogroups that each have arcs to exactly the same oformulas as the original ogroup. An application of *upward duplication* works in the opposite direction in that the premise cirquent is obtained by replacing an ogroup in the conclusion by two adjacent ogroups that are both identical to the original ogroup.

![Diagrams](downward
duplication_upward
duplication)

2.6. **Contraction (C)**. The contraction rule takes a premise cirquent which contains two adjacent and identical oformulas. The conclusion of an application of this rule is obtained from the premise by merging two adjacent and identical oformulas $F$ and $F$ into a single oformula $F$.

![Diagram](contraction)

2.7. **∨-introduction (∨)**. The conclusion of this rule is obtained from the premise by merging two adjacent oformulas $F$ and $G$ into a single oformula $F \lor G$ such that all arcs pointing to either $F$ or $G$ now point to $F \lor G$. Two examples of an application of this rule are given below.

![Diagrams](∨-introduction)
2.8. \(\land\)-introduction (\(\land\)). This rule takes a premise cirquent that contains two adjacent oformulas \(F\) and \(G\) such that no ogroup contains both \(F\) and \(G\) and every ogroup that contains \(F\) (resp. \(G\)) is immediately followed (resp. preceded) by an ogroup containing \(G\) (resp. \(F\)). The conclusion in an application of this rule is obtained from its premise by merging each ogroup that contains \(F\) with the ogroup containing \(G\) that immediately follows it. The oformulas \(F\) and \(G\) should then merge into \(F \land G\). We again give two examples below.

\[
\begin{array}{ccc}
E & F & G \\
\downarrow & \downarrow & \downarrow \\
E & F \land G \\
\end{array}
\quad
\begin{array}{cccc}
E & F & G & H \\
\downarrow & \downarrow & \downarrow & \downarrow \\
E & F \land G & H \\
\end{array}
\]

2.9. **The systems CCC, CL5 and CL5\(^{-}\).** The cirquent calculus system built from all eight of the above rules has been aptly named “Classical Cirquent Calculus”, or CCC. By removing the *contraction* rule from CCC, we get the system CL5. We further let \(\text{CL5}\(^{-}\)\) denote the system that results from additionally removing the *duplication* rule from \(\text{CL5}\).

Let \(S\) be one of the cirquent calculus systems CCC, CL5 or CL5\(^{-}\). A proof of a cirquent \(C\) in \(S\) is a tree of cirquents whose root is \(C\) where each node follows from its children by one of the rules of \(S\). When we say a formula \(F\) is provable in \(S\), we mean the cirquent containing a single oformula \(F\) with one ogroup and arc is provable in \(S\). In this paper, for simplicity, we are only interested in proving formulas, even though all of our results almost straightforwardly extend from formulas (as special cases of cirquents) to all cirquents. Correspondingly, we agree that, unless suggested otherwise by the context, “provability” means “provability of formulas”. It was shown in \([7]\) that the provable formulas of CCC coincide exactly with those of classical propositional logic. Interestingly enough, the provable formulas of CL5 can also be described in a very natural way. Because we will rely on this result and its associated concepts in several of our later proofs, we shall give the relevant details here.

A substitution for a formula \(C\) is a function \(\sigma\) that maps every atom \(P\) in \(C\) to some formula \(\sigma(P)\). If \(\sigma(P)\) is an atom for every \(P\) in \(C\), then we say that \(\sigma\) is an atomic-level substitution. This notion can be extended to all formulas by requiring that \(\sigma(\neg P) = \neg \sigma(P)\), \(\sigma(F \lor G) = \sigma(F) \lor \sigma(G)\) and \(\sigma(F \land G) = \sigma(F) \land \sigma(G)\). Let \(A\) and \(B\) be formulas. \(B\) is said to be an instance of \(A\) iff there exists a substitution \(\sigma\) such that \(\sigma(B) = A\). If \(\sigma\) is an atomic level substitution, then \(B\) is an atomic-level instance of \(A\). A formula is called binary iff no atom has more than two occurrences in it. A binary formula is said to be normal iff, whenever an atom occurs twice in the formula, one occurrence is positive and the other is negative. The following theorem is a combination of Theorem 12 and Lemma 9 of \([7]\).

**Theorem 2.2.** (Japaridze) A formula is provable in CL5 iff it is an instance of a binary tautology iff it is an atomic-level instance of a normal binary tautology.
At this point, a semantical characterization of the provable formulas of $\text{CL5}^-$ has yet to be given. In light of the results of this paper, such a finding would perhaps be very interesting.

