Combining proof-search and counter-model construction for deciding Gödel-Dummett logic

Dominique Larchey-Wendling

LORIA – Université Henri Poincaré
Campus Scientifique, BP 239
Vandœuvre-lès-Nancy, France

Abstract. We present an algorithm for deciding Gödel-Dummett logic. The originality of this algorithm comes from the combination of proof-search in sequent calculus, which reduces a sequent to a set of pseudo-atomic sequents, and counter-model construction of such pseudo-atomic sequents by a fixpoint computation. From an analysis of this construction, we deduce a new logical rule $[\supset_N]$ which provides shorter proofs than the rule $[\supset_R]$ of G4-LC. We also present a linear implementation of the counter-model generation algorithm for pseudo-atomic sequents.

1 Introduction

In [9], Gödel introduced the logic G_ω which was later axiomatized by Dummett in [4] and is known since as Gödel-Dummett logic LC. It is viewed as one of the most important intermediate logics, between intuitionistic logic IL and classical logic CL, with connections with the provability logic of Heyting's Arithmetics [14] and more recently fuzzy logic [10]. Starting from proof-search in intuitionistic logic IL, the development of efficient proof-search procedures for intermediate logics like Gödel-Dummett logic has been the subject of recent studies [1, 6, 2].

The first formulation of a cut-free Gentzen-type system for LC [13] does not terminate because of the duplication of formulae. The work of Dyckhoff [5] and Hudelmair [11] solved the termination problem for IL with a duplication-free sequent calculus now called G4-IL. This system was further refined by the author [8, 12] in order to completely remove all the duplications, including those of sub-formulae. Dyckhoff [6] successfully applied the ideas of the duplication-free system G4-IL to the LC sequent calculus leading to a duplication-free sequent calculus called G4-LC. Moreover, he showed that there is a complete proof-search strategy which is deterministic, meaning that all the logical rules become invertible. In the same time, Avellone et al. [1] and Fiorino [7] investigated the ideas of the duplication-free system within the semantic tableaux approach and proposed corresponding tableaux calculi for various intermediate logics including LC. In [2], Avron claims that all these systems suffer from the serious drawback of using a rule, called $[\supset_R]$, with an arbitrary number of premises: this rule may introduce exponential blowup in the proof search process. Avron's solution to this problem is to use a hypersequent calculus for LC [2].

In this paper, we propose an original solution to the problem of rule $[\supset_R]$ which has an unbounded number of premises. It is based on the combination of a proof-search method in standard sequent calculus and a counter-model generation algorithm. We have a process in three steps: first the formula (resp. the sequent) to decide is converted into a *flat sequent*, the size of which is linearly bounded by the size of the initial problem. This step consists in an indexing of subformulae. Then, we apply a *proof-search process* to the flat sequent in which all the rules have one or two premises and are *strongly invertible*, i.e. they preserve counter-models top-down. It results in a set of *pseudo-atomic sequents* which is equivalent to the initial formula (resp. sequent). The last step consists of a *counter-model generation* algorithm to decide such pseudo-atomic sequents. The algorithm is based on a fixpoint computation, and either outputs a short proof or a (short) counter-model of the pseudo-atomic sequent. Then, from these steps, we have a new decision procedure for LC that leads to a solution of the problem of rule $[\supset_R]$. A surprising consequence of the fixpoint computation is the discovery of a *new logical rule* $[\supset_N]$ which efficiently replaces $[\supset_R]$. We briefly explain how this computation can be implemented in linear time.

Throughout this paper, we respect the following methodology: each time a transformation of a sequent $\mathcal{A}$ into a sequent $\mathcal{B}$ is given, we justify this transformation by giving the methods to convert a proof (resp. counter-model) of $\mathcal{B}$ into a proof (resp. counter-model) of $\mathcal{A}$. Thus, we fully describe a proof or counter-model generation algorithm.

2 Gödel-Dummett logic LC

In this section, we present the propositional Gödel-Dummett logic LC, its algebraic semantics, and some admissible sequent calculus rules, including the contraction-free system G4-LC.

2.1 Formulae, sequents and their algebraic semantic

The set of propositional *formulae*, denoted Form is defined inductively, starting from a set of propositional *variables* denoted by Var with an additional bottom constant $\bot$ denoting *absurdity* and using the connectives $\wedge$, $\vee$ and $\supset$. A *substitution* denoted by σ is any function that associates a formula to every propositional variable. We denote by A_σ the result of the application of σ to the variables in A. IL will denote the set of formulae that are provable in any intuitionistic propositional calculus (see [5]) and CL will denote the classically valid formulae. As usual an *intermediate propositional logic* [1] is a set of formulae $\mathcal{L}$ satisfying $\mathsf{IL} \subseteq \mathcal{L} \subseteq \mathsf{CL}$ and closed under the rule of modus ponens[1] and under arbitrary substitution.[2]

The Gödel-Dummett logic LC is an intermediate logic: in a Hilbert axiomatic system, it is the smallest intermediate logic satisfying the axiom formula

[1] If $A \in \mathcal{L}$ and $A \supset B \in \mathcal{L}$ then $B \in \mathcal{L}$.

[2] If $A \in \mathcal{L}$ and σ is any substitution then $A_\sigma \in \mathcal{L}$.

$$\frac{}{\Gamma, A \vdash A, \Delta}\,[\mathrm{Ax}] \qquad \frac{\Gamma, A, B \vdash \Delta}{\Gamma, A \land B \vdash \Delta}\,[\land_L] \qquad \frac{\Gamma \vdash A, B, \Delta}{\Gamma \vdash A \lor B, \Delta}\,[\lor_R]$$

$$\frac{\Gamma, A, B \vdash \Delta}{\Gamma, A, A \supset B \vdash \Delta}\,[\supset_L^1] \qquad \frac{\Gamma, A \supset C, B \supset C \vdash \Delta}{\Gamma, (A \lor B) \supset C \vdash \Delta}\,[\supset_L^3] \qquad \frac{\Gamma, A \supset (B \supset C) \vdash \Delta}{\Gamma, (A \land B) \supset C \vdash \Delta}\,[\supset_L^2]$$

$$\frac{\Gamma, A \vdash \Delta \qquad \Gamma, B \vdash G}{\Gamma, A \lor B \vdash \Delta}\,[\lor_L] \qquad \frac{\Gamma, B \supset C \vdash A \supset B, \Delta \qquad \Gamma, C \vdash \Delta}{\Gamma, (A \supset B) \supset C \vdash \Delta}\,[\supset_L^4]$$

$$\frac{\Gamma \vdash A, \Delta \qquad \Gamma \vdash B, \Delta}{\Gamma \vdash A \land B, \Delta}\,[\land_R] \qquad \frac{\ldots \quad \Gamma, A_i \vdash B_i, \Delta^i \quad \ldots}{\Gamma \vdash \Delta}\,[\supset_R]$$

Fig. 1. The cut-free terminating system G4-LC.

$(X \supset Y) \lor (Y \supset X)$. On the semantic side, intermediate logics are characterized by monotonic Kripke models and more particularly, LC is characterized by monotonic and *linear Kripke models* [4]. In this paper, we will rather use the algebraic semantic characterization of LC [2]. Let $\overline{\mathbb{N}} = \mathbb{N} \cup \{\infty\}$ be the set of natural numbers with its natural order $\leqslant$ augmented with a maximal element ∞. An interpretation $[\![\cdot]\!] : \mathsf{Var} \to \overline{\mathbb{N}}$ of propositional variables is inductively extended to formulae: $\bot$ interpreted by 0, the conjunction $\land$ is interpreted by the *minimum* function denoted $\land$, the disjunction $\lor$ by the *maximum* function $\lor$ and the implication $\supset$ by the operator $\to$ defined by $a \to b =$ if $a \leqslant b$ then ∞ else b. A formula is *valid* for the interpretation $[\![\cdot]\!]$ if the equality $[\![A]\!] = \infty$ holds and we write $\Vdash A$ when A is *universally valid*. This interpretation is complete for LC [9]. A *counter-model* of a formula A is an interpretation $[\![\cdot]\!]$ such that $[\![A]\!] < \infty$.

