University of Groningen

Bachelor Project

Essay

Circular proofs in Gödel-Löb logic

Authors:
Wopke de Vries (s2712121)

Supervisors:
Prof. Dr. L. C. Verbrugge
Prof. Dr. T. Müller

April 3, 2020

Abstract

In the Gödel-Löb provability logic we want to find alternatives to the cut-rule. This paper provides an alternative in the form of circular proofs. This paper explains in detail the result that Shamkanov made in this field, closely following his original paper on the subject.

Contents

1 Introduction

There are those that argue that going around in circles is unhelpful. Even though these people have been notably wrong since the invention of the wheel, we will give a different example of the helpfulness of going around in circles by its use in logic. Now, the same people who think that going around in circles is unhelpful will argue that going around in circles is a logical fallacy. This paper on circular proofs will show that not only is it the case that going around in circles does not necessarily mean that we are creating a logical fallacy, we can actually prove things about provability of mathematical statements using circular proofs.

In this paper we will explain what these circular proofs are, how they relate to sequent calculus, and how they work in the Gödel-Löb logic. Though the reader may currently not understand a word of the previous sentence except for 'paper', we will in this paper go into detail and explain to the reader what is meant by the other terminology. We will step-by-step explain how to get to circular proofs and how to apply them. We will mainly follow and study the original paper by Shamkanov titled 'Circular Poofs for the Gödel-Löb Provability logic. In this paper he popularized looking at new ways of viewing systems of proof for certain logics and sparked an interest in applying circular proofs to different logics like μ-calculus. One of the main reasons to study circular proofs is that by applying it to the logic GL, we can eliminate the cut-rule, which has been a thorn in the side of researchers of logic, especially for those that are trying to automate proofs.

The general view of mathematicians and logicians on mathematics has drastically changed over the last century and we hope that by reading this paper, the reader will get a new perspective on mathematics, specifically on proofs in Peano arithmetic. Since it is the case that the study of circular proofs has only recently begun to be explored, a lot of progress can be expected to be made in the field. With the current interest in automating proofs for logical statements, the field of provability theory may become a more and more important field of logic in the upcoming years. Reading this paper is an easy way to familiarize one with the mathematical proofs behind provability logic and proof theory. Even if one is not reading this paper with automating proofs as their goal, it may still be useful to see how such proofs are done, especially because of the possible ramifications for proofs in Peano arithmetic.

We will first go over the history of proof theory and provability logic in Section 2. We will look how the field first came to be studied and the progress that has been made in recent years. In Section 3 we will familiarize the reader with the Gödel-Löb provability logic. Sequent calculus will be the topic of Section 4, where we will introduce the useful tool for helping us derive the truth of complex statements that is sequent calculus. Finally, in Section 5 we will discuss the main subject of this paper. We will introduce circular proofs and show that these actually work on the Gödel-Löb logic. Furthermore, we will give a proof that the Lyndon interpolation property holds for Gödel-Löb logic by using circular proofs, showing the reader that circular proofs are useful in practice.

2 History of Proof Theory and Provability Logic

In this section we will go over the history of proof theory and of provability logic. We will take a look at some of the people that have brought the field to the state that it is in today, and the advancements they have made over the previous iterations of thought about what it means for a proof to be a proof. We will mainly look at the history of proof theory and provability logic over the last century and discard most of the history that the subject has before this. Even though people like Aristotle [3] have made contributions to proof theory, they are not interesting to consider for the purposes of this paper or for the current state of proof theory and provability logic.

To talk about the current state of proof theory and provability logic, we will first take a look at the state that it was in when the field first started becoming more popular as a field of study. At the start of the 20th century, Hilbert [12] was interested in creating a proof theory such that mathematics had a foundation based on logic that had the following properties:

1. Axioms should be mutually independent, meaning that no information in an axiom can be derived from the other axioms. Stated differently, the set of axioms should be set-minimal.
2. The formalization must be complete: all statements must be true or false and provable as being such.
3. The formalization must be consistent, meaning that there must be no inherent contradiction in its axioms.

This way of thinking about mathematics, perhaps somewhat idealistically, was the standard for some time, and almost all mathematicians subscribed to the notion of this *Hilbert Program* and its goals. This includes many famous mathematicians amongst whom is Von Neumann.

The next major contribution to proof theory is probably also the best-known contribution. Because in 1930 Gödel came up with his famous Incompleteness Theorem [10]. Gödel's Incompleteness Theorem states that 'If a logically consistent system contains a certain amount of Peano arithmetic, it is incomplete'. This means that if we want to ground mathematics in logic, we either cannot allow Peano arithmetic to be a part of mathematics, which is a ridiculous notion, or the system that we create will contain Peano arithmetic and be incomplete, meaning that there are certain statements that are improvable. This caused a major change in the field, as it had been shown that the goals of Hilbert's Program were unachievable.

The next step in the history of proof theory was made by Gentzen [6]. He found the same result as Gödel, that the aim of the Hilbert Program was not achievable, but through a different method. He set out to put logic behind the principles that mathematicians used in their proofs. The first thing he contributed to such a goal was to create a system for how certain statements follow from other statements. This system is known as *natural deduction*, sometimes shortened to ND. Natural deduction has rules of the kind 'if A is true and B is also true, then A and B is true'. By formalizing these rules so that they are easier to use, he created one of the first formalized systems of logic for mathematics. This style of doing things had rules for conjunction, implication, and only a single cut rule. Because of its simplicity it was a great starting point to continue research from. And so he did: based on the notion of natural deduction he came up with *sequent calculus*, which is discussed in detail in Section 4. Sequent calculus deals with mathematical proofs. It is a way of simplifying statements that are true in ways of the truth of the propositional atoms used in such a statement. It does however not show us how to prove these atoms in and of themselves, but this is left to the way that a system is axiomized and which statements are seen as elementary truths of such a system. It is important to note that natural deduction and sequent calculus pertain to logic and not to mathematics and Peano arithmetic.

Therefore, Gentzen set out to prove the consistency of Peano arithmetic and succeeded to do so in 1934, however, this original proof has gotten lost and is not known. Then again, the proof that he gave in 1935 [6] is known. This proof is based on combining natural deduction and sequent calculus to create the sequent calculus of natural deduction. This 'second proof' that Gentzen gave starts by using the logic that allows only for conjunction and negation, which is equivalent to the entire logic, as all statements can be rewritten in a form that allows only conjunction and negation. Then, Gentzen shows that by using the rules of natural deduction and by applying some of the principles of sequent calculus, we get a result for Peano arithmetic that shows that every possible statement using Peano arithmetic is reducible and either gains a conclusion that is true, or assumptions that are inconsistent. Therefore, every statement that can be made using Peano arithmetic is either provably true or it can be shown that assumptions of a statement are inconsistent, meaning that Peano arithmetic is consistent. Even though there is nothing wrong with this proof of consistency for Peano arithmetic, Gentzen still received some criticism based on the assumptions for his model. He went on to creating an almost unreadable third proof [7] and a fourth proof [8] that finally settled the matter of the consistency of Peano arithmetic, this time completely in the style of sequent calculus. He also replicated the result of Gödel that arithmetic is incomplete using ϵ calculus.

Now that consistency of Peano arithmetic had been shown, the field of proof theory laid their sights on another question. The aim of the field at the end of Gentzen's career and after Gentzen was to prove (or disprove) the consistency of analysis, analysis being the theory of real numbers. Gentzen himself did manage to prove at the end of his career that analysis is consistent for transfinite ordinals up to ϵ_0. When studying analysis, we also deal with quantifiers, which makes the study of this field even more complex than the study of arithmetic. For some time after Gentzen, almost no tangible progress was made in this field.

Therefore we will now briefly aim our sight at provability logic. Provability logic is a logic that allows a provability predicate to exist. Provability logic has had two instances where it became interesting to study it. The first was after Gödel's incompleteness theorems showed that not everything that is true is provable in formal mathematical theory. This leads to a question about what kinds of statements are fundamentally not provable, which helps us in the pursuit of mathematical proofs by giving us a tool that can deem certain mathematical conjectures as not provable and therefore not a good investment of researchers' time. The second way that provability logic is interesting is because it is a type of meta-mathematics in the way that statements about provability say something fundamental about mathematics itself. Especially if we allow our atoms to be sentences such as: "this sentence is not provable", the implications for the types of statements that can be mathematically proven are interesting. The question of how a provability predicate changes the way we look at certain statements is a question by Henkin, based on Gödel's incompleteness theorem [11], it gave an influx in the study of provability theory in the 1950s, almost 20 years after Gödel came with his result. The main theorems and other facts known about provability theory came mostly after Henkin came with his questions about provability.