3. CL5 without duplication is NP-complete

In this section, we show that deciding provability for a formula of the logic $\text{CL5}^-$ is NP-complete. This result is achieved by a combination of two theorems, the first of which states that every formula $F$ provable in $\text{CL5}^-$ has a proof whose size is polynomial in the size of $F$. Towards this goal, we begin by presenting a set of technical lemmas.

Lemma 3.1. Every formula provable in $\text{CL5}^-$ is an atomic-level instance of a normal binary tautology.

Proof. This follows immediately from the “$\Rightarrow$” direction of Theorem 2.2, given that the theorems of $\text{CL5}^-$ form a subset of the theorems of $\text{CL5}$.

Lemma 3.2. Let $F$ be a formula provable in $\text{CL5}^-$ with $n$ positive occurrences of atoms. No $\text{CL5}^-$ proof of $F$ can contain a cirquent with more than $n$ ogroups.

Proof. Let $F$ and $n$ be as in the condition of the lemma and let $\Delta$ be a proof tree for $F$. Assume for a contradiction that $\Delta$ has a cirquent $D$ that contains more than $n$ ogroups. Now let $\Delta'$ be the subtree of $\Delta$ rooted at $D$. A careful examination of the rules of $\text{CL5}^-$ will show that, no matter which series of rules are applied in $\Delta'$, the total number of ogroups in all the leaves of $\Delta'$ must be greater than or equal to the number of ogroups in $D$. This is because the premise cirquent(s) in the application of a $\text{CL5}^-$ rule must, together, contain at least as many ogroups as the conclusion. Every leaf in $\Delta'$ must be derived by either the identity axiom or the empty cirquent axiom and thus cannot contain more than 1 ogroup. This means $\Delta'$ has at least $n + 1$ leaves with a single ogroup, each of which must follow by the identity axiom. To be a consequence of the identity axiom, a cirquent must contain exactly two oformulas $K$ and $\neg K$. But the total number of positive occurrences of atoms in oformulas in the leaves of $\Delta$ cannot exceed $n$. This is because, by our assumption, the conclusion of $\Delta$ contains a single oformula with $n$ positive literals. Further, the oformulas of the premise cirquent(s) in the application of a $\text{CL5}^-$ rule cannot contain more positive occurrences of atoms than the oformulas of the conclusion. This means at most $n$ applications of the identity axiom are possible, contradiction.

The length of a formula $F$ is defined as the total number of occurrences of literals and connectives in $F$. The size of a cirquent is then the sum of the lengths of the oformulas in its pool plus the sum of the sizes of each ogroup in its structure. Naturally, the size of a proof is the sum of the sizes of the cirquents it contains.

Lemma 3.3. Let $F$ be a formula provable in $\text{CL5}^-$ and let $k$ be the length of $F$. There exists a $\text{CL5}^-$ proof of $F$ using $O(k^6)$ applications of rules.

Proof. Let $F$ be a formula and let $\Delta$ be a $\text{CL5}^-$ proof tree for $F$. Given $\Delta$, we show that a new proof $\Delta'$ can be obtained from $\Delta$ such that $\Delta'$ proves $F$ using $O(k^6)$ applications of rules.
The Computational Complexity of Propositional Cirquent Calculus

We begin by noting that any proof containing applications of the *empty cirquent axiom* can be transformed into one in which no applications of the rule are made. Indeed, observe that the empty cirquent can only be a (“dummy”) premise of *mix*. In such a case, the conclusion of *mix* is simply the same as its other premise. Therefore, the empty cirquent can be deleted and the application of *mix* can be skipped. This can be done for all empty cirquents contained in the proof until none remain. Let $\Delta_1$ be the proof that results from removing all applications of the *empty cirquent axiom* in the preceding manner.

Observe now that $\Delta_1$ must contain exactly one application of *conjunction introduction* or *disjunction introduction* for each occurrence of $\land$ or $\lor$ in $F$, respectively. This is because every application of either rule introduces, in its conclusion, a single $\land$ or $\lor$ connective that cannot be later removed by the application of any CL5$^-$ rule. The number of positive occurrences of atoms in $F$ also bounds the number of applications of the *identity axiom*. This is because, in a bottom up view of a proof, no CL5$^-$ rule allows formulas to be removed or merged. With the number of applications of *conjunction introduction*, *disjunction introduction* and the *identity axiom* all bounded by $O(k)$ in $\Delta_1$, we can also bound the number of applications of the *mix* rule. To see this, first note that because $\Delta_1$ contains no applications of the *empty cirquent axiom*, every leaf node must be derived by the *identity axiom*. That is, there are $O(k)$ paths from root to leaf in $\Delta_1$. Viewing the proof tree in a top down fashion, *mix* is the only CL5$^-$ rule which allows the proof tree to “branch”, given it is the only rule with more than one premise. Thus, each application of *mix*, which must take two premises, increases the number of paths from root to leaf by 1. Because the number of such paths is bounded by $O(k)$, so too must be the number of applications of the *mix* rule.