A *sequent* is a pair $\Gamma \vdash \Delta$ where Γ and Δ are multisets of formulae. Γ, Δ denotes the sum of the two multisets and if Γ is the empty multiset, we write $\vdash \Delta$. Substitutions may also be applied to multisets and sequents in the obvious way and we denote by $\Gamma_\sigma \vdash \Delta_\sigma$ the resulting sequent. Given a sequent $\Gamma \vdash \Delta$ and an interpretation $[\![\cdot]\!]$ of variables, we interpret $\Gamma \equiv A_1, \ldots, A_n$ by $\lfloor\!\lfloor \Gamma \rfloor\!\rfloor = [\![A_1]\!] \land \cdots \land [\![A_n]\!]$ and $\Delta \equiv B_1, \ldots, B_p$ by $\lceil\!\lceil \Delta \rceil\!\rceil = [\![B_1]\!] \lor \cdots \lor [\![B_p]\!]$. This sequent is *valid*, with respect to the interpretation $[\![\cdot]\!]$, if $\lfloor\!\lfloor \Gamma \rfloor\!\rfloor \leqslant \lceil\!\lceil \Delta \rceil\!\rceil$ and we write $\Gamma \Vdash \Delta$ when the sequent is universally valid. On the other hand, a *counter-model* to this sequent is an interpretation $[\![\cdot]\!]$ such that $\lceil\!\lceil \Delta \rceil\!\rceil < \lfloor\!\lfloor \Gamma \rfloor\!\rfloor$, i.e, for any pair (i, j), the inequality $[\![B_j]\!] < [\![A_i]\!]$ holds. We denote by $\Gamma \nVdash \Delta$ when such a counter-model exists.

2.2 Sequent calculi

In this section, we present sequent calculus rules to deal with proofs in LC. We only consider the $\bot$-free fragment of LC, i.e, atoms are propositional variables.[3] We present the terminating system G4-LC of Dyckhoff [6] in figure 1.[4] It is com-

[3] In section 6, we explain how to remove $\bot$ at the first step of the proof-search process.

[4] In G4-LC, the use of rule $[\supset_L^1]$ is restricted to the case A atomic, but this condition is not required for either soundness or completeness.

plete for LC and the structural rules of contraction [Contract], weakening [Weak], cut [Cut] and substitution [Subst$_\sigma$] are admissible.[5] All the rules of G4-LC are *strongly invertible*[6] [15] except rule [$\supset_R$]. Its restricted form called [$\supset'_R$] is invertible, making the system deterministic.

Let us analyze the use of the rule [$\supset_R$] and its restriction [$\supset'_R$] and its consequences in terms of complexity of proofs and proof-search. Δ is a multiset of formulae containing the sub-multiset $\Delta^\star$ of the implicational formulae $A_1 \supset B_1, \ldots, A_n \supset B_n$ of Δ. Δ may also contain some other kinds of formulae. The rule indicates that for each $i \in [1, n]$, there is premise $\Gamma, A_i \vdash B_i, \Delta^i$. Δ^i is the result of the removal of $A_i \supset B_i$ from $\Delta^\star$. So the rule instance has exactly n premises. The rule [$\supset'_R$] has the same form but its use is restricted to the case where no other rule of G4-LC is applicable.

$$\frac{\ldots \quad \Gamma, A_i \vdash B_i, \Delta^i \quad \ldots}{\Gamma \vdash \Delta}\,[\supset_R]$$

Let us explore the logical implications of the rule [$\supset_R$]. Each premise of this rule corresponds to a particular choice of an $A_i \supset B_i$ formula. If we apply the same rule to each premise, we have to choose between the remaining $n-1$ implications, thus to each premise of the root sequent corresponds $n-1$ premises, etc. We see that there is a proof-search branch for each particular choice sequence τ (i.e. permutation) of $[1, n]$. There are of course $n!$ such possible sequences. A proof search branch may stop (with an axiom for example) before all the sequence $\tau_1, \tau_2, \ldots$ has been explored but the proof size remains exponential: for example, consider the provable cycle sequent $\vdash X_1 \supset X_2, \ldots, X_n \supset X_1$. Within G4-LC, the proof of this sequent uses only the axiom rule [Ax] and the rule [$\supset_R$] and one can find at least $(n/2)!$ branches of length greater than $n/2$, so the size of this proof is bounded from below by an exponential.

3 Linear reduction of sequents into flat sequents

In this section, we describe how to convert a sequent into a *flat sequent* and in the next section, how to convert a flat sequent into a set of *pseudo-atomic sequents*. This first phase consists in indexing the initial sequent in order to have an equi-valid *flat sequent*. Propositions $\mathcal{P}$ and $\mathcal{Q}$ are *equi-valid* if they are both either valid or invalid. Propositions could be either formulae or sequents.

Definition 1 (Flat formula and sequent). *A* formula *is said to be* flat *if it is of one of the following forms: X or $X \supset Y$ or $Z \supset (X \otimes Y)$ or $(X \otimes Y) \supset Z$ where X, Y and Z are propositional variables and $\otimes \in \{\wedge, \vee, \supset\}$. A* sequent *$\Gamma \vdash \Delta$ is* flat *if all formulae of Γ are flat and Δ is only composed of formulae of the form X or $X \supset Y$ with X and Y variables.*

The process of flattening a formula D is quite standard, at least in classical logic. It consists in transforming D into an equi-valid flat sequent. The principle is to index the sub-formulae of D by new variables and to introduce the "axioms" that correspond to the subformula relation between those variables.

[5] [Subst$_\sigma$]: if σ is any substitution and $\Gamma \vdash \Delta$ is provable then $\Gamma_\sigma \vdash \Delta_\sigma$ is provable.

[6] A logical rule is invertible if the invalidity of any of its premise implies the invalidity of its conclusion and is strongly invertible if any counter-model of one of its premises is also a counter-model of the conclusion.

Let us fix a formula D for the rest of this section. We introduce a new variable X_C for every subformula C of D.[7] We do not distinguish between occurrences of subformulae. Moreover, if V is a variable occurring in D, we do not introduce a new variable X_V for it, i.e. we require the syntactic identity $X_V \equiv V$. We define two linear functions δ^+ and δ^- on the set of subformulae of D by the mutual induction with the following equations :

$$\delta^+(V) = \delta^-(V) = \emptyset \text{ when } V \text{ is a variable}$$

$$\begin{aligned}
\delta^+(A \otimes B) &= \delta^+(A), \delta^+(B), X_{A\otimes B} \supset (X_A \otimes X_B) \text{ when } \otimes \in \{\wedge, \vee\} \\
\delta^+(A \supset B) &= \delta^-(A), \delta^+(B), X_{A\supset B} \supset (X_A \supset X_B)
\end{aligned}$$

$$\begin{aligned}
\delta^-(A \otimes B) &= \delta^-(A), \delta^-(B), (X_A \otimes X_B) \supset X_{A\otimes B} \text{ when } \otimes \in \{\wedge, \vee\} \\
\delta^-(A \supset B) &= \delta^+(A), \delta^-(B), (X_A \supset X_B) \supset X_{A\supset B}
\end{aligned}$$

In this definition, $\delta^+(\cdot)$ and $\delta^-(\cdot)$ are multisets. The size of a formula is the number of occurrences of its subformulae, which is the number of nodes in its decomposition tree. Let C be a formula of size n. It is obvious to prove that the cardinals of $\delta^+(C)$ and $\delta^-(C)$ are smaller than n by mutual induction on C. Moreover, both of theses multisets are only composed of flat formulae, the size of which is 5, thus the size of either $\delta^+(C)$ or $\delta^-(C)$ is bounded by $5n$.

Proposition 1. *Any proof of the sequent $\delta^-(D) \vdash X_D$ can be transformed into a proof of the sequent $\vdash D$.*

Proof. Let σ be the substitution defined by $X_C \mapsto C$ for any subformula C of D. The result of applying the substitution σ to any formula of either $\delta^+(D)$ or $\delta^-(D)$ is a formula of the form $K \supset K$. Let us consider the following proof using one application of the rule [Subst$_\sigma$] and a repeated application of the cut rule [Cut]:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dots}{\delta^-(D) \vdash X_D}}{K_1 \supset K_1, \dots, K_p \supset K_p \vdash D}[\mathrm{Subst}_\sigma] \qquad \dfrac{\dfrac{}{K_1 \vdash K_1}[\mathrm{Ax}]}{\vdash K_1 \supset K_1}[\supset_R]}{\dots}[\mathrm{Cut}] \qquad \dfrac{\dfrac{}{K_p \vdash K_p}[\mathrm{Ax}]}{\vdash K_p \supset K_p}[\supset_R]}{\vdash D}[\mathrm{Cut}]$$

This last proof part describes the transformation of a proof of the flat sequent $\delta^-(D) \vdash X_D$ into a proof of the formula D. □

Now we prove the converse result: a counter-model to the sequent $\delta^-(D) \vdash X_D$ is also a counter-model to the formula D. This justifies the equi-validity of the flattening of the formula D. For that, we introduce some useful derived rules to prove semantic properties of δ^+ and δ^-: these derived rules express the variance of the logical operators with respect to the validity preorder $\Vdash$.