The first step in thinking about provability logic is establishing the rules that come with the provability predicate, and how to incorporate it into arithmetic. The latter is done by encoding any logical statement into a unique number, using the uniqueness of prime factorization. For this number it is not really important in what way we code it, just that every statement has a unique number associated with it. Usually this is done by using primes. The way that we note down the number associated with a statement P is $\ulcorner A \urcorner$. The major step is then to see that if a statement P is true, that another sequence of logic symbols, let's say S, has to exist that is a proof for statement P. Then we can introduce the provability predicate as being $\text{Prov}(\ulcorner P \urcorner)$, which stands for $\exists S$ $\text{Proof}(S, P)$. Meaning that for the number associated with statement P, there exists a number associated with a statement S, such that S proves that P is true. As we can see, this provability predicate nicely describes the way we think about proofs and the way that we use proofs in reality.

Now that a language has been defined for the study of Provability Logic, we can try to see what happens when certain statements are plugged into formulas that use such a predicate. After these definitions were established, Löb [17] started to answer the question that Henkin asked about statements asserting their own provability. Löb therefore looked at the statement

$$P \leftrightarrow \text{Prov}(\ulcorner P \urcorner).$$

After studying this statement, Löb came to the conclusion that in Peano arithmetic, the only way that

$$\text{Prov}(\ulcorner P \urcorner) \rightarrow P$$

can be true, is if P is already provable in Peano arithmetic. Even though this result may see really mundane and not interesting at first glance, it is an important result. It means that we have another universal rule for Provability logic. This rule, also written

$$\text{Prov}(\ulcorner \text{Prov}(\ulcorner P \urcorner) \rightarrow P \urcorner) \rightarrow \text{Prov}(\ulcorner P \urcorner)$$

is called Löb's Theorem. Löb went on in his paper to discover three more rules for the provability predicate:

1. If $\text{PA} \vdash P$, then $\text{PA} \vdash \text{Prov}(\ulcorner P \urcorner)$
2. $\text{PA} \vdash \text{Prov}(\ulcorner P \rightarrow S \urcorner) \rightarrow (\text{Prov}(\ulcorner P \urcorner) \rightarrow \text{Prov}(\ulcorner S \urcorner)$
3. $\text{PA} \vdash \text{Prov}(\ulcorner P \urcorner) \rightarrow \text{Prov}(\ulcorner \text{Prov}(\ulcorner P \urcorner) \urcorner)$

Now, the notation using the provability predicate started to become too cumbersome. Luckily, it was realized that the provability predicate shares a lot of commonalities with modal logic, and instead of the provability predicate, the switch was made to use the $\Box$ as a replacement.

Putting Provability logic into the form of modal logics has the added benefit that we can study Provability logic as an extension of the basic modal logic **K**. This logic has gotten the name 'Gödel-Löb logic' or GL for short, and will be studied further in Section 3.

Meanwhile, in the field of proof theory, other steps were being taken to further the development of sequent calculus. Ketonen [14] managed to create a sequent calculus and to proof that the rules that this sequent calculus uses are invertible, meaning we can go back up the tree after having reached our conclusion. This discovery is very useful in application, as it helps us simplify certain other questions within the study of proof theory. Later two other proofs were given of invertibility [24] [4] and also a proof of height preservation [4].

For some time after Ketonen, the field just went on improving and expanding on the previous results and no extremely ground-breaking results were made. One example of expanding the known proof theory was by inserting quantifiers into the mix of predicates that can be used, as done by Quine [20]. Adding existential and universal quantifiers is only one of the ways that people have expanded onto the groundwork that was laid out by Gentzen. There has been a lot of study of proof theory of various logical systems, and almost every possible modification of the axioms of certain logics like the logic K has at least some amount of research behind it with differing results.

In 1976 another big result in the area of provability logic came out, Solovay [30] managed to show a relation between the provability logic of Gödel-Löb and Peano arithmetic. This is a huge result as it shows that mathematical statements about arithmetic can be studied within the scope of logic, and that the results gotten in Gödel-Löb logic have repercussions for the kind of statements that are provable within Peano arithmetic. The relation that Solovay managed to show is

$$\text{GL} \vdash A \text{ iff for all formulations } f,\ \text{PA} \vdash f(A),$$

where GL stands for the Gödel-Löb logic of provability and PA for Peano arithmetic. A formulation f is a way of representing a logical sentence in the language of Peano arithmetic. As for how to find these realizations in Peano arithmetic from the structure of the statement A we refer to Solovay's paper [30].

After this time, there have been a number of research fields that have captured some attention relating to the Gödel-Löb logic that have had some result. For example there has been development in the field of finding cut-free systems of sequent calculus. Many different results have been published in this field, one of the earlier one a paper by Leivant in 1981 [15] that creates a cut-free sequent calculus for the Gödel-Löb logic. Though the sequent calculus created by him was correct, Leivant's proof had some mistakes in it and was corrected by Valentini in 1983 [31]. In more recent years, there have been more small improvements in the field of cut-free sequent calculi for certain logic systems, amongst these are a paper by Brotherston and Simpson [2] on cut-free sequent calculus the systems LKID and LKID^{ω}, but also progress in the field of provability logic specifically, for example a paper by Poggiolesi on a cut-free sequent calculus for the Gödel-Löb logic [19], and a paper by Ramayanake that delivered a more accurate proof for Valentini's earlier cut-free version of sequent calculus on the Gödel-Lob logic [9].

More recently, there have been a number of articles on provability logic, notably by Shamkanov on Gödel-Löb logic, amongst which is the paper studied in Section 5 of this paper on circular proofs [27]. He has written extensively on the topic, including an article on interpolation in Gödel-Löb logic [26] and putting forward a theorem on realization [28]. Shamkanov still does not seem to be done writing on the topic, and published another paper on non-well-founded derivations in Gödel-Löb in 2019 [25].

Ever since Gödel came out with the result on incompleteness of arithmetic, the field has been an interest for many. This can be seen at the steady stream of results that have been published. When we study the result by Shamkanov on Circular Proofs in Section 5 we hope to clarify this result, however it must be noted that though this result is important it is by no means the final result that we can expect in this field, or even from Shamkanov. In the future we can expect more steady progress, helping us to understand the underlying mechanics behind logic and mathematics. With so many possibilities in the way that we choose our logic to behave, we can be sure that there will be no shortage of things to prove in the field of proof theory for some time.

3 The Gödel-Löb logic

The Gödel-Löb logic is one of the many provability logics out there, however it is also seen as the root of all of them. This is because the system of Gödel-Löb (GL) is the first of such systems to be studied, and also because it is in a way the most intuitive and basic way of thinking about provability. The rules of GL are the same rules as those of the logic K, with some additions. Its rules are the following: From the system K:

- All instances of propositional tautologies,
- all instances of the Kripke schema

$$\Box(A \to B) \to (\Box A \to \Box B), \tag{1}$$

- the closure rules Modus Ponens

$$A, A \to B \vdash B, \tag{2}$$

- and the necessitation rule

$$\text{If} \vdash A \text{ then } \vdash \Box A. \tag{3}$$

Where we note that $\Box A$ has interpretation ‘there exists a proof for the statement with Gödel number A’, it is the same as ‘Prov ($\ulcorner A \urcorner$)’. In addition to these rules from the logic of Kripke, K, we have the following rule;

- Löb’s Theorem which gives the logic part of its name

  Theorem 3.1. (**Löb’s Theorem**)
  For any propositional formula P, we have that $\Box(\Box P \to P) \to \Box P$.

The form in which we have written this theorem above is not the original form, as Löb's theorem is a result on the provability of statements in Peano Arithmetic. If we recall Section 2, Löb's theorem is a result that was gained after the study of the question by Henkin. To prove Löb's theorem we must first introduce Gödel's diagonalization lemma

Lemma 3.2. (Gödel's diagonalization lemma) For any arithmetical formula $f(x)$ there exists an arithmetical formula P such that

$$P \leftrightarrow f(P)$$

and another result of Löb, namely his third derivability condition

Proposition 3.3. In provability logic the following holds for any statement P;

$$\text{PA} \vdash \text{Prov}(\ulcorner P \urcorner) \to \text{Prov}(\ulcorner \text{Prov}(\ulcorner P \urcorner) \urcorner) \tag{4}$$

in our alternative notation $\vdash \Box P \to \Box(\Box P)$

Proof of Löb's theorem (adapted from Verbrugge [32])
To prove Löb's theorem we first assume that

$$PA \vdash \Box A \to A.$$

Take Gödel's diagonalization lemma and apply it to the formula

$$f(x) = x \leftrightarrow (\Box x \leftrightarrow A)$$

Let's take an instance that satisfies this condition and call this statement B. Then we have the following:

$$PA \vdash B \leftrightarrow (\Box B \leftrightarrow A). \tag{5}$$

Applying the necessitation rule 3 gives us

$$PA \vdash \Box B \leftrightarrow \Box(\Box B \leftrightarrow A),$$

adding this together with one of the basic modular rules we get

$$PA \vdash \Box B \leftrightarrow (\Box\Box B \leftrightarrow \Box A).$$

applying Löb's third derivability condition (4), as well as Modus Ponens we gain the statement

$$PA \vdash \Box B \to \Box A.$$

Recall our assumption

$$PA \vdash \Box A \to A,$$

this means that together with the earlier statement we have

$$PA \vdash \Box B \to A$$

by the earlier use of the diagonal lemma 5 we get

$$PA \vdash B,$$

and therefore we have by an application of the necessitation rule

$$PA \vdash \Box B$$

which gives us finally

$$PA \vdash A.$$

This completes the proof, as we have shown from the assumption of

$$PA \vdash \Box A \to A$$

that

$$PA \vdash A$$

$\Box$.