Each application of *pool weakening* introduces, in its conclusion, an oformula that must be present (perhaps only as a proper subformula of some oformula) in the conclusion of $\Delta_1$. This is because no CL5$^-$ rule can remove, in its conclusion, an oformula contained in its premise cirquent. Thus we have an immediate bound of $O(k)$ for the number of applications of *pool weakening* in $\Delta_1$. Observe that this also implies a bound of $O(k)$ on the number of oformulas contained in any cirquent. To bound the number of possible applications of *ogroup weakening* in $\Delta_1$, notice that no cirquent in $\Delta_1$ can contain more than $k^2$ arcs. This is because, by Lemma 3.2, $k$ bounds the maximum number of ogroups in any cirquent and, as noted previously, $O(k)$ bounds the number of oformulas in any cirquent. Further, *conjunction introduction* and *disjunction introduction* are the only CL5$^-$ rules whose conclusion can contain fewer arcs than its premise. The number of applications of these rules in $\Delta_1$ does not exceed $O(k)$ and each application can remove no more than the maximum $k^2$ arcs contained in any premise cirquent. Thus, no more than $O(k^3)$ total arcs can be removed from premise to conclusion for all applications of *conjunction* and *disjunction introduction* in $\Delta_1$. Each application of *ogroup weakening* creates a single arc in its conclusion that was not present in its premise. As the conclusion of $\Delta_1$ contains a single arc, no more than $O(k^3)$ arcs can be created from premise to conclusion in $\Delta_1$ by applications of *ogroup weakening*.

Every leaf of $\Delta_1$ must be derived by the *identity axiom*, which is applied at most $O(k)$ times in $\Delta_1$. That is, there are at most $O(k)$ paths from root to leaf in $\Delta_1$. Each such path $\Delta_1^i$ for $1 \leq i \leq O(k)$ contains at most $O(k^3)$ applications of CL5$^-$ rules other than oformula or ogroup exchange. Thus, any $\Delta_1^i$ can contain at most $O(k^3)$ sequences

---

\[1\] The only purpose of this axiom in [2] is to ensure the provability of the empty cirquent itself; everything else is provable without using the empty cirquent axiom.
Theorem 3.4. Let \( \Phi_w \) for \( 0 \leq w \leq O(k^3) \) where each \( \Phi_w := C^w_1, C^w_2, ..., C^w_n \) (for \( n \in \mathbb{N} \)) is a sequence of cirquents such that every cirquent \( C^w_i \) follows from \( C^w_{i+1} \) by \textit{exchange} (of either sort) for all \( 0 \leq i < n \). In \( \Delta_1 \), each \( \Phi_w \) can be of arbitrary length. We show, however, that a new proof \( \Delta' \) can be obtained from \( \Delta_1 \) such that each \( \Phi_w \) uses no more than \( O(k^2) \) applications of \textit{oformula} and \textit{ogroup exchange}. This is because, the last cirquent \( C^w_n \) in any \( \Phi_w \) can always be obtained from \( C^w_i \) using no more than \( O(k^2) \) applications of \textit{oformula} and \textit{ogroup exchange}. Let \( \Delta' \) be the CL5\(^-\) proof tree that results from replacing each \( \Phi_w \) in \( \Delta_1 \) by \( \Phi'_w \). \( \Delta' \) must again contain \( O(k) \) paths from root to leaf. Each such path now has a bound of \( O(k^3) \times O(k^2) \) applications of \textit{oformula} or \textit{ogroup exchange}, resulting in a total bound of \( O(k^6) \) applications of \textit{exchange} in all branches of \( \Delta' \).

It should be clear that if \( \Delta \) proves \( F \), then \( \Delta' \) will also prove \( F \). The number of applications of non-\textit{exchange} rules does not change from \( \Delta_1 \) to \( \Delta' \) and remains \( O(k^3) \). Further, \( \Delta' \) uses no more than \( O(k^6) \) applications of \textit{exchange}. Totaling the number of applications of every rule in \( \Delta' \), we obtain a bound of \( O(k^3) + O(k^6) \). \( \square \)

Theorem 3.5. Deciding provability for the logic CL5\(^-\) is NP-complete.