[7] As D has a finite number of subformulae and Form is infinite, this is always possible.

Proposition 2. *The following rules (with $\otimes$ is either $\vee$ or $\wedge$) are admissible in* LC*:*

$$\frac{\Gamma, A \vdash B \qquad \Delta, A' \vdash B'}{\Gamma, \Delta, A \otimes A' \vdash B \otimes B'}\,[\otimes_M] \qquad \frac{\Gamma, B \vdash A \qquad \Delta, A' \vdash B'}{\Gamma, \Delta, A \supset A' \vdash B \supset B'}\,[\supset_M]$$

We do not give the proof of this standard result. From these rules, we derive a relation between C and $\delta^+(C)$ (resp. $\delta^-(C)$):

Lemma 1. *The sequents $\delta^+(C), X_C \vdash C$ and $\delta^-(C), C \vdash X_C$ are valid for any subformula C of D,*

Proof. By mutual induction on C. We only present the case of $C \equiv A \supset B$. Let us prove $\delta^+(A \supset B), X_{A \supset B} \Vdash A \supset B$. By induction hypothesis, we know that $\delta^-(A), A \Vdash X_A$ and $\delta^+(B), X_B \Vdash B$. Then by the proof

$$\cfrac{\cfrac{\cfrac{\delta^-(A), A \vdash X_A \quad \delta^+(B), X_B \vdash B}{\delta^-(A), \delta^+(B), X_A \supset X_B \vdash A \supset B}\,[\supset_M]}{\delta^-(A), \delta^+(B), X_{A \supset B}, X_A \supset X_B \vdash A \supset B}\,[\text{Weak}]}{\delta^-(A), \delta^+(B), X_{A \supset B}, X_{A \supset B} \supset (X_A \supset X_B) \vdash A \supset B}\,[\supset_L^1]$$

and the soundness of the logical rules, we deduce the validity of the sequent $\delta^+(A \supset B), X_{A \supset B} \vdash A \supset B$. The other cases are similar. □

Proposition 3. *Let $[\![\cdot]\!]$ be a counter-model of the sequent $\delta^-(D) \vdash X_D$. Then it is also a counter-model of D, i.e. $[\![D]\!] < \infty$.*

Proof. As $[\![\cdot]\!]$ is a counter-model, the relation $[\![X_D]\!] < \llbracket \delta^-(D) \rrbracket$ holds. Moreover the relation $[\![D]\!] > [\![X_D]\!]$ would imply $[\![X_D]\!] < \llbracket \delta^-(D) \rrbracket \wedge [\![D]\!]$ and $[\![\cdot]\!]$ would be a counter-model of the sequent $\delta^-(D), D \vdash X_D$ which is impossible by lemma 1. As a consequence, we have $[\![D]\!] \leqslant [\![X_D]\!] < \infty$. □

Corollary 1. *Let D be any formula of size n, there exists a flat sequent which is equi-valid to D and of size smaller than $5n + 1$.*

Proof. We know by proposition 1 and 3 that D is equi-valid to $\delta^-(D) \vdash X_D$. This flat sequent is of size smaller than $5n + 1$. □

We point out the fact that it is also possible to transform the sequent $A_1, \ldots, A_n \vdash B_1, \ldots, B_p$ into the flat sequent

$$\delta^+(A_1), \ldots, \delta^+(A_n), X_{A_1}, \ldots, X_{A_n}, \delta^-(B_1), \ldots, \delta^-(B_p) \vdash X_{B_1}, \ldots, X_{B_p}$$

4 From flat to pseudo-atomic sequents

In this section, we describe the second stage of our decision algorithm. It is a proof-search process that converts a flat sequent into a set of pseudo-atomic sequents such that the flat sequent is valid if and only if all the pseudo-atomic sequents are valid. Moreover, any counter-model of any of the pseudo-atomic sequents is also a counter-model to the flat sequent.

We present six strongly invertible rules to reduce any formula of the form $Z \supset (X \otimes Y)$ or $(X \otimes Y) \supset Z$ on the left-hand side of the $\vdash$ sign into variables X and/or implicational formulae $X \supset Y$ (all the X, Y and Z represent variables). But before, we introduce some logical equivalences holding in LC:[8]

Proposition 4. *The following equivalences hold in* LC*:*

1) $(A \wedge B) \supset C \dashv\vdash (A \supset C) \vee (B \supset C)$ 1′) $A \supset (B \wedge C) \dashv\vdash (A \supset B) \wedge (A \supset C)$
2) $(A \vee B) \supset C \dashv\vdash (A \supset C) \wedge (B \supset C)$ 2′) $A \supset (B \vee C) \dashv\vdash (A \supset B) \vee (A \supset C)$
3) $A \supset (B \supset C) \dashv\vdash (A \supset C) \vee (B \supset C)$

The reader can find proofs of similar equivalences in [2]. Now we introduce six rules that can decompose any flat formula on the left-hand side of $\vdash$ into implicational formula $(X \supset Y)$ or variables (X):

Proposition 5. *The following rules are sound and strongly invertible for* LC*:*

$$\frac{\Gamma, A \supset C \vdash \Delta \qquad \Gamma, B \supset C \vdash \Delta}{\Gamma, (A \wedge B) \supset C \vdash \Delta}\,[\supset_2] \qquad \frac{\Gamma, A \supset B, A \supset C \vdash \Delta}{\Gamma, A \supset (B \wedge C) \vdash \Delta}\,[\supset_2']$$

$$\frac{\Gamma, A \supset C, B \supset C \vdash \Delta}{\Gamma, (A \vee B) \supset C \vdash \Delta}\,[\supset_3] \qquad \frac{\Gamma, A \supset B \vdash \Delta \qquad \Gamma, A \supset C \vdash \Delta}{\Gamma, A \supset (B \vee C) \vdash \Delta}\,[\supset_3']$$

$$\frac{\Gamma, B \supset C \vdash A \supset B, \Delta \qquad \Gamma, C \vdash \Delta}{\Gamma, (A \supset B) \supset C \vdash \Delta}\,[\supset_4] \qquad \frac{\Gamma, A \supset C \vdash \Delta \qquad \Gamma, B \supset C \vdash \Delta}{\Gamma, A \supset (B \supset C) \vdash \Delta}\,[\supset_4']$$

Proof. The rule $[\supset_3]$ (resp. $[\supset_4]$) is included in G4-LC under the name $[\supset_L^3]$ (resp. $[\supset_L^4]$) so they are sound. For the other rules, we use the preceding equivalences. We prove soundness of rule $[\supset_3']$, using the cut rule [Cut] in conjunction with proposition 4, part 2′):

$$\frac{\dfrac{\Gamma, A \supset B \vdash \Delta \quad \Gamma, A \supset C \vdash \Delta}{\Gamma, (A \supset B) \vee (A \supset C) \vdash \Delta}\,[\vee_L] \qquad \dfrac{\dots}{A \supset (B \vee C) \vdash (A \supset B) \vee (A \supset C)}}{\Gamma, A \supset (B \vee C) \vdash \Delta}\,[\text{Cut}]$$

Let us also prove the strong invertibility of rule $[\supset_2']$. Let $[\![\cdot]\!]$ be a counter-model of the premise, by proposition 4, part 1′), and soundness, we obtain the relation $[\![\Delta]\!] < [\![\Gamma]\!] \wedge [\![A \supset B]\!] \wedge [\![A \supset C]\!] = [\![\Gamma]\!] \wedge [\![(A \supset B) \wedge (A \supset C)]\!] \leqslant [\![\Gamma]\!] \wedge [\![A \supset (B \wedge C)]\!]$ and then, $[\![\cdot]\!]$ is a counter-model of the conclusion. □

[8] The notation $A \dashv\vdash B$ means that both sequents $A \vdash B$ and $B \vdash A$ are valid in LC.