Another important theorem for GL is the fixed point theorem by Sambin [23].

Theorem 3.4. Fixed point theorem
For any atom p that is under the scope of a modal in a formula $A(p)$, there exists another formula B not containing p, such that

$$GL \vdash B \leftrightarrow A(B).$$

Where all atoms occurring in B already occur in A.

For the proof of this theorem see the original paper by Sambin [23] or see Reidhaar-Olson [22] for a more compact proof and a constructive algorithm for the fixed point.

Example 3.5. For example, the formula

$$A(p) = \Box \neg p$$

has the fixed point

$$B = \Box \bot$$

meaning that

$$GL \vdash \Box \bot \leftrightarrow \Box \neg (\Box \bot)$$

It is good to note that B also does not contain any atoms, as the only atom in the statement $A(p)$ is p.

The other main result in GL is the result shown by Solovay in 1976 [30] which showed that the link between Peano Arithmetic and GL is really strong.

Theorem 3.6. Solovay's completeness theorem

$$GL \vdash A \text{ if and only if for all realizations } f,\ PA \vdash f(A).$$

This theorem shows that we can really say everything about provability in Peano Arithmetic while studying it using the GL logic. This is one of the reasons why studying the GL logic can be very useful. To prove this result, Solovay used the possible world semantics. For the proof see Solovay [30].

Lemma 3.7. The GL logic can be studied using a possible worlds model $M =< W, R, V >$ with a restriction on the frames $F =< W, R >$ that we study, namely the restriction that the accessibility relation has to be transitive and conversely well-founded.

This lemma is also useful when studying proofs in the GL logic. Even though different methods of proving exist besides the possible worlds model, the possible worlds model is one of the most intuitive in understanding the meaning of modal operators. One of the other ways that we can study proofs in the GL logic is sequent calculus, which we study in the next section, Section 4.

4 Sequent Calculus

In this section we will take a look at sequent calculus. Sequent calculus is one of the proof systems that has been proposed and came after the introduction of natural deduction by Gentzen. In this section on sequent calculus we will mainly try to explain the rules of sequent calculus for Gödel-Löb and not go too much into the other details concerning sequent calculus. The main goal of this Section is to understand sequent calculus to such a degree that we can begin to understand the paper on circular proofs by Shamkanov [27].

Sequent calculus gets its name from the German word 'Sequenz' meaning sequence, from Gentzen. Sequent calculus therefore means the calculus of sequences. The reason it is a calculus of sequences is because the assumption set can be seen as a list or sequence. We will denote such a *sequent* by Γ, where $\Gamma = A_1, A_2, ...A_n$.

Sequent calculus is a different way of defining a logical system. This alternative notation we will denote for Gödel-Löb logic by $\mathrm{GL_{Seq}}$, the sequent-style notation for the Gödel-Löb logic. Applying the rules of sequent calculus, we have to note that we will get trees; these trees should be read from bottom to top. Even though there are people using sequent calculus with trees that go top to bottom, it is easy to be confused if the reader is used to tableaux-style proofs of systems, which are top to bottom.

For the semantics of our language, let P be a propositional variable, and let A and B be formulas. Then the semantics for our language is:

$$P|\overline{P}| \perp |\top|A \wedge B|A \vee B|\Box A| \diamond A$$

To define the rules of sequent calculus we will first note that for negation we use $\overline{A}$ as 'negation of A', where A is any formula. The rules for this operation are from De Morgan's laws. As for the rules of negation together with the modal operators we have the rules:

$$\overline{\Box A} = \diamond \overline{A}$$

$$\overline{\diamond A} = \Box \overline{A}$$

where we note that $\diamond A$ can be read as 'possibly A', or, in the context of provability logic, 'not A is not provable', we additionally use the rules

$$\overline{\bot} = \top$$

$$\overline{\top} = \bot \ .$$

It is also important to note that when we write down a statement in sequent calculus that the statement A, B for example, is read as; 'in a sequent, we have A or B as conclusion'. Often we have statements of the form Γ, A, B. In such a case, consider Γ as a set of sequents; $\Gamma = \{A_1, A_2, ..., A_n\}$ in such a case we can read this as 'Either one of the statements in Γ is true or A is true or B is true.'

Definition 4.1. A rule is said to be *admissible* in a certain system if it does not change the set of provable things in that system [13]. In other words, everything that is provable with the addition of a rule that is *admissible* should be provable without it. The definition of admissibility is useful to us since we want to add two rules to GL_∞.

For GL, sequent calculus admits the following axioms and inference rules that are admissible for the logic K:

- $\Gamma, A, \overline{A}$
- $\Gamma, \top$
- $\wedge \ \dfrac{\Gamma, A \qquad \Gamma, B}{\Gamma, A \wedge B}$
- $\vee \ \dfrac{\Gamma, A, B}{\Gamma, A \vee B}$

in addition, $\mathrm{GL}_{\mathrm{Seq}}$ also admits the $\Box$-rule for GL:

$$\Box_{GL} \frac{\Gamma, \diamond\Gamma, \diamond\overline{A}, A}{\diamond\Gamma, \Box A, \Delta} \tag{6}$$

and the cut rule

$$\text{cut} \frac{\Gamma, A \qquad \Gamma, \overline{A}}{\Gamma}.$$

To get the sequent calculus rules for the standard modal logic K4, we have to replace the rule $\Box_{\mathrm{GL}}$ by the rule [18]

$$\Box \frac{\Gamma, \diamond\Gamma, A}{\diamond\Gamma, \Box A, \Delta} \tag{7}$$

Proposition 4.2. The generalized Löb rule

$$\frac{\Gamma, \diamond\Gamma, \diamond\overline{A}, A}{\Gamma, \diamond\Gamma, A}$$

is admissible for GL.

Proof. The $\Box$ rule for GL together with the nessecitation rule, shows that the generalized Löb rule is admissible for GL, by the following inferences:

$$\Gamma, \diamond\Gamma, A \to \Gamma, \diamond\Gamma, \Box A$$

$$\frac{\Gamma, \diamond\Gamma, \diamond\overline{A}, A}{\diamond\Gamma, \Box A, \Delta}$$

Where in the last step, we put Γ into the 'miscellaneous set' Δ of the inference rule. $\Box$

The goal of every branch of a sequent-style proof is to end up at an axiom. This is useful, since then only these axioms will have to be checked to verify the truth of the final sequent.

Example 4.3. We will do a short sequent-style derivation of the statement $(P \vee \Box P) \to Q$. We first note that by De Morgan's laws we can rewrite this to $\overline{P \vee \Box P} \vee Q$

$$\cfrac{\cfrac{\cfrac{\overline{\Box P}, Q \qquad \overline{P}, Q \ (\wedge)}{\overline{P} \wedge \overline{\Box P}, Q \ (\text{De Morgan})}}{\overline{P \vee \Box P}, Q \ (\vee)}}{\overline{P \vee \Box P} \vee Q}$$

In this example we first apply the $\vee$ rule, then one of the De Morgan's laws to rewrite our statement, and finally the $\wedge$ rule to get to a form that contains axioms. The statements $\overline{\Box P}, Q$ and $\overline{P}, Q$ are considered the leaves of this tree. This example shows that if we want to prove the statement $GL \vdash \overline{P \vee \Box P} \vee Q$, that this is equivalent to showing $GL \vdash \overline{P}, Q$ and $GL \vdash \overline{\Box P}, Q$. Because of this reduction, we have simplified this statement into respective formulae that have to be checked to see if the statement holds. The significance for proofs of this type of proof is that it reduces fairly complex statements to simpler ones of which the validity can be more easily ascertained. It is to be noted that in this example we have given a basic unwrapping of a statement using sequent calculus. We note that sequent calculus does not claim anything about the truth of the formulae $\overline{P}$, $\overline{\Box P}$ and Q.

The only thing that this leaves us is to introduce some more of the lingo that is used in sequent calculus. There are two notions that are the most important to know: that of *formal* derivations and proofs and the notion of a *regular* derivation.