Proof. It follows from Theorem 3.4 that CL5\(^-\) provability is in NP. To see it is NP-hard, we give a polynomial time reduction \( f \) to it from the vertex cover problem. Fix some arbitrary graph \( G = (V,E) \) and some \( k \in \mathbb{N} \). The reduction, borrowed from \[12\], follows.

\[
f(V,E,k) := (\Psi(k)) \lor (\Theta(V,E)) \lor (\Omega(E))
\]

\[
\Psi(k) := q \lor q \lor ... \lor q
\]

total of \( k \) literals
\[ \Theta(V, E) := (-q \land (-v_1 \lor -v_1 \lor ... \lor -v_1)) \lor ... \lor (-q \land (-v_n \lor -v_n \lor ... \lor -v_n)) \]

for each vertex \( v_1, v_2, ..., v_n \in V \)

\[ \Omega(E) := (e_1^1 \lor e_1^2) \land (e_2^1 \lor e_2^2) \land ... \land (e_m^1 \lor e_m^2) \]

for each edge \( e_1, e_2, ..., e_m \in E, \)

Above, \( q \) is a new atom that differs from all other atoms in the formula. In \( \Omega(E) \), \( e_1^1 \) and \( e_2^2 \) are the vertices on the endpoints of edge \( e_i \) for \( 1 \leq i \leq m \). It is also important to note that each \( v_j \) for \( 1 \leq j \leq n \) represents both an atom in \( f(V, E, k) \) as well as the label of a vertex in \( G \).

Obviously the mapping \( f \) is computable in polynomial time. It now remains to show that a graph \( (V, E) \) has a \( k \) vertex cover if and only if the formula \( f(V, E, k) \) is provable in \( \text{CL}5^- \).

“⇒” Our reduction is identical to that of [12] (Section 5.2) for multiplicative affine (direct) logic. As a direct consequence of Theorem 3 from [7], \( \text{CL}5^- \) proves every formula provable in multiplicative affine logic\(^2\), so the result follows immediately.

“⇐” Assume \( f(V, E, k) \) is provable in \( \text{CL}5^- \). We need to show that there exists a \( k \) vertex cover of \( G = (V, E) \). By Theorem 2.2, there exists a normal binary tautology \( \beta \) and an atomic-level substitution \( \sigma \) such that \( \sigma(\beta) = f(V, E, k) \). Let \( \Psi' \) be the subformula of \( \beta \) such that \( \sigma(\Psi') = \Psi(k) \). Let \( \Pi \) be the set of the \( k \) atoms of \( \Psi' \), and let \( \Sigma \subseteq \Pi \) be the set of those members of \( \Pi \) that have (not only positive but also) negative occurrences of \( \beta \). For each \( l \in \Sigma \), let \( \Theta_l \) be the conjunct in the \( \Theta(V, E) \) component of \( f(V, E, k) \) that contains \( \neg \sigma(l) \). By our construction, each \( \Theta_l \) takes the form

\[ (-q \land (-v_j \lor -v_j \lor ... \lor -v_j)) \]

for \( 1 \leq j \leq n \). Define a vertex cover \( V' \subset V \) for \( G \) as the set of all vertices in \( G \) labeled \( v_j \) where \( v_j \) is contained in \( \Theta_l \) for some \( l \in \Sigma \).

To see that \( V' \) is indeed a \( k \) vertex cover for \( G \), note first that \( \sigma \) is an atomic-level substitution, and hence each positive literal \( l \in \Sigma \) must be mapped to a unique positive occurrence of \( q \) in \( f(V, E, k) \). By the definition of \( \Psi(k) \), however, there are exactly \( k \) positive occurrences of \( q \) in \( f(V, E, k) \). This means \( \Sigma \) contains no more than \( k \) atoms and subsequently the vertex cover derived from \( \Sigma \) contains no more than \( k \) vertices.

Because \( f(V, E, k) \) is an atomic-level instance of \( \beta \), both formulas take exactly the same form, the only difference being in the atoms they are built from. Let us now define a model \( ^* \) for \( \beta \). For each \( l \in \Pi \) let \( l^* = \bot \). For any atom \( l \not\in \Pi \) with the property that \( \sigma(l) = q \), let \( l^* = \top \). Further, for each atom \( l \) of \( \beta \) where \( \sigma(l) = a \) for some \( a \in V' \), let \( l^* = \top \). All remaining atoms \( l \) of \( \beta \) should be interpreted as \( l^* = \bot \).

Note that every atom \( l \) of the earlier defined \( \Phi' \) is interpreted as \( l^* = \bot \), meaning that \( (\Phi')^* = \bot \). Next let \( \Theta' \) be the subformula of \( \beta \) such that \( \sigma(\Theta') = \Theta(V, E) \). Each disjunct of \( \Theta' \) takes the form \( \neg l_1 \land (\neg l_2 \lor \neg l_3 \lor ... \lor \neg l_n) \) for some positive integer \( n \). If \( l_1 \not\in \Sigma \) then

\( \text{From Theorem 3 of [7], we have affine logic = CL5}^* \), where CL5\(^*\) is the system CL5 with the limitation that cirquents contained in proofs do not have groups that share formulas. Because upward (resp. downward) duplication is only applicable when the premise (resp. conclusion) of the rule is a cirquent in which groups share formulas, all cirquents provable in CL5\(^*\) are also provable in CL5\(^-\).
Deciding provability for the logic CL5 is $\Sigma_2^p$-complete.