With the six preceding rules, we are able to decompose any flat sequent until all the formulae of the form $Z \supset (X \otimes Y)$ or $(X \otimes Y) \supset Z$ have been replaced by variables or atomic implications. What we obtain is called a pseudo-atomic sequent:

Definition 2 (Pseudo-atomic and atomic sequents). *An* atomic context *denoted by Γ_a is a multiset of the form $A_1, \ldots, A_l, B_1 \supset C_1, \ldots, B_m \supset C_m$ where all the A_i, B_i, C_i are (propositional) variables. An* atomic sequent *is a sequent of the form $\Gamma_a \vdash X_1, \ldots, X_n$ where Γ_a is an atomic context and all the X_i are variables. A* pseudo-atomic sequent *is a sequent of the form $\Gamma_a \vdash X_1 \supset Y_1, \ldots, X_n \supset Y_n, Z_1, \ldots, Z_q$ where all the X_i, Y_i and Z_i are variables.*

Proposition 6. *The bottom-up application of the rules of proposition 5 preserves flat sequents. If a flat sequent is irreducible by those rules then it is pseudo-atomic.*

Proof. The result of the conversion of a formula $Z \supset (X \otimes Y)$ or $(X \otimes Y) \supset Z$ is one or two formulae of the form $X \supset Y$ on the left-hand side of the $\vdash$ sign for all the rules except rule $[\supset_4]$. In this last case, we add $X \supset Y$ on the right-hand side (left premise) and the introduction of a variable X on the left-hand side (right premise). Then flat sequents are preserved.

Then it is clear that flat sequents without formulae of the form $Z \supset (X \otimes Y)$ or $(X \otimes Y) \supset Z$ in the left-hand side are in fact pseudo-atomic sequents. □

5 Deciding pseudo-atomic sequents

In this section we develop the last step of our decision algorithm for LC. We present a counter-model generation algorithm to decide pseudo-atomic sequents. Pseudo-atomic sequents are sequents to which only the rules [Ax], $[\supset_L^1]$ or $[\supset_R]$ of the G4-LC calculus may be applied bottom-up. But as explained in section 2.2, the use of rule $[\supset_R]$ is not efficient in a decision algorithm. We propose a computationally efficient procedure which is based on counter-model generation.

Proposition 7. *The validity of the atomic sequent $\Gamma_a \vdash X_1, \ldots, X_n$ can be decided in linear time and is equivalent to the validity of one of the $\Gamma_a \vdash X_i$.*

Proof. We apply the rule $[\supset_L^1]$ in any order until this rule is no more applicable. As this rule is strongly invertible, the validity is preserved by this process. Each $B_i \supset C_i$ occurring in Γ_a may be reduced at most once and this algorithm is linear. If the obtained sequent is not an axiom, then it is necessarily of the form $A_1, \ldots, A_l, B_1 \supset C_1, \ldots, B_m \supset C_m \vdash X_1, \ldots, X_n$ where $\{A_1, \ldots, A_l\} \cap \{X_1, \ldots, X_n, B_1, \ldots, B_m\} = \emptyset$ and such a sequent has a classical counter-model: $[\![A_i]\!] = 1$ and $[\![X_i]\!] = [\![B_i]\!] = 0$ for any i. This interpretation is also a counter-model for all the $\Gamma_a \vdash X_i$ sequents. □

The reader may have noticed that on atomic sequents, all intermediate logics collapse to classical logic and its boolean semantic. Of course, this is not the case for pseudo-atomic sequents.

5.1 Decision as a fixpoint computation

We present the general method to decide a fixed pseudo-atomic sequent with no variables on the right-hand side of the $\vdash$ sign, i.e. of the form

$$\Gamma_a \vdash X_1 \supset Y_1, \ldots, X_n \supset Y_n \qquad (n > 0)$$

Let $I \subseteq [1,n]$ be a subset of $[1,n]$. If I is the subset $\{i_1, \ldots, i_k\}$ then we denote by $\mathcal{X}_I$ the multiset of variables $\{X_{i_1}, \ldots, X_{i_k}\}$. We also denote by $\overline{I} = [1,n] - I$ the complement of I and by $\mathcal{S}_n$ the symmetric group i.e. the set of permutations of $[1,n]$. We define an increasing function φ on the complete (and finite) lattice of subsets of $[1,n]$, by:

$$\varphi \begin{cases} 2^{[1,n]} \longrightarrow 2^{[1,n]} \\ I \longmapsto \{i \mid \Gamma_a, \mathcal{X}_{\overline{I}} \nvdash Y_i\} \end{cases}$$

We recall that the sequent $\Gamma_a, \mathcal{X}_{\overline{I}} \vdash Y_i$ is atomic and then $\varphi(I)$ can be computed in linear time using the method of proposition 7. Because of the two negations ($\overline{I}$ and $\nvdash$), the function φ is monotonic. Then we can compute the least fixpoint[9] μ_φ of φ:

$$I_0 = \emptyset \subsetneq I_1 = \varphi(\emptyset) \subsetneq \cdots \subsetneq I_p = \varphi^p(\emptyset) = \mu_\varphi$$

This process takes a finite number of steps p which is less than the size of $[1,n]$: $0 \leqslant p \leqslant n$. The following theorem shows that the cardinal of the fixpoint μ_φ characterizes the validity of the pseudo-atomic sequent.

Theorem 1. *The three following propositions are equivalent:*

1. *The sequent* $\Gamma_a \vdash X_1 \supset Y_1, \ldots, X_n \supset Y_n$ *has a counter-model*
2. $\exists \tau \in \mathcal{S}_n,\ \forall k \in [1,n] \quad \Gamma_a, X_{\tau_1}, \ldots, X_{\tau_k} \nvdash Y_{\tau_k}$
3. $\mu_\varphi = [1,n]$

In the following three subsections, we prove $1 \Rightarrow 2$, $2 \Rightarrow 3$ and finally $3 \Rightarrow 1$.

A necessary condition of invalidity

Proposition 8 ($1 \Rightarrow 2$). *Let the interpretation* $[\![\cdot]\!]$ *be a counter-model of the pseudo-atomic sequent* $\Gamma_a \vdash X_1 \supset Y_1, \ldots, X_n \supset Y_n$*. Then there exists a permutation* $\tau \in \mathcal{S}_n$ *such that for any* $k \in [1,n]$*,* $[\![\cdot]\!]$ *is also a counter-model of* $\Gamma_a, X_{\tau_1}, \ldots, X_{\tau_k} \vdash Y_{\tau_k}$*.*

Proof. Let τ be any permutation such that $[\![X_{\tau_n}]\!] \leqslant \cdots \leqslant [\![X_{\tau_1}]\!]$, obtained by sorting all these values. As $[\![\cdot]\!]$ is a counter-model of $\Gamma_a \vdash X_1 \supset Y_1, \ldots, X_n \supset Y_n$, we obtain $[\![X_k \supset Y_k]\!] < \llbracket \Gamma_a \rrbracket$ for any $k \in [1,n]$. We fix a particular k and consider $\tau_k \in [1,n]$. We can then derive $[\![X_{\tau_k} \supset Y_{\tau_k}]\!] < \infty$ and thus $[\![X_{\tau_k}]\!] \to [\![Y_{\tau_k}]\!] < \infty$ holds. Then it is necessary that $[\![Y_{\tau_k}]\!] < [\![X_{\tau_k}]\!] = [\![X_{\tau_1}]\!] \wedge \cdots \wedge [\![X_{\tau_k}]\!]$ and thus $[\![Y_{\tau_k}]\!] = [\![X_{\tau_k} \supset Y_{\tau_k}]\!] < \llbracket \Gamma_a \rrbracket$. As a conclusion, $[\![Y_{\tau_k}]\!] < \llbracket \Gamma_a, X_{\tau_1}, \ldots, X_{\tau_k} \rrbracket$. We deduce that $[\![\cdot]\!]$ is a counter-model of $\Gamma_a, X_{\tau_1}, \ldots, X_{\tau_k} \vdash Y_{\tau_k}$. □

[9] Or equivalently, this is the greatest fixpoint of $I \mapsto \{i \mid \Gamma_a, \mathcal{X}_I \Vdash Y_i\}$.