Proposition 4.4. We define the following statements:

- A *formal derivation from premises* is a finite tree of sequents.
- A *formal proof* is a derivation where all the trees are marked by axioms.
- A *regular tree of sequents* is a tree with only finitely many different subtrees.

Any other definitions are not assumed to be knowledge and will, if needed, be defined in the section where we study Shamkanov's paper on Circular Proofs [27].

One of the things that is frequently studied in the field of sequent calculus is systems where the cut rule can be removed. The reason to eliminate the cut rule from systems is that it is an annoyance when trying to find a proof from premises to conclusion, since the cut rule effectively removes statements from the proof if you work from premises to conclusion, whereas if we are busy reducing our statement to axioms that it depends on we suddenly introduce a new statement where it is unclear when to apply the cut rule.

5 Circular Proofs

In this section we will take a look at a paper by Shamkanov [27] that is about *circular proofs* for the GL logic. The main result of this paper is that when we use these circular proofs instead of the Löb rule for GL as a rule for Sequent Calculus, we can show that the system we end up with is equivalent to the GL logic with the Löb rule. Furthermore, Shamkanov shows that when we use circular proofs instead of the Löb rule for our derivations, we can show a stronger version of Lyndon interpolation property for the Gödel-Löb logic.

5.1 Circular Proofs and Equivalency to Deductions on the GL Logic

To understand the paper by Shamkanov it is first important to understand what a circular proof is.

Proposition 5.1. (from Shamkanov [27]) A *circular derivation* is a pair (k, d) where k is an ordinary formal derivation and d is a function with the following properties: d is defined on a subset of leaves of the derivation k; the image $d(x)$ of a leaf x lies on the path from the root of k to the leaf x; and x and $d(x)$ are marked by the same sequents. If the function d is defined at a leaf x, then we say the the nodes x and $d(x)$ are marked by a *back-link*.
A *formal circular proof* is a circular derivation in which every leaf is either connected with some node by a back-link or marked by an axiom.

To make sense of this proposition, we will try to phrase it differently. A circular proof links a sequent in a derivation, with the same sequent on a different node in the same path. Let's say we mark the higher node by x_i, then a circular derivation is the pair (k, d) where k is a regular derivation without any circular derivations, and d is the function that shows for every possible circular derivation which nodes are linked together by a back-link that is a circular derivation.

In the not unlikely case that this still leaves the reader confused, we will give an example of a circular proof. It is also noted by Shamkanov [27].

Example 5.2.

$$\dfrac{\dfrac{\dfrac{\dfrac{(\Box)\Box\mathbf{P}\wedge\overline{\mathbf{P}},\diamond(\Box\mathbf{P}\wedge\overline{\mathbf{P}}),\mathbf{P}}{(\wedge)\Box P\diamond(\Box P\wedge\overline{P}),P}\qquad(\wedge)\overline{P},\diamond(\Box P\wedge\overline{P}),P}{(\Box)\Box\mathbf{P}\wedge\overline{\mathbf{P}},\diamond(\Box\mathbf{P}\wedge\overline{\mathbf{P}}),\mathbf{P}}}{(\vee)\diamond(\Box P\wedge\overline{P}),\Box P}}{\diamond(\Box P\wedge\overline{P})\vee\Box P}$$

Where we have marked the nodes x and $d(x)$ in boldface and we note that the node $d(x)$ is always the lower one. Note that we can only construct a back-link in this way since the sequents corresponding to the nodes are on the same subtree of the total tree. We also note that an application of the box rule has happened in between x and $d(x)$, which is in fact nessecary.

Proposition 5.3. Any back-link will have an application of the $\Box$-rule in between $d(x)$ and x.

Proof. Every inference rule decreases the complexity of our statement, except for the $\Box$-rule. Since the sequents at x and $d(x)$ are the same, so is their complexity. Therefore, since x and $d(x)$ do not refer to the same node, a $\Box$-rule will have to have been applied in between both nodes. $\Box$

The big theorem put forward in this paper by Shamkanov is one concerning an equivalence relation between several types of proofs.

Theorem 5.4. The following equivalencies hold:

$$GL_{seq} \vdash \Gamma \Longleftrightarrow GL_{\infty} \vdash \Gamma \Longleftrightarrow GL_{circ} \vdash \Gamma. \tag{8}$$

We note that GL_{Seq} is the standard sequent calculus style of derivations on the Gödel-Löb logic, GL_{∞} the ∞-derivation type of derivation for the Gödel-Löb logic and GL_{circ} the type of derivation that consider circular proofs for the Gödel-Löb logic. The theorem says that any of these derivabilities are equivalent. We will prove this theorem by a circle of implications. First we will show that $GL_{Seq} \vdash \Gamma \Longrightarrow GL_{\infty} \vdash \Gamma$, then show that $GL_{\infty} \vdash \Gamma \Longrightarrow GL_{circ} \vdash \Gamma$ and finally $GL_{circ} \vdash \Gamma \Longrightarrow GL_{Seq} \vdash \Gamma$.

We will, just like in Shamkanov's paper, first get some preparatory work out of the way, making it easier to prove the aforementioned statements.

Proposition 5.5. The following statements hold:

1. All circular derivations can be unraveled to become a regular ∞-derivation.
2. All regular ∞-derivations can be obtained by unraveling a circular derivation.

Firstly, it is easy to see that the first statement holds. For any circular derivation, we can remove the circular derivations (k, d) and replace them with the process that goes on between the sequent at $d(x)$ and the sequent at x, including the sequent at x. This process can then keep being repeated, leading to a regular ∞-derivation, as by this process the subtrees will repeat, meaning that there will still only be a finite number of different subtrees.

Secondly, for the proof of the second statement we have to recall that any regular ∞-derivation π can only have a finite number of different subtrees. We can therefore say that the number of different subtrees is some number $m \in \mathbb{N}$. Since any node b of the tree that is the derivation

π determines some subtree π_b, we know that two cases are possible: there is a finite number of nodes b, in which case each leaf is already marked by an axiom; meaning that the circular derivation is equivalent to the ∞-derivation. In the other case, there is an infinite number of nodes b in the tree that is the derivation π. This can only mean that there is at least one subtree with infinitely many nodes. Any branch that has an number of nodes exceeding m must have some nodes c, d that have the same sequent. Without loss of generality we assume that c is closer to the root of π than d. Then we can cut the branch at the node d and connect the sequent at d with the one at c with a back-link. Doing so for any branch with an number of nodes exceeding m we can create a circular derivation. Any other branch will already have an axiom at the end of it. Since by doing this process, every leaf is either connected with some node by a back-link or marked by an axiom, we now have a (formal) circular proof. $\square$

Lemma 5.6. The following implication holds:

$$GL_{Seq} \vdash \Gamma \Longrightarrow GL_{\infty} \vdash \Gamma \tag{9}$$

Proof. To prove this lemma, we need to find a transformation $h(\pi)$ that creates a proof for GL_{∞} from a proof in GL_{Seq}. We can create such a proof by travelling along the tree π from conclusions to premises, replacing applications of the $\Box_{GL}$-rule by applications of the $\Box$-rule.

This means that for any sequent other than where the $\Box_{GL}$-rule is applied, a formal proof stays the same when the map h is applied to it, whereas when there is an application for the box rule for GL:

$$\Box_{GL}\frac{\Delta, \diamond\Delta, \diamond\overline{A}, A}{\diamond\Delta, \Box A, \Sigma} \tag{10}$$

h replaces it with an application of the Box rule:

$$\Box\frac{\Delta, \diamond\Delta, A}{\diamond\Delta, \Box A, \Sigma} \tag{11}$$

Additionally, when this operation is applied on the GL-$\Box$ rule, the proof gets an additional operation on it. Assume that after this operation we have the subtree τ, then this proof is transformed to $h(f(\tau))$, where $f(\tau)$ is a proof of $\Delta, \diamond\Delta, A$ in GL_{Seq}. We know that $f(\tau)$ exists, as the generalized Löb rule

$$\Box_{GL}\frac{\Delta, \diamond\Delta, \diamond\overline{A}, A}{\Delta, \diamond\Delta, A} \tag{12}$$

is admissible for GL_{Seq}, by virtue of Proposition 4.2. Since this is the only rule that changes the proof in GL_{∞} and the proof for Löb's rule $f(\tau)$ exists, we know that $h(f(\tau))$ will exist. Transforming a tree in this way, by applying h step-by-step travelling from conclusion to premise(s), we get a proof for a sequent in GL_{∞} from one in GL_{Seq}. This sequent tree $h(\pi)$ will have leaves marked by axioms, or infinite trees but finitely many different subtrees. Therefore $h(\pi)$ is a formal ∞-proof of Γ in GL_{∞}. $\square$

For the second part of the proof of Theorem 5.4, we have to introduce some new notions. First we will introduce some additional rules for GL_{∞}. Recalling Definition 4.1 on admissibility, we introduce a lemma on admissible rules for GL_{∞}.