This section contains our main result, namely, the $\Sigma_2^p$-completeness of the decision problem for provability of formulas in CL5.

**Lemma 4.1.** Deciding provability for CL5 is in $\Sigma_2^p$.

**Proof.** The following is a $\Sigma_2^p$ algorithm that, if view of Theorem 2.2, decides provability of a formula $G$ in CL5. On input $G$, existentially guess a binary formula $F$ such that $G$ is an instance of $F$. Then, universally guess a truth assignment $*$ for $F$. If $F$ is true under $*$, accept. Otherwise, reject.

Let TQBF-$\Sigma_2$ be the problem of deciding truth for a quantified Boolean formula of the form $\exists X \forall Y \Theta$, where $X$ and $Y$ are sequences of variables and $\Theta$ is a quantifier-free Boolean formula all of whose variables are among $X$ or $Y$. As shown in Theorem 4.1 of [15], this problem is $\Sigma_2^p$-complete. We say an atom $z$ is isolated in a formula $\phi$ if there is only a single (positive or negative) occurrence of $z$ in $\phi$. Otherwise, it is non-isolated.

**Theorem 4.2.** Deciding provability for the logic CL5 is $\Sigma_2^p$-complete.

**Proof.** By Lemma 4.1, the problem of deciding provability for CL5 is in $\Sigma_2^p$. To show it is $\Sigma_2^p$-hard, we construct a polynomial time mapping reduction $f$ from TQBF-$\Sigma_2$ to CL5-provability. We can safely restrict our attention to instances of TQBF-$\Sigma_2$ where the Boolean portion of the formula is in disjunctive normal form, as the complexity of the problem is not reduced with these limitations. Our reduction follows.

Let $\phi$ be a formula that takes the form $\exists X \forall Y \Theta$ with $X$ and $Y$ being sets of variables and $\Theta$ being a boolean formula in disjunctive normal form of whose variables are among $X \cup Y$. The following steps are used to construct the corresponding CL5 formula $f(\phi)$.

1. For each $z \in X$, let $k^z$ and $t^z$ be the number of positive occurrences of the literals $z$ and $\neg z$ in $\Theta$, respectively. Define

$$g(z) = Z^z \land (Z^z \rightarrow (u^z_1 \land u^z_2 \land \ldots \land u^z_{k^z})) \land (Z^z \rightarrow \neg v^z_1 \land \neg v^z_2 \land \ldots \land \neg v^z_{t^z})$$

where $Z^z, u^z_1, u^z_2, \ldots, u^z_{k^z}$ and $v^z_1, v^z_2, \ldots, v^z_{t^z}$ are all fresh, pairwise distinct variables, uniquely chosen for $z$. Here, if $k^z$ (resp. $t^z$) is 0, the second (resp. third) conjunct should be

\[\text{Here, fresh variables are those not occurring elsewhere in } \phi.\]
omitted. Now let \( z_1, z_2, \ldots, z_l = X \) and let \( \phi_0 \) be the formula \((g(z_1) \land g(z_2) \land \ldots \land g(z_l)) \rightarrow \Theta_1\). Here \( \Theta_1 \) is a formula derived from \( \Theta \) such that, for each \( z \in X \), every positive occurrence of \( z \) in \( \Theta \) is replaced by a unique literal from \( u^z_1, u^z_2, \ldots, u^z_k \) and every occurrence of \( \neg z \) in \( \Theta \) is replaced by a unique literal from \( \neg v^z_{1}, \neg v^z_{2}, \ldots, \neg v^z_{\ell} \).

(2) Consider any \( y \in Y \). Let \( r_y \) be the number of positive occurrences of \( y \) in \( \phi_0 \), and \( s_y \) be the number of negative occurrences. For each pair \( i, j \) with \( 1 \leq i \leq r_y \) and \( 1 \leq j \leq s_y \), we choose a fresh and unique variable \( P^y_{i,j} \). Now, define \( f(\phi) \) to be the result of replacing in \( \phi_0 \), for each \( y \in Y \), every positive occurrence of the literal \( y \) by \((P^y_{i,1} \lor P^y_{i,2} \lor \ldots \lor P^y_{i,s_y})\) and every (positive) occurrence of the literal \( \neg y \) by \((\neg P^y_{1,j} \lor \neg P^y_{2,j} \lor \ldots \lor \neg P^y_{r_y,j})\) where \( 1 \leq i \leq r_y \) (resp. \( 1 \leq j \leq s_y \)) is unique for each replacement of an occurrence of \( y \) (resp. \( \neg y \)).