Computing the fixpoint

Proposition 9 (2 ⇒ 3). *If there exists a permutation* $\tau \in \mathcal{S}_n$ *satisfying the condition* $\forall k \in [1,n]\ \Gamma_a, X_{\tau_1}, \ldots, X_{\tau_k} \not\Vdash Y_{\tau_k}$ *then* $\mu_\varphi = [1,n]$.

Proof. We write μ for μ_φ. Let $k \in [1,n]$. We proceed by descending induction on $k \geqslant 1$. We prove the induction step:

$$\{\tau_{k+1}, \ldots, \tau_n\} \subseteq \mu \Rightarrow \tau_k \in \mu$$

The identity $\mathcal{X}_{\overline{\{\tau_{k+1},\ldots,\tau_n\}}} = \{X_{\tau_1}, \ldots, X_{\tau_k}\}$ holds and $\Gamma_a, X_{\tau_1}, \ldots, X_{\tau_k} \not\Vdash Y_{\tau_k}$ also holds so $\tau_k \in \varphi(\{\tau_{k+1}, \ldots, \tau_n\})$ holds. With the induction hypothesis and the monotonicity of φ, we obtain $\tau_k \in \varphi(\{\tau_{k+1}, \ldots, \tau_n\}) \subseteq \varphi(\mu) = \mu$ which proves the induction step. Then it is trivial to prove $\tau_k \in \mu$ for all k: $\tau_n \in \mu$, then $\tau_{n-1} \in \mu$, ... and finally $\tau_1 \in \mu$. Thus we obtain $\mu = [1,n]$ □

From the fixpoint to the counter-model

We now suppose that we have computed the fixpoint μ_φ and that it equals $[1,n]$. How to build a counter-model from this information? Let us consider the strictly increasing sequence $I_0 = \emptyset \subsetneq I_1 = \varphi(\emptyset) \subsetneq \cdots \subsetneq I_p = \varphi^p(\emptyset) = \mu_\varphi$. As μ_φ is not empty,[10] the inequation $p > 0$ holds. We show how to build a counter-model out of this strictly increasing sequence. We define a decreasing sequence $\mathcal{M}_0 \supseteq \mathcal{M}_1 \supseteq \cdots \supseteq \mathcal{M}_{p+1}$ of subsets of Var by

$$\mathcal{M}_0 = \mathsf{Var} \quad \text{and} \quad \mathcal{M}_{k+1} = \{Z \in \mathsf{Var} \mid \Gamma_a, \mathcal{X}_{\overline{I_k}} \Vdash Z\} \text{ for } k \in [0,p]$$

Then we define the following interpretation for any variable Z:

$$[\![Z]\!] = \max\{k \in [0, p+1] \mid Z \in \mathcal{M}_k\} \qquad (1)$$

The next two propositions establish that $[\![\cdot]\!]$ is a counter-model of the sequent $\Gamma_a \vdash X_1 \supset Y_1, \ldots, X_n \supset Y_n$.

Proposition 10. *If the formula* A *is in* Γ_a *then* $[\![A]\!] \geqslant p+1$.

Proof. Let A be an element of Γ_a, if A is a variable then $[\![A]\!]$ is given by equation (1). Since $A \in \Gamma_a$ holds, we deduce $\Gamma_a, \mathcal{X}_{\overline{I_p}} \Vdash A$ by the axiom rule [Ax], then $A \in \mathcal{M}_{p+1}$ and $[\![A]\!] = p+1$.

Otherwise, A is of the form $P \supset Q$ where P and Q are variables. If $[\![P]\!] = 0$ then $[\![P \supset Q]\!] = \infty \geqslant p+1$. Otherwise let $[\![P]\!] = k+1$ with $k \in [0,p]$. Since P is a variable we obtain $P \in \mathcal{M}_{k+1}$, thus $\Gamma_a, \mathcal{X}_{\overline{I_k}} \Vdash P$ holds. Since $P \supset Q \in \Gamma_a$, $\Gamma_a, \mathcal{X}_{\overline{I_k}} \Vdash P \supset Q$ also holds. So, by application of the rule of modus ponens (which is admissible[11]) the validity of $\Gamma_a, \mathcal{X}_{\overline{I_k}} \Vdash Q$ holds. As Q is a variable, we deduce $Q \in \mathcal{M}_{k+1}$. $[\![Q]\!]$ is given by the equation (1) and we obtain $[\![Q]\!] \geqslant k+1 = [\![P]\!]$. Finally $[\![P \supset Q]\!] = \infty$. □

---

[10] We have supposed $n > 0$. The case $n = 0$ is treated separately in the proof of corollary 3, section 5.2.

[11] The modus ponens rule can be viewed as a combination of the cut rule [Cut] and the contraction rule [Contract] in $\mathsf{G4\text{-}LC}$.

Proposition 11. *For any $i \in [1,n]$, the relation $[\![X_i \supset Y_i]\!] < p$ holds.*

Proof. Let us fix a particular $i \in [1,n]$. By the definition of the sequence $\emptyset = I_0 \subsetneq I_1 \subsetneq \cdots \subsetneq I_p = [1,n]$, there exists a unique $k \in [0, p-1]$ such that $i \in I_{k+1}$ and $i \notin I_k$. From $i \notin I_k$, we derive $i \in \overline{I_k}$, and then $\Gamma_a, \mathcal{X}_{\overline{I_k}} \Vdash X_i$. As X_i is a variable, $X_i \in \mathcal{M}_{k+1}$ holds thus $[\![X_i]\!] \geqslant k+1$ holds by equation (1).

From $i \in I_{k+1} = \varphi(I_k)$, we deduce by definition of φ that $\Gamma_a, \mathcal{X}_{\overline{I_k}} \nVdash Y_i$ and $Y_i \notin \mathcal{M}_{k+1}$. Then, we have $[\![Y_i]\!] \leqslant k < [\![X_i]\!]$ and $[\![X_i \supset Y_i]\!] = [\![Y_i]\!] \leqslant k < p$ holds. □

Corollary 2 (3 ⇒ 1). *The semantic $[\![\cdot]\!]$ defined by equation (1) is a counter-model of the sequent $\Gamma_a \vdash X_1 \supset Y_1, \ldots, X_n \supset Y_n$.*

Proposition 12. *If Z is a variable such that $\Gamma_a \nVdash Z$ holds then $[\![Z]\!] \leqslant p$ holds.*

Proof. $I_p = [1,n]$, so $\overline{I_p} = \emptyset$ and finally $Z \notin \mathcal{M}_{p+1} = \{Z \mid \Gamma_a \Vdash Z\}$. □

5.2 Deciding all pseudo-atomic sequents

We have an algorithm to decide pseudo-atomic sequents with no variables on the right-hand side of the $\vdash$ sign. But it is straightforward to generalize it to any pseudo-atomic sequent.

Corollary 3. *Let $\Gamma_a \vdash X_1 \supset Y_1, \ldots, X_n \supset Y_n, Z_1, \ldots, Z_q$ be a pseudo-atomic sequent. It is provable in* LC *iff one of the sequents $\Gamma_a \vdash Z_i$ or the sequent $\Gamma_a \vdash X_1 \supset Y_1, \ldots, X_n \supset Y_n$ is provable.*

Proof. The (if) part is a simple application of a weakening rule on the right of the $\vdash$ sign of sequents. For the (only if) part, we distinguish between $n = 0$ and $n > 0$. In the former case, we use proposition 7. In the later case, suppose that neither the sequents $\Gamma_a \vdash Z_i$ nor the sequent $\Gamma_a \vdash X_1 \supset Y_1, \ldots, X_n \supset Y_n$ are provable (i.e. valid). We compute the fixpoint for this last sequent. Then by theorem 1, the fixpoint is $[1,n]$ and by proposition 12 and corollary 2, the semantics defined by equation (1) is also a counter-model of the sequent $\Gamma_a \vdash X_1 \supset Y_1, \ldots, X_n \supset Y_n, Z_1, \ldots, Z_q$. □

5.3 A new logical rule inspired by the fixpoint computation

From theorem 1, we know that $\mu_\varphi = [1,n]$ holds when the pseudo-atomic sequent $\Gamma_a \vdash X_1 \supset Y_1, \ldots, X_n \supset Y_n$ is not valid. When $\mu_\varphi \subsetneq [1,n]$, the sequent is provable and we aim to provide a proof of it. Unfortunately, with the rule $[\supset_R]$, we would not be able to provide a proof of reasonable size, as explained in section 2.2. Now, we propose a new rule in order to replace $[\supset_R]$. We show that the condition $\mu_\varphi \subsetneq [1,n]$ is the expression of a very natural logical rule.