Lemma 5.7. The following rules are admissible in GL_∞:

$$\frac{\Gamma, A \wedge B}{\Gamma, A}$$

$$\frac{\Gamma, A \wedge B}{\Gamma, B}$$

$$\frac{\Gamma, A \vee B}{\Gamma, A, B}$$

$$\frac{\Gamma, \bot}{\Gamma}$$

Proof idea. It is easy to see that we can prove these for GL_∞ by applying the standard rules that we have introduced in Section 4. □

Lemma 5.8. The weakening rule

$$\frac{\Gamma}{\Gamma, A}$$

and the contraction rule

$$\frac{\Gamma, A, A}{\Gamma, A}$$

are admissible for GL_∞

Proof. That the weakening rule is admissible for GL_∞ is not that hard to see: it commutes with the introduction rules $\wedge$ and $\vee$. The admissibility for the weakening rule thus follows from the forms of the axioms and the □-rule.

That the contraction rule is admissible for GL_∞ is a bit harder to prove. We will do so by induction on the structure of a formula A. Let P be an atom, and let B and C be formulae. Though it is not that hard to see that if A has the form $P, \overline{P}, \bot, \top, B \wedge C, B \vee C$ or even $\Box B$, that this holds. Consider $A = B \wedge C$. By the induction hypothesis, the contraction rule holds for B and C separately.

We will give the proof for $A = \diamond B$. The induction hypothesis states that the contraction rule is admissible for B. Once again, let π be the ∞-proof tree of the sequent $\Gamma \cup \{\diamond B, \diamond B\}$. We will define another function $h(\pi)$ that maps a proof of $\Gamma \cup \{\diamond B, \diamond B\}$ to a proof of $\Gamma \cup \{\diamond B\}$. We will look at such a proof travelling from conclusions to premises. First we take a look at what h does when we deal with the $\wedge$ and $\vee$ introduction rules. As for the $\wedge$ rule, h maps

$$\frac{\diamond B, \diamond B, \Delta, C \qquad \diamond B, , \Delta, D}{\diamond B, \diamond B, \Delta, C \wedge D}$$

onto

$$\frac{\diamond B, \Delta, C \qquad \diamond B, \Delta, D}{\diamond B, \Delta, C \wedge D}$$

and in the case of the $\vee$ rule it maps

$$\frac{\diamond B, , \Delta, D}{\diamond B, \diamond B, \Delta, C \vee D}$$

onto

$$\frac{\diamond B\Delta, C, D}{\diamond B, \Delta, C \vee D}$$

All that is left is to define h in the case of the application of the $\Box$ rule. Recall that the $\Box$ rule is the rule

$$\frac{\Delta, \diamond\Delta, C}{\diamond\Delta, \Box C, \Sigma}$$

There are two cases, either $\{\diamond B, \diamond B\} \in \Sigma$ or $\{B, B\} \in \Delta$. In the case $\{\diamond B, \diamond B\} \in \Sigma$, h will delete a copy of $\diamond B$ from the conclusion sequent. In the other case, $\{B, B\} \in \Delta$, we can write $\Delta = \Delta' \cup \{B, B\}$. The map h then does the following transformation on π at such a sequent: it maps

$$\frac{B, B, \Delta', \diamond B, \diamond B, \diamond\Delta', C}{\diamond B, \diamond B, \diamond\Delta\, \Box C, \Sigma}$$

to

$$\frac{B, \Delta', \diamond B, \diamond\Delta', C}{\diamond B, \diamond\Delta\, \Box C, \Sigma}$$

where by the induction hypothesis we know that a proof $f(\tau)$ for the premise must exist. The proof then continues by transforming it to $h(f(\tau))$. The new tree $h(\pi)$ will then be a formal ∞-proof of $\Gamma \cup \{\diamond B\}$ in GL_∞. $\Box$

We can now prove the following lemma:

Lemma 5.9. The following implication holds:

$$GL_\infty \vdash \Gamma \Longrightarrow GL_{circ} \vdash \Gamma$$

Proof. Again, let π be the tree corresponding to an ∞-proof of Γ in GL_∞. Once again, we travel from conclusions to premises through the proof. For a given sequent Δ, let Δ^S denote the set of formulas in Δ, meaning that $\Delta = \Delta^S \cup \Delta'$. We use the previous result to find a function h that maps π to an ∞-proof of Γ that does not contain any duplicates in its sequents, and only finitely many different sequents, since the number of different subtrees is limited. The function h maps the rules for $\wedge$ and $\vee$ onto the same ones. However, for the box rule, h does the following: it changes

$$\frac{\Delta, \diamond\Delta, A}{\diamond\Delta, \Box A, \Sigma}$$

to

$$\frac{\Delta^S, \diamond\Delta^S, A}{\diamond\Delta^S, \Box A, \Sigma, \diamond\Delta'}$$

Once again, this also changes the proof when we go upward. However, once again, there also exists a function $f(\tau)$ that is a proof for $\Delta^S, \diamond\Delta^S, A$, because of the admissibility of the contraction rule. All formulas in $h(\pi)$ are sub-formulae of those in Γ. Since $h(\pi)$ only contains finitely many formulae that are premises of the $\Box$ rule, additionally, premises in all other rules are shorter than their conclusions. Therefore, $h(\pi)$ will contain only finitely many different sequents. This means that from any formal ∞-proof we can obtain another, regular ∞-proof. Therefore, by Proposition 5.5, we can conclude that $GL_\infty \vdash \Gamma \Longrightarrow GL_{circ} \vdash \Gamma$. $\Box$

We jump right into the last lemma of the proof.

Lemma 5.10. The following implication holds:

$$GL_{circ} \vdash \Gamma \Longrightarrow GL_{Seq} \vdash \Gamma$$

Proof. Consider the set of assumptions for a circular derivation (k, d) as a set of non-axiomatic leaves of k that are not connected to a back-link. An assumption is called *boxed* when an application of the $\Box$ rule occurs on the path from such an assumption to the root. We create a partition in these assumptions: $BH(\pi)$ the set of boxed assumptions; and $H(\pi)$, the set of all other (non-boxed) assumptions. We introduce $\boxdot A$ as a shorthand notation for $\Box A \wedge A$. Additionally, we introduce $\Gamma^\sharp$ as a shorthand. If $\Gamma = A_1, A_2, ..., A_n$ then

$$\Gamma^\sharp = \begin{cases} \bot & \text{if } n = 0 \\ A_1 \vee A_2 \vee ... \vee A_n & \text{otherwise} \end{cases}$$

Now, let (k, d) be a circular derivation for Γ. We claim that

$$GL \vdash \bigwedge\{\boxdot\Delta_a^\sharp : a \in H(\pi)\} \wedge \bigwedge\{\Box\Delta_a^\sharp : a \in BH(\pi)\} \to \Gamma^\sharp$$

where Δ_a denotes the sequent corresponding to node a. We want to prove this using induction on the derivation k. In case k contains only one sequent, this statement holds trivially. However, to explain how the notation works we will look at an example. If we have just a sequent A, this statement reads:

$$(A \wedge \Box A) \to A,$$

Which, as mentioned, holds trivially. In case Δ would consist of (A, B) then the antecedent of this implication would read

$$(A \wedge B)^\sharp \wedge \Box(A \wedge B)^\sharp$$

$$(A \vee B) \wedge \Box(A \vee B),$$

and from this it is left to the reader to infer how to extend this to more complicated cases. Of course, we also have to consider the non-trivial cases, so sadly our proof cannot end here. In case k contains multiple sequents, we will take a look at the last application of an inference rule in k. Three possibilities arise:

The $\wedge$ rule

$$\frac{\Delta, A \qquad \Delta, B}{\Delta, A \wedge B}$$

the $\vee$ rule

$$\frac{\Delta, A, B}{\Delta, A \vee B}$$

and the $\Box$ rule

$$\frac{\Delta, \diamond\Delta, A}{\diamond\Delta, \Box A, \Sigma}$$

If this root of k is not connected by a back-link to some leaf, it is important to see that

$$GL \vdash (\Delta, A)^\sharp \wedge (\Delta, B)^\sharp \to (\Delta, A \wedge B)^\sharp$$

$$GL \vdash (\Delta, A, B)^\sharp \to (\Delta, A \vee B)^\sharp$$

$$GL \vdash \Box(\Delta, \diamond\Delta, A)^\sharp \to (\diamond\Delta, \Box A, \Sigma)^\sharp$$

It is not hard to see that these implications hold. We will, however do so explicitly for the first statement by doing simple operations on the antecedent till we get the consequent:

$$(\Delta, A)^\sharp \wedge (\Delta, B)^\sharp$$

$$(\Delta^\sharp \vee A) \wedge (\Delta^\sharp \vee B)$$

We can now see that in case $\Delta^\sharp$ is not true, meaning that none of the sequents in the multiset Δ are true, A must be true and so must B. Therefore we can conclude our deduction with the following steps:

$$(\Delta^\sharp \vee (A \wedge B)$$

$$(\Delta, A \wedge B)^\sharp.$$

We hope that by doing such an elementary deduction, the reader will understand our notation going forward.