“\( \Rightarrow \)”. Assume \( \phi \) is true. Then there exists some truth assignment \( \circ : X \rightarrow \{\top, \bot\} \) such that \( \Theta^\circ \) is true under any truth assignment \( \ast \) that extends \( \circ \) to \( X \cup Y \). By our assumption, \( \Theta \) is in disjunctive normal form and hence takes the form

\[
(\psi_1 \land \psi_2 \land \ldots \land \psi_n) \lor \ldots \lor (\psi_{m+1} \land \psi_{m+2} \land \ldots \land \psi_{m+l})
\]

where each \( \psi_w \) is either a positive or negative literal. Now let \( \Omega \) and \( \Sigma \) represent the antecedent and consequent of the outermost implication in \( f(\phi) \) such that \( f(\phi) = \Omega \rightarrow \Sigma \). Our construction guarantees that \( \Sigma \) takes the form

\[
(\Psi_1 \land \Psi_2 \land \ldots \land \Psi_n) \lor \ldots \lor (\Psi_{m+1} \land \Psi_{m+2} \land \ldots \land \Psi_{m+l})
\]

where each \( \Psi_w \) is a disjunction of literals (such a “disjunction” may have only a single “disjunct”). That is, \( \Sigma \) is obtained from \( \Theta \) by replacing each literal \( \psi_w \) by \( \Psi_w \), where \( \Psi_w \) is a disjunction of literals. We will henceforth use \( \psi_w \) to represent a unique position in \( \Theta \) and \( \Psi_w \) to represent the corresponding position in \( \Sigma \).

We want to show that \( f(\phi) \) is provable in CL5. By Theorem 2.2, it suffices to show that \( f(\phi) \) is an instance of a binary tautology. We construct a binary tautology \( \Phi \) of which \( f(\phi) \) is an instance. Namely, let \( \Phi \) be the formula obtained from \( f(\phi) \) as follows. For each \( z \in X \), if \( z^{\circ} = \top \) (resp. \( \bot \)) replace the third (resp. second) occurrence of \( Z^z \) by an atom \( Q^z \) such that \( Q^z \) does not occur elsewhere in \( \Phi \) and is unique for each \( z \in X \). It should be easy to see that \( \Phi \) is a quantifier free binary formula and \( f(\phi) \) is an instance of \( \Phi \). We need only show that \( \Phi \) is a tautology. Again notice that \( \Phi \) takes form \( \Phi = \Pi \rightarrow \Sigma \) where \( \Sigma \) is the same as in \( f(\phi) \).

Given \( X = z_1, z_2, \ldots, z_l \), we have \( \Pi = g(z_1)' \land g(z_2)' \land \ldots \land g(z_l)' \) where each \( g(z)' \) matches one of the following forms:

1. \( Z^2 \land (Z^2 \rightarrow u^z_1 \land u^z_2 \land \ldots \land u^z_k) \land (Q^z \rightarrow \neg v^z_1 \land \neg v^z_2 \land \ldots \land \neg v^z_{\ell}) \)
2. \( Z^2 \land (Q^z \rightarrow u^z_1 \land u^z_2 \land \ldots \land u^z_k) \land (Z^2 \rightarrow \neg v^z_1 \land \neg v^z_2 \land \ldots \land \neg v^z_{\ell}) \)

For any \( g(z)' \) in \( \Pi \) where \( z \in X \), if \( (Z^z)^* = \top \) then \( \Pi^* = \top \), and hence \( \Phi^* = \top \). If \( (Z^z)^* = \bot \), then all of the literals in the consequent of the implication in \( g(z)' \) with antecedent literal \( Z^z \) must be true under \( \ast \), otherwise we will have \( \Pi^* = \bot \) and again \( \Phi^* = \top \). Thus, we need only guarantee \( \Sigma^* = \top \) under truth assignments such that, for each conjunct \( g(z)' \) in \( \Pi \), \( Z^z \) and every literal in the consequent of the implication containing antecedent literal \( Z^z \) are true under \( \ast \).