Proposition 13. *If $\mu_\varphi \subsetneq [1,n]$ then there exists a non empty subset I of $[1,n]$ such that for any $i \in I$, the sequent $\Gamma_a, \mathcal{X}_I \vdash Y_i$ is valid.*

Proof. Let I be the complementary subset of μ_φ so I is not empty and $\overline{I} = \mu_\varphi$. Let $i \in I$ then $i \notin \overline{I} = \varphi(\overline{I})$ and thus $\Gamma_a, \mathcal{X}_I \Vdash Y_i$. □

Then, with all the sequents $\Gamma_a, \mathcal{X}_I \vdash Y_i$ being valid, it would be nice to have a sound logical rule from which we could derive in only one step the conclusion $\Gamma_a \vdash X_1 \supset Y_1, \ldots, X_n \supset Y_n$. Now, we present a rule for decomposing implicational formulae on the right-hand side but, as opposed to the rule $[\supset_R]$, all the implications can be decomposed in only one step and for which there are no side conditions:[12]

Proposition 14. *Let $I = \{i_1, \ldots, i_k\}$ by a non empty subset of $[1, n]$, the following rule $[\supset_N]$ is sound for* LC*:*

$$\frac{\Gamma, A_{i_1}, \ldots, A_{i_k} \vdash B_{i_1} \quad \ldots \quad \Gamma, A_{i_1}, \ldots, A_{i_k} \vdash B_{i_k}}{\Gamma \vdash A_1 \supset B_1, \ldots, A_n \supset B_n, \Delta}\ [\supset_N]$$

Proof. We prove soundness by showing that any model $[\![\cdot]\!]$ of the premises is also a model of the conclusion. Let $[\![\cdot]\!]$ be a model of the premises. Then, for any $j \in [1, k]$, the inequality $\lfloor\!\lfloor \Gamma \rfloor\!\rfloor \wedge [\![A_{i_1}]\!] \wedge \cdots \wedge [\![A_{i_k}]\!] \leqslant [\![B_{i_j}]\!]$ holds. Let δ be the index such that $[\![A_{i_\delta}]\!]$ is minimal among the values $[\![A_{i_j}]\!]$. The property $[\![A_{i_\delta}]\!] = [\![A_{i_1}]\!] \wedge \cdots \wedge [\![A_{i_k}]\!]$ holds and also $\lfloor\!\lfloor \Gamma \rfloor\!\rfloor \wedge [\![A_{i_\delta}]\!] \leqslant [\![B_{i_\delta}]\!]$.

Now, we prove that we have $\lfloor\!\lfloor \Gamma \rfloor\!\rfloor \leqslant [\![A_{i_\delta} \supset B_{i_\delta}]\!]$. If $[\![A_{i_\delta}]\!] \leqslant [\![B_{i_\delta}]\!]$ then $[\![A_{i_\delta} \supset B_{i_\delta}]\!] = \infty$ and the property is trivially verified. On the other hand, suppose that $[\![A_{i_\delta}]\!] > [\![B_{i_\delta}]\!]$ holds. Then $[\![A_{i_\delta} \supset B_{i_\delta}]\!] = [\![B_{i_\delta}]\!]$ holds. The relation $\lfloor\!\lfloor \Gamma \rfloor\!\rfloor > [\![B_{i_\delta}]\!]$ is false because otherwise the relation $\lfloor\!\lfloor \Gamma \rfloor\!\rfloor \wedge [\![A_{i_\delta}]\!] > [\![B_{i_\delta}]\!]$ would hold. Therefore we obtain $\lfloor\!\lfloor \Gamma \rfloor\!\rfloor \leqslant [\![B_{i_\delta}]\!] = [\![A_{i_\delta} \supset B_{i_\delta}]\!]$.

The property $\lfloor\!\lfloor \Gamma \rfloor\!\rfloor \leqslant [\![A_1 \supset B_1]\!] \vee \cdots \vee [\![A_n \supset B_n]\!] \vee \lceil\!\lceil \Delta \rceil\!\rceil$ holds because $A_{i_\delta} \supset B_{i_\delta}$ is one of the $A_j \supset B_j$. □

5.4 Remarks on complexity

From the complexity point of view, this new rule $[\supset_N]$ has major advantages over the rule $[\supset_R]$: it allows to prove the sequent $\Gamma_a \vdash X_1 \supset Y_1, \ldots, X_n \supset Y_n$ in only one step using proposition 13:

$$\frac{\Gamma_a, \mathcal{X}_I \vdash Y_{i_1} \quad \ldots \quad \Gamma_a, \mathcal{X}_I \vdash Y_{i_k}}{\Gamma_a \vdash X_1 \supset Y_1, \ldots, X_n \supset Y_n}\ [\supset_N]$$

Compared to the $[\supset_R]$ rule, this $[\supset_N]$ rule avoids the exponential blowup which occurs because a proof-search algorithm based on $[\supset_R]$ needs to explore branches corresponding to all possible permutations of $[1, n]$ (see section 2.2). The case of pseudo-atomic sequents is a worst case example for the application of rule $[\supset_R]$. On the contrary, applicability of the $[\supset_N]$ rule can be decided using a fixpoint

[12] In rule $[\supset_N]$, Δ can be any multiset of formulae, i.e. it is not necessary that the $A_i \supset B_i$ enumerate all the implicational formulae on the right-hand side of $\vdash$.

computation and the fixpoint contains an instance of rule $[\supset_N]$. So in the case of pseudo-atomic sequent, the new rule $[\supset_N]$ is clearly much more efficient than $[\supset_R]$. Now what about replacing $[\supset_R]$ by $[\supset_N]$ in G4-LC ? This direct replacement does not lead to a complete cut-free calculus for LC. Indeed, the valid sequent $A \supset (B \vee C) \vdash (A \supset B) \vee (A \supset C)$ has no proof in such a system. So care has to be taken when designing a proof-search calculus based on $[\supset_N]$. We will investigate these logical properties in some future work. We have proposed a particular transformation of sequents into pseudo-atomic sequents. Other possible transformations will also be studied from a complexity point of view.

6 Removing the constant $\perp$ from formulae

In this section, we present a linear transformation of a formula into an equi-valid sequent that does not contain $\perp$ as a subformula.[13] The idea is to replace $\perp$ by new variable α and to introduce hypothesis sufficient enough to be able to deduce "anything" from α. We denote by A_α the formula A where $\perp$ has been substituted by α, i.e. $A_\alpha = A_{\{\perp \mapsto \alpha\}}$. If $X_1, \ldots, X_n$ are the variables occurring in A, this idea is well described by the following rule

$$\frac{\vdash A}{\alpha \supset X_1, \ldots, \alpha \supset X_n \vdash A_\alpha} \ [\alpha \text{ new variable}]$$

and we prove that it is sound and invertible in appendix A.

Theorem 2. *Let A be a formula, $\{X_1, \ldots, X_n\}$ its variables and α be another variable which is not one of the X_i's. Any proof (resp. counter-model) of the sequent $\alpha \supset X_1, \ldots, \alpha \supset X_n \vdash A_\alpha$ can be transformed into a proof (resp. counter-model) of $\vdash A$. The size of the former sequent is linear in the size of A.*

7 Computation of μ_φ

In this section, we describe an algorithm to compute the iterated sequence $I_0 = \emptyset \subsetneq I_1 = \varphi(\emptyset) \subsetneq \cdots \subsetneq I_p = \varphi^p(\emptyset) = \mu_\varphi$ in time linear to the size of the pseudo-atomic sequent. We do not give a full proof of the algorithm but rather explain the basic ideas. Suppose we want to compute the fixpoint for the sequent

$$A_1, \ldots, A_l, B_1 \supset C_1, \ldots, B_m \supset C_m \vdash X_1 \supset Y_1, \ldots, X_n \supset Y_n$$

We describe an algorithm that computes the fixpoint for this sequent. It can be seen as a *reference counting algorithm* [3]. In this scheme, an occurrence of an implication $B_i \supset C_i$ in the context represents a relative reference of the variable

[13] The proof search method we have described in the preceding sections can be easily extended to the $\perp$-case. But as it lengthens all the proofs, we have chosen to present a $\perp$-free decision procedure together with the removal of $\perp$ at the beginning of the process.