In the case that the root of k is connected by a back-link to some leaf of k, it is important to remember that in such a case an application of the $\Box$ rule occurs. See Proposition 5.3 if this is not clear. By once again using the induction hypothesis and arguing in the same way as for the case without back-link, we get

$$GL \vdash \bigwedge\{\boxdot\Delta_a^\sharp : a \in H(\pi)\} \wedge \bigwedge\{^\sharp_a : a \in BH(\pi)\} \wedge \Box\Gamma^\sharp \to \Gamma^\sharp$$

By Löb's theorem, we can then drop the assumption $\Gamma^\sharp$ from the implication premises. This is the case because if we can show that if the first part holds, then $\Box\Gamma^\sharp \to \Gamma^\sharp$, which would mean that $\Gamma^\sharp$ is provable anyway in GL. Therefore we can drop it from our premises. This gives us

$$GL \vdash \bigwedge\{\boxdot\Delta_a^\sharp : a \in H(\pi)\} \wedge \bigwedge\{\Box\Delta_a^\sharp : a \in BH(\pi)\} \to \Gamma^\sharp$$

Therefore, if π is a tree that corresponds to a circular proof of Γ, then $GL \vdash \Gamma^\sharp$. By definition, this is equivalent to $GL_{Seq} \vdash \Gamma$. $\Box$

We have finally shown the main result of the paper. Now we can ask ourselves what the allowance of circular proofs for GL can actually be used for. Luckily for us, Professor Shamkanov helpfully provides us with a result that can be shown using the circular logic for GL, GL_{circ}.

5.2 The Lyndon Interpolation Property

In this subsection we will take a look at the Lyndon Interpolation Property and provide a proof for it using the definitions of circular proofs. Additionally, as it turns out, we can prove a slightly stronger version of the Lyndon Interpolation Property for the logic GL. For an interesting paper about Lyndon interpolation on non-classical logics see [5].

It will come as no surprise that we first want to introduce Lyndon interpolation. However, we must first introduce some other notions, so that the reader can make sense of the theorem regarding Lyndon interpolation.

We will call the atomic variables P_i and their negations $\overline{P_i}$ *literals.* The set of all literals L occurring in a formula A outside of the scope of modal operators is called $u(A)$. Furthermore, we will introduce notation that helps us recognize certain literals, $P_i{}^\circ$ and their negations $\overline{P_i{}^\circ}$ and call them *marked literals.* The set of marked literals L° that do occur under the scope of a modal operator we will call $v(A)$. The set off all such literals we will define as being $w(A) = u(A) \cup v(A)$.

Theorem 5.11. Lyndon Interpolation
If $GL \vdash A \to B$ then there exists a formula C, called the *interpolant* of $A \to B$, such that $w(C) \subset w(A) \cap w(B)$ and

$$GL \vdash A \to C, \qquad GL \vdash C \to B$$

It is important to read this correctly and remember that C cannot be any formula, but is constrained to consisting of formulae that are already in both A and B. This is important, since otherwise any implication can take A as interpolant, which is not what Lyndon interpolation is about.

Definition 5.12. For a sequent Γ_1, Γ_2 such that $\Gamma_1 \to \Gamma_2$ the *splitting* is denoted by $\Gamma_1 \mid \Gamma_2$. For a splitting $\Gamma_1 \mid \Gamma_2$, the interpolant of such a splitting is the interpolant of $\overline{\Gamma_1^\sharp} \to \Gamma_2^\sharp$.

As an example, for a splitting $A \mid B$, the interpolant of such a splitting would be an interpolant of $\overline{A} \to B$. It is important to remember that for a splitting, the antecedent will be negated, otherwise one might get lost in notation.

As a next step toward understanding how interpolation works, we will construct interpolants for every possible step on a tree with split sequents. Once again, do not let the notation $\Gamma_1 \mid \Gamma_2$ deceive you into thinking that we are constructing an inference of $\Gamma_1^\sharp \to \Gamma_2^\sharp$. With that in mind, we must additionally say that if you want to find an interpolant of a certain sequent, it is best to first work out the derivation of the sequent from bottom to top, to then find the interpolant by working top to bottom. It is also good to note that we now will have differing left- and right-hand rules when working on this *split inference system.* We will ask the reader to observe that any splitting in a conclusion leads to splittings in premises, furthermore, a splitting on one side will at the very least lead to different conclusions on that side, with only the $\Box$-rule changing the other side of the split. Considering all this, we present a split inference system, where we note in parenthesis the interpolant.
First the rules for axioms that will help us start off at the leaves:
$(\top)\Gamma_1 \mid \Gamma_2, \top \quad (\bot)\Gamma_1, \top \mid \Gamma_2 \quad (\bot)\Gamma_1, A, \overline{A} \mid \Gamma_2 \quad (\overline{A})\Gamma_1, A \mid \overline{A}, \Gamma_2 \quad (\top)\Gamma_1 \mid A, \overline{A}, \Gamma_2$
Then we have the inference rules; The left conjunction rule $\wedge_l$

$$\frac{(C)\Gamma_1, A \mid \Gamma_2 \qquad (D)\Gamma_1, B \mid \Gamma_2}{(C \vee D)\Gamma_1, A \wedge B \mid \Gamma_2}$$

the left disjunction rule $\vee_l$

$$\frac{(C)\Gamma_1, A, B \mid \Gamma_2}{(C)\Gamma, A \vee B \mid \Gamma_2}$$

the right conjunction rule $\wedge_r$

$$\frac{(C)\Gamma_1 \mid \Gamma_2, A \qquad (D)\Gamma_1 \mid \Gamma_2, B}{(C \wedge D)\Gamma_1 \mid \Gamma_2, A \wedge B}$$

the right disjunction rule $\vee_r$

$$\frac{(C)\Gamma_1 \mid \Gamma_2, A, B}{(C)\Gamma_1 \mid \Gamma_2, A \vee B}$$

the left $\Box$-rule $\Box_l$

$$\frac{(C)\Gamma_1, \diamond\Gamma_1, A \mid \Gamma_2, \diamond\Gamma_2}{(\diamond C) \diamond \Gamma_1, \Box A \Delta_1 \mid \diamond\Gamma_2, \Delta_2}$$

and finally, the right $\Box$-rule $\Box_r$

$$\frac{(C)\Gamma_1, \diamond\Gamma_1 \mid \Gamma_2, \diamond\Gamma_2, A}{(\Box C) \diamond \Gamma_1, \Delta_1 \mid \diamond\Gamma_2, \Box A, \diamond_2.}$$

The validity of these rules and the correctness of the interpolant are fairly easily checked and will be left as an exercise to the reader.

Using this split inference system we can define the notion of a *split formal circular derivation* parallel to that of a formal circular derivation. A *split formal circular derivation* links a split sequent at a node x to the same sequent at a node $d(x)$ via a back-link. We note that it is still the case that such a back-link can only occur when a $\Box$-rule is applied between the nodes.

Lemma 5.13. If a formal circular proof exists of a sequent Γ_1, Γ_2 then a split circular proof exists for $\Gamma_1 \mid \Gamma_2$.

Proof. Let π be a circular proof of Γ_1, Γ_2. If we then travel bottom to top along π, i.e. from conclusions to premises, we construct a formal ∞-proof of $\Gamma_1 \mid \Gamma_2$. Since π contains only finitely many different subtrees, π will also contain finitely many different sequents. Therefore, there are only finitely many different split sequents in the split formal ∞-derivation of $\Gamma_1 \mid \Gamma_2$. Since this split formal ∞-proof must also have finitely many different split sequents, a regular split formal ∞-proof can be obtained by the same method as before. Since we can obtain a circular derivation from any regular ∞-derivation, we have then proven the lemma. $\Box$

To prove Theorem 5.11 using the notion of circular derivations and circular proofs, we first have to introduce a version of the fixed point theorem for the GL logic. Before we introduce that theorem we first define the set S^{o}. Let S be a set of literals L and marked literals L^{o}, then we define

$$S^{o} = L^{o} : L \in S \mathrm{or} L^{o} \in S$$

and we define

$$w^{*}(A) = w(A) \cup w^{o}(A).$$

That is, S^{o} would be the set that has all the literals (marked and unmarked) that are in the set S, but instead all of them will be marked. This means that the set $w^{*}(A)$ is the set of all marked and unmarked literals in $w(A)$, and then additionally the literals that were unmarked now with a marking in them. This means that if for example $w(A) = \{P, Q^{o}\}$, that $w^{o}(A) = \{P^{o}, Q^{o}\}$ leading us to the set $w^{*}(A) = \{P, P^{o}, Q^{o})$. Having gotten this preliminary process out of the way we can now introduce our intermediate theorem.