Let \( \Theta' \) be the formula that results from replacing in \( \Theta \) every positive occurrence of \( z \) or \( \neg z \), where \( z \in X \), by its truth value under \( \circ \). For example, if \( z^{\circ} = \bot \), replace \( \neg z \) by

---

\(^4\)It is possible that the third (resp. second) conjunct in formula 1 (resp. 2) is absent.
\(\top\) and \(z\) by \(\bot\). It should be easy to see that \(\Theta'\) is a tautology. For any position \(\psi_w\) that contains \(z\) (resp. \(\neg z\)) in \(\Theta\) and \(\top\) in \(\Theta'\), the position \(\Psi_w\) in \(\Sigma\) must contain a single literal \(u^\epsilon_i\) (resp. \(\neg v^\epsilon_i\)) such that \((u^\epsilon_i)^* = \top\) (resp. \((\neg v^\epsilon_i)^* = \top\)) if \(\Pi^* = \top\). This is because, by our construction, if \(z^0 = \top\) (resp. \((\neg z)^0 = \top\)), every \(u^\epsilon_i\) for \(1 \leq i \leq k^z\) (resp. \(\neg v^\epsilon_i\) for \(1 \leq i \leq t^z\)) must occur in the consequent of the implication in \(\Pi\) with non-isolated antecedent \(Z^z\). For reasons already discussed, such a literal must be true under any truth assignment \(\star\) where \(\Pi^* = \top\). Define \(\Sigma'\) as the formula such that, for each occurrence of \(\top\) or \(\bot\) in position \(\psi_w\) of \(\Theta'\), the literal in position \(\Psi_w\) of \(\Sigma\) is replaced by the same value (\(\top\) or \(\bot\)) as \(\psi_w\). Note that \(\Sigma'\) only substitutes the logical atom in position \(\Psi_w\) of \(\Sigma\) when \(\Psi_w\) contains \(z\). We define a truth assignment \(\sigma\) from \(\Phi\) to \(\Sigma'\) such that \(\sigma(\Phi) = f(\phi)\). Let \(\Phi = \Pi \rightarrow \Sigma\), where \(\Pi\) and \(\Sigma\) represent the antecedent and consequent of the outermost implication in \(\Phi\). We want to define a truth assignment \(\circ: X \rightarrow \{\top, \bot\}\) such that \(\Theta^*\) is true for any truth assignment \(\star\) that extends \(\circ\) to \(X \cup Y\). In what follows, we define such a partial truth assignment \(\circ\) for \(\Theta\) while concurrently defining a partial truth assignment \(\star\) for \(\Phi\).

**Procedure 1** - Consider a \(z \in X\) and let \(A\) be the atom of \(\Phi\) such that the first occurrence of \(Z^z\) in \(f(\phi)\) originates from \(A\) (i.e., \(A\) gets replaced by \(\sigma(A) = Z^z\)) when transitioning from \(\Phi\) to \(\sigma(\Phi) = f(\phi)\).

**Case 1:** The second and third occurrences of \(Z^z\) in \(f(\phi)\) originate from \(A\) and \(B\), respectively (for some \(B \neq A\) in \(\Phi\)). Define \(z^0 = \top\), \(A^* = \top\) and \(B^* = \bot\). The consequent \(\circ\) of the second occurrence of \(A\) in \(\Phi\) should take the form \(a_1 \land a_2 \land \ldots \land a_k\) for some positive literals \(a_1, a_2, \ldots, a_k\) in \(\Phi\) and the consequent of \(B\) should take the form \(\neg b_1 \land \neg b_2 \land \ldots \land \neg b_k\) for some negative literals \(\neg b_1, \neg b_2, \ldots, \neg b_k\). Let all of \(a_1, a_2, \ldots, a_k\) and \(b_1, b_2, \ldots, b_k\) be true under \(\star\).

**Case 2:** The second and third occurrences of \(Z^z\) in \(f(\phi)\) originate from \(B\) and \(A\), respectively (for some \(B \neq A\) in \(\Phi\)). Define \(z^0 = \bot\), \(A^* = \top\) and \(B^* = \bot\). The consequent \(\circ\) of the second occurrence of \(A\) in \(\Phi\) should take the form \(\neg b_1 \land \neg b_2 \land \ldots \land \neg b_k\) for some negative literals \(\neg b_1, \neg b_2, \ldots, \neg b_k\) and the consequent of \(B\) should take the form \(a_1 \land a_2 \land \ldots \land a_k\) for some positive literals \(a_1, a_2, \ldots, a_k\). Let all of \(a_1, a_2, \ldots, a_k\) and \(b_1, b_2, \ldots, b_k\) be true under \(\star\).

**Case 3:** There are only two occurrences of \(Z^z\) in \(f(\phi)\), both of which originate from \(A\). If the consequent of the second occurrence of \(A\) in \(\Phi\) takes the form \(a_1 \land a_2 \land \ldots \land a_k\) for some positive literals \(a_1, a_2, \ldots, a_k\) then define \(z^0 = \top\) and \(A^* = \top\). Further, let all of \(a_1, a_2, \ldots, a_k\) be true under \(\star\).