B_i to the variable C_i. An occurrence variable A_i or X_i in the context represents an absolute reference. For any variable X, the reference count of X equals the number of absolute references to X plus the number of relative references to X from any K which has a strictly positive reference count. The main point is that a variable is deducible from the context if and if only its reference count is strictly positive.

First, we represent this pseudo-atomic sequent by a graph $\mathcal{G}$: the *vertexes* are the variables occurring in the sequent and the *arrows* are $B_i \to C_i$ for all the implications $B_i \supset C_i$ on the left-hand side of the $\vdash$ sign. Let $\mathcal{S}$ be a multiset of vertexes (thus variables) and X a vertex. We represent the validity of the sequent $\mathcal{S}, B_1 \supset C_1, \ldots, B_m \supset C_m \vdash X$ by *accessibility* from $\mathcal{S}$ in the graph $\mathcal{G}$:

$$\mathcal{S}, B_1 \supset C_1, \ldots, B_m \supset C_m \Vdash X \quad \text{iff} \quad \exists Z \in \mathcal{S}, Z \to^\star X \text{ in } \mathcal{G}$$

Thus, the computation of the fixpoint can be done on the contraction of the graph $\mathcal{G}$ where directed connected components are collapsed.[14] Then we suppose that the graph $\mathcal{G}$ is acyclic, i.e. there are no loops inside this graph.

We compute accessibility from $\mathcal{S}$ in $\mathcal{G}$ by a *reference counting function* $\mathcal{S}_Z$ defined inductively on the vertex Z:[15] this weight function counts the number of occurrences of the vertex Z in $\mathcal{S}$ plus the number of vertexes K below Z ($K \to Z \in \mathcal{G}$) such that $\mathcal{S}_K > 0$. There are three important facts: $\mathcal{S}_Z > 0$ holds iff Z is accessible from $\mathcal{S}$; the sum of all the weights $\sum_Z \mathcal{S}_Z$ is smaller than the number of arrows in $\mathcal{G}$ plus the cardinal of $\mathcal{S}$; $(\mathcal{S} \cup \{X\})_Z$ (resp. $(\mathcal{S} - \{X\})_Z$) can be computed incrementally from $\mathcal{S}_Z$ using a depth-first search algorithm and the total time to recompute $(\mathcal{S} \cup \{X\})_Z$ (resp. $(\mathcal{S} - \{X\})_Z$) is linearly bounded by the increase (resp. decrease) of the value $\sum_Z \mathcal{S}_Z$.

Let $\mathcal{A}$ be the multiset vertexes $\{A_1, \ldots, A_l\}$. For the computation of the fixpoint sequence, we first compute $(\mathcal{A}, \mathcal{X}_{\overline{I_0}})_Z = (\mathcal{A}, X_1, \ldots, X_n)_Z$ which takes a time linear in the size of $\mathcal{G}$ plus $l + n$, i.e. is linearly bounded by the size of the initial sequent. Then, I_1 is the set of indexes i such that $(\mathcal{A}, \mathcal{X}_{\overline{I_0}})_{Y_i} = 0$ holds. We remove those indexes from $\overline{I_0}$ obtaining $\overline{I_1}$ and recompute the corresponding weight function $(\mathcal{A}, \mathcal{X}_{\overline{I_1}})_Z$. Thus we can compute $\overline{I_2}$, etc. The total time for this computation is also linearly bounded by the size of the initial sequent because of the incremental computation of the sequence $(\mathcal{A}, \mathcal{X}_{\overline{I_0}})_Z, \ldots, (\mathcal{A}, \mathcal{X}_{\overline{I_p}})_Z$ of weight functions. In appendix B, we develop a complete execution of this algorithm.

What about the complexity of the three steps algorithm we have described ? Without entering the full details, it should appear that the final goal is to obtain an implementation with a complexity equivalent to that of a connection method for classical propositional logic. In this setting, atomic paths correspond to our pseudo-atomic sequents. To fulfill this design goal, we have to be able to compute the fixpoint on-the-fly, i.e. using a incremental reference count (garbage collection) algorithm so as to be able to decide pseudo-atomic sequent in constant time when we obtain an atomic path. For the moment, this step takes a linear

[14] Computing the connected components of a graph is a linear time process.

[15] That is why we need $\mathcal{G}$ acyclic.

time. But existing results in cyclic and incremental garbage collection techniques suggest the feasibility of such a design.

8 Conclusion

In this paper, we have proposed an algorithm, in three steps, that is able to compute either a proof or a counter-model of any formula of LC. The main contributions are: a counter-model generation algorithm for pseudo-atomic sequents than can be implemented in linear time and a new proof system where a new logical rule $[\supset_N]$ efficiently replaces $[\supset_R]$. The main perspectives of this work are the resource-conscious implementation of this algorithm and the study of the logical properties of the new rule. We would also like to investigate the extension of our methodology to some other intermediate logics.

References

1. Alessandro Avellone, Mauro Ferrari, and Pierangelo Miglioli. Duplication-Free Tableau Calculi and Related Cut-Free Sequent Calculi for the Interpolable Propositional Intermediate Logics. *Logic Journal of the IGPL*, 7(4):447–480, 1999.
2. Arnon Avron. A Tableau System for Gödel-Dummett Logic Based on a Hypersequent Calculus. In Roy Dyckhoff, editor, *Automated Reasoning with Analytic Tableaux and Related Methods*, volume 1847 of *Lecture Notes in Artificial Intelligence*, pages 98–111, St Andrews, Scotland, July 2000.
3. L. Peter Deutsch and Daniel G. Bobrow. A Efficient Incremental Automatic Garbage Collector. *Communications of the ACM*, 19(9):522–526, September 1976.
4. Michael Dummett. A Propositional Calculus with a Denumerable matrix. *Journal of Symbolic Logic*, 24:96–107, 1959.
5. Roy Dyckhoff. Contraction-free Sequent Calculi for Intuitionistic Logic. *Journal of Symbolic Logic*, 57(3):795–807, 1992.
6. Roy Dyckhoff. A Deterministic Terminating Sequent Calculus for Gödel-Dummett logic. *Logical Journal of the IGPL*, 7:319–326, 1999.
7. Fiorino. An $\mathcal{O}(n \log n)$-SPACE decision procedure for the propositional Dummett Logic. to appear in Journal of Automated Reasoning.
8. Didier Galmiche and Dominique Larchey-Wendling. Structural Sharing and Efficient Proof-Search in Propositional Intuitionistic Logic. In *Asian Computing Science Conference, ASIAN'99*, volume 1742 of *Lecture Notes in Computer Science*, pages 101–102, Phuket, Thaïland, December 1999.
9. Kurt Gödel. Zum intuitionistischen Aussagenkalkül. *Ergeb. Math. Koll*, 4:40, 1933.
10. P. Hajek. *Metamathematics of Fuzzy Logic*. Kluwer Academic Publishers, 1998.
11. Jörg Hudelmaier. An $\mathcal{O}(n \log n)$-space decision procedure for Intuitionistic Propositional Logic. *Journal of Logic and Computation*, 3(1):63–75, 1993.
12. Dominique Larchey, Daniel Méry, and Didier Galmiche. STRIP: Structural Sharing for efficient Proof-Search. In *International Joint Conference on Automated Reasoning, IJCAR 2001*, volume 2083 of *Lecture Notes in Artificial Intelligence*, pages 696–700, Siena, Italy, January 2001.
13. O. Sonobe. A Gentzen-type Formulation of Some Intermediate Propositional Logics. *Journal of Tsuda College*, 7:7–14, 1975.

14. A. Visser. On the Completeness Principle: A study of provability in Heyting's arithmetic. *Annals of Mathematical Logic*, 22:263–295, 1982.
15. Klaus Weich. Decisions Procedures for Intuitionistic Logic by Program Extraction. In *International Conference TABLEAUX'98*, volume 1397 of *Lecture Notes in Artificial Intelligence*, pages 292–306, Oisterwijk, The Netherlands, May 1998.