Theorem 5.14. If A is a formula in which the literals P and $\overline{P}$ occur only within the scope of a modal operator, then a formula F exists such that

$$w(F) \subset (w^*(A) \cup w^{\text{o}}(A)) \setminus \{P^{\text{o}}, \overline{P^{\text{o}}}\}$$

and

$$GL \vdash \boxdot(P \leftrightarrow A) \leftrightarrow \boxdot(P \leftrightarrow F)$$

hold simultaneously.

This theorem is a known theorem in logic, however its proof is complex enough that we will not give it here explicitly. If the reader is interested in such a proof we refer them to articles by Lindström [16] and Smoryński [29].

To apply this to sequents, we say that if we have a sequent Γ, that $\overline{\Gamma}$ is the set of negations of formulae in Γ. Additionally we define w for a sequent Γ as

$$w(\Gamma) = \bigcup\{w(A) : A \in \Gamma\}.$$

With the very intuitive definition of these expressions out of the way, we will start on the proof of Theorem 5.11 using the tools of circular logic.

Proof. (Theorem 5.11)
For the proof of Theorem 5.11 we will take an approach in which we will try to construct interpolants for all splittings of provable sequents. Assume that we have a formal circular proof for a sequent Γ_1, Γ_2. We can then find a split circular proof of the splitting $\Gamma_1 \mid \Gamma_2$ by using the tools we acquired in Lemma 5.13.

Let $\pi = (k, d)$ be such a split circular derivation of $\Gamma_1 \mid \Gamma_2$. We take a look at the sequent at all non-axiomatic leafs a of such a proof k. For such a we define X_a to be our unknown interpolant of the split sequent at this leaf. We also define w_a as the set $w(X_a)$ of literals and marked literals in X_a. Now consider such a specific leaf a that is marked by a split sequent $\Delta_1 \mid \Delta_2$. We define I_a as one part of the requirement for X_a to be an interpolant of the split sequent at a

$$I_a := \overline{(\Delta_1^\sharp} \to X_a) \wedge (X_a \to \Delta_2^\sharp)$$

and I'_a as the other part of the requirement for X_a

$$I_a := w_a \subset (w(\overline{\Delta_1}) \cap w(\Delta_2)).$$

Furthermore, for a formula D, which possibly contains the variables of X_a we define $w_X(D)$ as

$$w_X(D) := w(D) \setminus \{X_a, {X_a}^{\text{o}} : X_a \text{is contained in D,}\}$$

and we claim that a formula C must exist which contains no literals of the form $\overline{X_a}$ such that the variables $\{X_a : a \in BH(\pi)\}$ can occur in C only within the scope of modal operators. Additionally, this satisfies

$$GL \vdash \bigwedge\{\boxdot I_a : a \in H(\pi)\} \wedge \bigwedge\{\Box I_a : a \in BH(\pi)\} \to (((\overline{\Gamma_1^\sharp}) \to C) \wedge (C \to \Gamma_2^\sharp)),$$

$$\bigwedge\{I'_a : a \in H(\pi) \cup BH(\pi)\} \Longrightarrow$$

$$\mathrm{w}_X(C) \cup \bigcup\{w_a : a \in H(\pi)\} \cup \bigcup\{w_a{}^{\circ} : a \in BH(\pi)\} \subset w(\overline{\Gamma_1} \cap w(\Gamma_2). \tag{13}$$

To prove this claim we will do induction on the structure of our derivation k. If k consists of a single sequent and this sequent is an axiom, then we can use the rules for the axioms that we have defined before, and we set C equal to the interpolant specified for these axioms. If the only leaf a of the derivation k is nonaxiomatic, then we set C to be equal to X_a.

Consider the case where the derivation k does not contain any back-links. Then we can construct an interpolant for the split sequent by induction on the last application of an inference rule. Since we have seen that we can find an interpolant in case we are at a leaf that is axiomatic, and since we have also seen that we can, from such a premise, construct an interpolant for any inference rule, that gives us the sequent at the next node, this process is trivial.

The interesting case for this paper is of course when we are dealing with circular proofs and circular derivations. Consider such a case where the root of a derivation k is linked by a back-link with some leaf b on the subtree of its derivation. If we imagine the back-link to be gone for a moment, it is easy to see that we can construct the tree π_0 corresponding to this case. We can then use the same argument of induction to show that some formula C_0 exists satifying the condition of interpolant for the subtree π_0. It has been noted before that in the split case of circular proofs, we also have the result that the leaf b must be a boxed rule, i.e. $b \in BH(\pi_0)$. We then have that C_0 will contain no literals of the form $\overline{X_a}$ and variables $\{X_a : a \in BH(\pi)\} \cup X_b$ will occur in C_0 only within the scope of modal operators, as b must be boxed. We thus have

$$GL \vdash \bigwedge\{\boxdot I_a : a \in H(\pi)\} \wedge \bigwedge\{\Box I_a : a \in BH(\pi)\} \wedge \Box I_b \to (((\overline{(\Gamma_1^\sharp)} \to C) \wedge (C \to \Gamma_2^\sharp)),$$

$$\bigwedge\{I'_a : a \in H(\pi) \cup BH(\pi)\} \wedge I'_b \Longrightarrow$$

$$w_X(C) \cup w_b{}^{\circ} \cup \bigcup\{w_a : a \in H(\pi)\} \cup \bigcup\{w_a{}^{\circ} : a \in BH(\pi)\} \subset w(\overline{\Gamma_1}) \cap w(\Gamma_2). \tag{14}$$

Now we can use Theorem with $P = X_a$ 5.14 to show the existence of a formula F with the properties that $w(F) \subset w^*(C_0) \setminus \{X_b\}$ and

$$GL \vdash \boxdot(X_b \leftrightarrow A) \leftrightarrow \boxdot(X_b \leftrightarrow F)$$

We can then replace all occurrences of X_b in C_0 by this formula F. We will call the resulting formula C. What is left is to check if C satisfies the required conditions for the tree π. It is clear that C will not contain any literals of the form $\overline{X_a}$. The variables of $X_a : a \in BH(\pi)$ will only occur in C within the scope of a modal operator.

Now since

$$GL \vdash I_b(F) \leftrightarrow (((\overline{(\Gamma_1)^\sharp}) \to C) \wedge C \to \Gamma_2^\sharp)),$$

we can drop $\Box I_b(F)$ from the formula

$$GL \vdash \bigwedge\{\boxdot I_a : a \in H(\pi)\} \wedge \bigwedge\{\Box I_a : a \in BH(\pi)\} \wedge \Box I_b \to (((\overline{(\Gamma_1^\sharp)} \to C) \wedge (C \to \Gamma_2^\sharp)),$$

by Löb's theorem on GL, the same step that we used to prove the last step of the proof for the equivalency of circular proofs.

The final thing we have to verify is the following restriction on $w_X(C)$:

$$w_X(C) \subset w(\overline{\Gamma_1}) \cap w(\Gamma_2).$$

Assume we have

$$\bigwedge\{I'_a : a \in H(\pi) \cup BH(\pi) \wedge I'_b.\}$$

then we should have, by 14, that

$$I'_b \Longrightarrow w_X(C_0) \cup w_b{}^{\text{o}} \subset w(\overline{\Gamma_1}) \cap w(\Gamma_2).$$

Taking a sequent such that $I_b = \emptyset$ we get that

$$w_X(C_0) \subset w(\overline{\Gamma_1}) \cap w(\Gamma_2).$$

This statement is the meaning of $I'_b(w_X(C_0))$, which therefore is valid. We can now replace the unknown w_b in I'_b by $w_X(C_0)$ and obtain the statement

$$w_X(C_0) \cup w_X{}^{\text{o}}(C_0) \subset w(\overline{\Gamma_1}) \cap w(\Gamma_2).$$

This means that

$$w_X(C) \subset w_X(C_0) \cup w_X{}^{\text{o}}(F) \subset w_X(C_0) \cup w_X{}^{\text{o}}(C_0) \subset w(\overline{\Gamma_1}) \cup w(\Gamma_2),$$

from 14 we can then get, due to $w_X(C_0) \cup w_X{}^{\text{o}}(F) \subset w(\overline{\Gamma_1} \cup w(\Gamma_2)$,

$$I'_b \Longrightarrow \bigcup\{w_a : a \in H(\pi)\} \cup \bigcup\{w_a{}^{\text{o}} : a \in BH(\pi)\} \subset w(\overline{\Gamma_1}) \cap w(\Gamma_2).$$

We can then by replacing w_b in I_b by $\emptyset$ obtain

$$\bigcup\{w_a : a \in H(\pi)\} \cup \bigcup\{w_a{}^{\text{o}} : a \in BH(\pi)\} \subset w(\overline{\Gamma_1}) \cap w(\Gamma_2).$$