---

5Here and later in similar contexts, the “consequent of W” should be understood as the consequent of the implication whose antecedent is W. Similarly for “antecedent of W.”
a₁, a₂, ..., aᵢ be true under *). If the consequent of the second occurrence of A in Φ takes the form ¬b₁ ∧ ¬b₂ ∧ ... ∧ ¬bᵢ for some negative literals ¬b₁, ¬b₂, ..., ¬bᵢ then define z² = ⊥ and A* = ⊤. Further, let all of b₁, b₂, ..., bᵢ be false under *.

Case 4: If none of the cases 1 – 3 are satisfied, then the second and third occurrences of Z² in f(ϕ) must originate from B and C, respectively (where A ≠ B and A ≠ C). Define z² = ⊥, A* = ⊤ and B* = C* = ⊥. Further, let every atom in the consequent of B evaluate to ⊥ under * and every atom in the consequent of C evaluate to ⊤ under *.

As we remember, Θ in disjunctive normal form, taking the form

\((ψ₁ ∧ ψ₂ ∧ ... ∧ ψₙ) ∨ ... ∨ (ψₘ₊₁ ∧ ψₘ₊₂ ∧ ... ∧ ψₘ₊l)\)

where each ψₙ is a literal. It is also the case that Σ takes the form

\((Ψ₁ ∧ Ψ₂ ∧ ... ∧ Ψₙ) ∨ ... ∨ (Ψₘ₊₁ ∧ Ψₘ₊₂ ∧ ... ∧ Ψₘ₊l)\)

where each Ψₙ is a disjunction of literals (possibly with just a single “disjunct”). Thus, we will use our previous convention in which ψₙ represents a unique position in Θ and Ψₙ represents the corresponding position in Σ.

Our construction guarantees that for each position ψₙ in Θ containing some positive (resp. negative) literal z (resp. ¬z) such that z ∈ X, Ψₙ contains a positive (resp. negative) literal a (resp. ¬a). By procedure 1 we have z² = a*. As in the previous direction, let Θ' be the formula that results from replacing, in Θ, for every z ∈ X, all positive occurrences of the literals z and ¬z by their truth values under *°. Let Σ' be the formula such that, for each position ψₙ in Θ' containing a logical atom d ∈ {⊤, ⊥}, the literal in the corresponding position Ψₙ of Σ is replaced by d. The interpretation *° defined as part of procedure 1 is such that Π* = ⊤. Because Φ is a tautology, any extension of ° defined on all atoms of Σ must make Σ true. We also know that for each position Ψₙ in Σ' that contains a logical atom ⊤ (resp. ⊥), the literal in position Ψₙ of Σ evaluates to ⊤ (resp. ⊥) under *°. This means that Σ' is true regardless of how its non-logical atoms are interpreted and is a tautology. Our goal is to show that Θ' is a tautology as well.

Pick some arbitrary truth assignment *° for Θ'. We show (Θ')° = ⊤. For each position ψₙ in Θ' containing a positive literal y, the corresponding position Ψₙ in Σ' contains a disjunction of positive literals (qᵢ,y₁ ∨ qᵢ,y₂ ∨ ... ∨ qᵢ,yₘ) such that σ(qᵢ,y₁) = Pᵢ,y₁, σ(qᵢ,y₂) = Pᵢ,y₂, ..., σ(qᵢ,yₘ) = Pᵢ,yₘ, for some 1 ≤ i ≤ r_y. Similarly, for each position ψₙ in Θ' containing a negative literal ¬y, the corresponding position Ψₙ in Σ' contains a disjunction of negative literals (¬tᵢ,j ∨ ¬tᵢ,j ∨ ... ∨ ¬tᵢ,j) such that σ(tᵢ,j) = Pᵢ,j, σ(tᵢ,j) = Pᵢ,j, ..., σ(tᵢ,j) = Pᵢ,j, for some 1 ≤ j ≤ s_y. We now define a truth assignment † for Σ'. If y° = ⊤, let † be such that all of the corresponding literals ¬tᵢ,j, ¬tᵢ,j, ..., ¬tᵢ,j, for every 1 ≤ j ≤ s_y evaluate to false under †°. If y° = ⊥, let † be such that all corresponding literals qᵢ,j, qᵢ,j, ..., qᵢ,j, for every 1 ≤ i ≤ r_y evaluate to false under †°. With some thought, one can see that whenever Θ' has a false (under °) literal in a position ψₙ, Σ' has a false (under †°) disjunction of literals in the corresponding position Ψₙ. So, if (Θ')° = ⊥, then (Σ')° = ⊥. That is, (Σ')° = ⊤ (which is the case due to the tautology of Σ') implies (Θ°) = ⊤. □
References