A Proof of theorem 2

Theorem 2. *Let A be a formula, $\{X_1, \ldots, X_n\}$ its variables and α be another variable which is not one of the X_i's. Any proof (resp. counter-model) of the sequent $\alpha \supset X_1, \ldots, \alpha \supset X_n \vdash A_\alpha$ can be transformed into a proof (resp. counter-model) of $\vdash A$. The size of the former sequent is linear in the size of A.*

Proof. We show how to transform a proof (resp. a counter-model) of $\alpha \supset X_1, \ldots, \alpha \supset X_n \vdash A_\alpha$ into a proof (resp. a counter-model) of $\vdash A$.

Suppose that we have a proof of $\alpha \supset X_1, \ldots, \alpha \supset X_n \vdash A_\alpha$. We remark that substituting $\bot$ for α in A_α produces A. Let σ be the substitution $\{\alpha \mapsto \bot\}$. We obtain the following proof of $\vdash A$:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\cdots}{\alpha \supset X_1, \ldots, \alpha \supset X_n \vdash A_\alpha}}{\bot \supset X_1, \ldots, \bot \supset X_n \vdash A}[\text{Subst}_\sigma] \quad \dfrac{\dfrac{}{\bot \vdash X_1}[\bot_L]}{\vdash \bot \supset X_1}[\supset_R]}{\bot \supset X_2, \ldots, \bot \supset X_n \vdash A}[\text{Cut}] \quad \cdots}{\cdots} \quad \dfrac{\dfrac{}{\bot \vdash X_n}[\bot_L]}{\vdash \bot \supset X_n}[\supset_R]}{\vdash A}[\text{Cut}]$$

On the other hand, we suppose that $[\![\cdot]\!]$ is a counter-model of the sequent $\alpha \supset X_1, \ldots, \alpha \supset X_n \vdash A_\alpha$. Then for any i, the property $[\![\alpha \supset X_i]\!] > [\![A_\alpha]\!]$ holds. In the $n = 0$ case (i.e. A does not contain any variable) we get the property $[\![A_\alpha]\!] < \infty$, and this property also holds in the case $n > 0$.

We now prove that the identity $[\![\alpha]\!] \leqslant [\![X_i]\!]$ holds for any i. If $n = 0$, the property trivially holds. Otherwise, let i_0 an index such that the value of $[\![\alpha \supset X_i]\!]$ is minimal and let $\delta = [\![\alpha \supset X_{i_0}]\!]$ be this value. We prove by contradiction that $[\![\alpha]\!] \leqslant \delta$.

We suppose $[\![\alpha]\!] > \delta$. Then all the atoms of A_α are interpreted by values (the $[\![X_i]\!]$'s and $[\![\alpha]\!]$) which are greater than δ. Then by definition of $[\![\cdot]\!]$, $[\![A_\alpha]\!]$ is necessarily greater than δ. So $[\![\alpha \supset X_{i_0}]\!] > [\![A_\alpha]\!] \geqslant \delta$. But as $[\![\alpha]\!] > [\![X_{i_0}]\!] = \delta$, we obtain $[\![\alpha \supset X_{i_0}]\!] = [\![\alpha]\!] \rightarrow [\![X_{i_0}]\!] = \delta$ and a contradiction.

For any i, $[\![\alpha]\!] \leqslant [\![X_i]\!]$ holds. Thus we can define $[\![X]\!]' = [\![X]\!] - [\![\alpha]\!]$ for $X \in \{\alpha, X_1, \ldots, X_n\}$, the other values of the semantic function do not matter. In this new semantic, α is interpreted by 0 which is the same as $\bot$ and thus, $[\![A]\!]' = [\![A_\alpha]\!]'$. Moreover, by the definition of the semantic function $[\![\cdot]\!]$ on formulae, for any formula B, built with atoms in $\{\alpha, X_1, \ldots, X_n\}$, the identity $[\![B]\!]' = [\![B]\!] -$

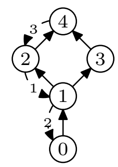
$[\![\alpha]\!]$ holds.[16] In particular $[\![A_\alpha]\!]' = [\![A_\alpha]\!] - [\![\alpha]\!] < \infty$. Thus, since $[\![A]\!]' = [\![A_\alpha]\!]'$, the function $[\![\cdot]\!]'$ is a counter-model of A.

For the size of the sequent $\alpha \supset X_1, \ldots, \alpha \supset X_n \vdash A_\alpha$, it is linear in the size of A since the number of variables in A is lower than the size of A. □

B Example of linear computation of μ_φ

We develop an full example of computation of the fixpoint μ_φ on the graph of variables $\mathcal{G}$, see section 7. We choose the following sequent:

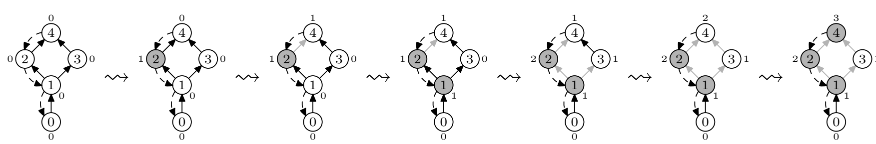
$$0 \supset 1, 1 \supset 2, 1 \supset 3, 2 \supset 4, 3 \supset 4 \\ \vdash 2 \supset_1 1, 1 \supset_2 0, 4 \supset_3 2$$

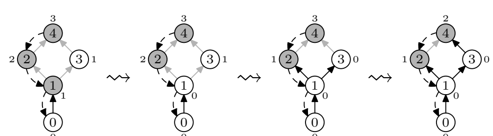


In the graph on the right-hand side, the black arrows represent the real graph structure, the dashed (and numbered) arrows are only displayed to remind the reader of the implications on the right ($X_i \supset Y_i$).

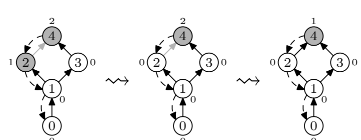
We display the weight function $\mathcal{S}_Z$ on $\mathcal{G}$ by marking the vertexes K such that K occurs in the multiset $\mathcal{S}$ and the arrows $K \to Z$ such that $\mathcal{S}_K > 0$. We also display the current value of $\mathcal{S}_Z$ beside the vertex Z

The first stage is to compute $(\mathcal{X}_{\{1,2,3\}})_Z = (2,1,4)_Z$. We start from $(\emptyset)_Z$ which is the zero weight function and compute successively $(2)_Z$ (two steps), $(2,1)_Z$ (three steps) and $(2,1,4)_Z$ (one step):





Thus, we obtain the value of I_1 which is $\{2\}$ because $1 \to_2 0$ is the only dashed arrow for which the end-vertex has weight 0. So, we have to compute $(\mathcal{X}_{\overline{I_1}}) = (\mathcal{X}_{\{1,3\}})_Z = (2,4)_Z$. We unmark vertex 1 (corresponding to the dashed arrow $1 \to_2 0$) and recompute the weight function in 3 steps.



The computed value of I_2 is $\{1,2\}$ because $2 \to_1 1$ and $1 \to_2 0$ are the two arrows for which the end-vertex has weight 0. We unmark vertex 2 (corresponding to the dashed arrow $2 \to_1 1$) and recompute the weight function $(\mathcal{X}_{\overline{I_2}}) = (\mathcal{X}_{\{3\}})_Z = (4)_Z$ in 2 steps.

We obtain $I_3 = \{1,2,3\}$ and stop. The fixpoint is $[1,3]$. We can derive the counter-model: from the weights we obtain $\mathcal{X}_{\{1,2,3\}} \Vdash \{1,2,3,4\}$, $\mathcal{X}_{\{1,3\}} \Vdash \{2,4\}$, $\mathcal{X}_{\{3\}} \Vdash \{4\}$ and $\mathcal{X}_\emptyset \Vdash \emptyset$. Thus the counter-model is defined by $[\![0]\!] = 0$, $[\![1]\!] = [\![3]\!] = 1$, $[\![2]\!] = 2$ and $[\![4]\!] = 3$.

[16] This is trivial by induction on B, since the operation $x \mapsto x - [\![\alpha]\!]$ strictly preserves the order on the semantic values of atoms. Remark that the $-$ operator is defined in such a way that the identity $\infty - [\![\alpha]\!] = \infty$ holds.