This means that the final condition we had to satisfy, formula 13 is now satisfied. Therefore, we can finally assert that for a split formal circular proof $\pi = (k, d)$ of the split sequent $\Gamma_1 \mid \Gamma_2$, we can take this formula C as the interpolant. □

We note that this proof is a bit stronger than the theorem for Lyndon interpolation, since we have a stronger restriction on the variables in C, $w_X(C)$, namely

$$w_X(C) \subset w_X(C_0) \cup w_X{}^{\text{o}}(F) \subset w_X(C_0) \cup w_X{}^{\text{o}}(C_0) \subset w(\overline{\Gamma_1}) \cup w(\Gamma_2)$$

instead of the slightly weaker condition on C for Lyndon interpolation

$$w_X(C) \subset w(\overline{\Gamma_1}) \cup w(\Gamma_2).$$

6 Conclusion and Discussion

Circular proofs are a relatively new field of study. The applications for circular proofs certainly go beyond their application in the the logic GL. Within this paper, we have seen that the application of a circular proof can be a useful alternative to the use of cut-rules with respect to certain proof-systems, specifically when making derivations using Sequent Calculus. We have also seen that circular proofs allow us to prove stronger versions of certain theorems and can make it easier to find proofs in logical systems.

We can conclude that there are methods to circumvent having to use the cut-rule in derivations. For this conclusion alone, the paper will be useful to logicians that are looking to remove the annoying cut-rule from their derivations and proofs. Surely, having seen that alternatives exist will spur logicians to try to apply circular proofs to other logical systems. We can also conclude that by replacing the cut-rule, not only do we get an equivalent system of derivation, the new system is also useful in practice.

We hope that this paper has given a detailed account of the workings of circular proofs, and expanded the knowledge of the reader in the field of logical proofs and proof systems. Though the results shown in this paper are not new results, with the discussed paper [27] having been published in 2014, the results are still recent and their implications have surely not been exhausted.

In the future, we can expect more work to be done in the field of circular proofs. Perhaps circular proofs allow us to prove more theorems in the Gödel-Löb provability logic, or construct new results that can help us find proofs for statements in Peano arithmetic. We can definitely expect circular proofs to be applied to other logical systems, perhaps together with stronger conditions on when a circular derivation can be made. The use of circular proofs in removing cut-rules will definitely be useful to researchers looking to automate proofs. It is likely that other methods of removing cut-rules will be attempted and they might even succeed in doing so for the logic GL, or perhaps different logics, but with circular proofs as a method that has shown success, there is an example that researchers can try to look at for inspiration in finding these other methods of removing cut-rules for different logical systems. For example, there has already been a paper published by Afshari and Leigh [1] on circular proofs for the modal μ-calculus, showing that the use of circular proofs is not limited to the domain of the logic GL. With more research like this being done, we can expect to see more uses for circular proofs in certain types of programming and automation.

We hope that by reading this paper, we have given the reader enough background that they may try to find their own results in the fields of circular proofs and proofs theory. Since there are many different logics that use cut-rules, there are many different systems to try to apply circular proofs to. Though the goal of this paper was to explain the details behind circular proofs, using the information gained by reading this paper it should be possible to at least give a shot at adapting circular proofs to other logical systems that the reader is already familiar with. Though there is no guarantee that new results will be found in such a way, we wish any reader that will give a try at finding new results in this manner the best of luck in their endeavors.

Acknowledgements The writer wishes to acknowledge professor L.C. Verbrugge in her work and patience in proofreading this paper. I wish to express my thanks for her guidance during the writing of this paper. Even though the circumstances during the time of writing of this paper were extraordinary, she put in her time and effort in supervising the writing of this paper and for that she has my thanks.

I also wish to acknowledge professor Shamkanov who wrote the original paper on circular proofs and thank him for his quick response to my questions about his paper.

References

[1] B. Afshari and G. E. Leigh. Circular proofs for the modal mu-calculus. *PAMM*, 16(1):893–894, 2016.

[2] J. Brotherston and A. Simpson. Sequent calculi for induction and infinite descent. *Journal of Logic and Computation*, 21(6):1177–1216, 10 2010.

[3] H. P. Cooke and H. Tredennick. *Aristotle: The Organon*. Harvard University Press, 1938.

[4] H. B. Curry. *Foundations of mathematical logic*. Courier Corporation, 1977.

[5] G. D'Agostino. Interpolation in non-classical logics. *Synthese*, 164(3):421–435, 2008.

[6] G. Gentzen. *Untersuchungen über das logisches Schliessen*. Universität Göttingen, 1935.

[7] G. Gentzen. Die gegenwartige Lage in der mathematischen Grundlagenforschung. *Deutsche Mathematik*, 3:255–268, 1939.

[8] G. Gentzen. Beweisbarkeit und Unbeweisbarkeit von Anfangsfällen der transfiniten Induktion in der reinen Zahlentheorie. *Mathematische Annalen*, 119(1):140–161, 1943.

[9] R. Goré and R. Ramanayake. Valentini's cut-elimination for provability logic resolved. *The Review of Symbolic Logic*, 5(2):212–238, 2012.

[10] K. Gödel. *On formally undecidable propositions of Principia Mathematica and related systems*. Dover Publications, 1992. Translation B. Meltzer.

[11] L. Henkin. A problem concerning provability. *Journal of Symbolic Logic*, 17(2):160, 1952.

[12] D. Hilbert. *Grundlagen der Geometrie*. Leipzig: B.G. Teubner, 1899.

[13] E. Jeřábek. Admissible rules of modal logics. *Journal of Logic and Computation*, 15(4):411–431, 2005.

[14] O. Ketonen. Untersuchungen zum Prädikatenkalkul. *The Journal of Symbolic Logic*, 10(4):127–130, 1945.

[15] D. Leivant. On the proof theory of the modal logic for arithmetic provability. *The Journal of Symbolic Logic*, 46(3):531–538, 1981.

[16] P. Lindström. Provability logic—a short introduction. *Theoria*, 62(1-2):19–61, 1996.

[17] M. H. Löb. Solution of a problem of Leon Henkin 1. *The Journal of Symbolic Logic*, 20(2):115–118, 1955.

[18] S. Negri. Proof analysis in modal logic. *Journal of Philosophical Logic*, 34(5-6):507, 2005.

[19] F. Poggiolesi. A purely syntactic and cut-free sequent calculus for the modal logic of provability. *The Review of Symbolic Logic*, 2(4):593–611, 2009.

[20] W. V. O. Quine. A proof procedure for quantification theory. *The Journal of Symbolic Logic*, 20(2):141–149, 1955.

[21] M. Rathjen and W. Sieg. Proof theory. In *The Stanford Encyclopedia of Philosophy.* Metaphysics Research Lab, Stanford University, fall 2018 edition, 2018.

[22] L. Reidhaar-Olson. A new proof of the fixed-point theorem of provability logic. *Notre Dame J. Formal Logic*, 31(1):37–43, 12 1989.

[23] G. Sambin. An effective fixed-point theorem in intuitionistic diagonalizable algebras (the algebraization of the theories which express Theor, ix). *Studia Logica: An International Journal for Symbolic Logic*, 35(4):345–361, 1976.

[24] K. Schütte. Schlußweisen-kalküle der Prädikatenlogik. *Mathematische Annalen*, 122(1):47–65, 1950.

[25] D. S. Shamkanov. Non–well-founded derivations in the Gödel-Löb provability logic. *The Review of Symbolic Logic*, page 1–21.

[26] D. S. Shamkanov. Interpolation properties for provability logics GL and GLP. *Proceedings of the Steklov Institute of Mathematics*, 274(1):303, Oct 2011.

[27] D. S. Shamkanov. Circular proofs for the Gödel-Löb provability logic. *Mathematical Notes*, 96(3-4):575–585, 2014.

[28] D. S. Shamkanov. A realization theorem for the Gödel-Löb provability logic. *Sbornik: Mathematics*, 207(9):1344–1360, Sep 2016.

[29] C. Smoryński. Modal logic and self-reference. In *Handbook of Philosophical Logic*, pages 441–495. Springer, 1984.

[30] R. M. Solovay. Provability interpretations of modal logic. *Israel Journal of Mathematics*, 25(3):287–304, Sep 1976.

[31] S. Valentini. The modal logic of provability: Cut-elimination. *Journal of Philosophical Logic*, 12(4):471–476, 1983.

[32] L.C. Verbrugge. Provability logic. In *The Stanford Encyclopedia of Philosophy.* Metaphysics Research Lab, Stanford University, fall 2017 edition, 2017.

[33] J. von Plato. The development of proof theory. In *The Stanford Encyclopedia of Philosophy.* Metaphysics Research Lab, Stanford University, winter 2018 edition, 2018.